Adapting to Technological Trends: Instituting an Electronic Evidence Recovery Technician

Craig Timko

Abstract

This research paper discusses the value and frequency that surveillance video and mobile phone evidence are used in criminal cases as well as some pitfalls encountered during prosecution. Data was compiled by surveying a detective unit in an effort to determine the utility of training a dedicated civilian employee to collect and process these forms of electronic evidence.

Introduction

There are various forms of evidence that law enforcement officers use to investigate criminal cases, and attorneys use to prosecute cases. While physical evidence left behind at the scene of a crime such as latent fingerprints, blood, or DNA, have long been the cornerstone of criminal prosecution, the past couple decades have introduced new forms of evidence thanks to technological advancements. This research paper will focus on video evidence captured on CCTV cameras at or near a crime scene, as well as mobile phone evidence gleaned from cellular technology, and who should be recovering it.

Modern society has fundamentally embraced video surveillance. Thanks to the advancements in technology, higher quality cameras can be purchased at a cheaper price than ever before. Similarly, the ability to store vast amounts of data is easier than ever thanks to “cloud storage” and the advancements in processing power and software. Local businesses, police, banks, ATMs, schools, and private residences are commonly installing CCTV cameras to protect their investments. There are an estimated 30 million surveillance cameras now deployed in the United States shooting 4 billion hours of footage a week. Vast networks of cameras around any given city regularly prove invaluable to investigators who are looking to capture a suspect description, vehicle make or model, or direction of travel to expand the crime scene search. (Vlahos, 2009)

Mobile phones have essentially become extensions of our beings in this day in age. The vast majority of Americans, 95%, now own a cellular phone of some kind. The share of Americans who own smartphones is now 77%, up from 35% in a survey conducted in 2011. The vast number of mobile phones in the pockets of Americans increase the likelihood that cellular data can be used to put a suspect at the scene of a crime. The challenges become collecting and understanding the vast amounts of data available. (Pew Research Center, 2018)

It is naive of us to think that we can stop these technological advances, especially as they become more affordable and are hard-wired into everyday life. Law enforcement routinely adapts with changing trends as noticed after September 11, 2001, the IRS green dot scams of the early 2000s, and body worn cameras of today. The problem that this research paper will focus on is the inherent complexities involved with collecting video and cellular data evidence and testifying about each in court.

Literature Review

CCTV Video as Evidence:

Law enforcement investigators around the world rely on video footage from CCTV cameras around crime scenes to assist in the investigation of crimes. The video recordings of the actual crime as it was committed is extremely valuable evidence for the jury to view during the trial. A recent study demonstrates the value of video footage used by Scotland Yard detectives while investigating murders. A 2009 report showed that of 90 murder cases recorded that year, CCTV footage was used in 86 of those cases. According to senior officials, 65 of those cases were solved solely because the crimes were tracked on video either before or after the crime occurred. According to Commander Simon Foy of Scotland Yard's Homicide Department, CCTV cameras are as important as forensic evidence like DNA samples and fingerprints in the investigations conducted by their detectives. (Edwards, 2009)

Challenges of Video Collection:

Current digital CCTV services rely on digital transformation of the data that it records. The challenge that this digital transformation creates is the lack of interoperability between the recording system itself, and the software provided to law enforcement investigators and trial attorneys to collect and share the files. Each system works independently of each other and are not integrated. With so many digital video file formats in use today, law enforcement is limited to download only the format compliant with the software that they have for viewing. This format may not be the native format, which provides the most utility to the forensic enhancing of the video. It is important for the process of downloading, sharing, and playing the video evidence to be on a common platform to make the process of collection and sharing more efficient and decreasing the risk of loss. (Perkins, 2018)

A vast number of residential CCTV camera systems are increasingly moving toward cloud storage of the recorded data versus storing the data locally on a recorder. In theory, that would make the recovery of the data easier to obtain. However, investigators must rely on home owners to be on scene and available, have a working knowledge of their system, and have the passwords and access to the accounts. Hours, and even days, can be spent making appointments with business managers and homeowners collect video footage. This process currently involves law enforcement investigators, who have little to no training, acting as glorified couriers responding to scenes to manually download footage onto disks or USB memory sticks. This process presents a waste of time for the investigator and a significant drain on resources. (Perkins, 2018)

Once the investigator receives a copy of the video, actually viewing it can be a bigger challenge. The investigator must first attempt to find the appropriate file format that will play on the agency issued computer that they are provided. They may spend hours searching the internet, as well as security camera forums and websites trying to identify the correct viewing software. This process is hugely inefficient, especially if the agency computer has firewalls which block the downloading of the viewing software. Once the investigator is able to view the footage, the next time consuming process is sifting through the multiple camera angles for the length of time needed to review the entire video. (Perkins, 2018)

CCTV Video in the Courtroom:

Regardless of how good the video is, the video evidence can be deemed inadmissible if the investigator can't authenticate it. In the past, video evidence was recorded directly onto a videotape. The chain of custody could easily be documented from receipt of the videotape, to the playing of the footage in open court. However, we now live in an age where recorded video can be edited to rearrange the chronology of events depicted, distort the passage of time, and display events out of sequence and context. The video evidence typically gets compressed during the recording process in order to save vast amounts of data onto the hard drive or cloud. This compression of data can lead to data loss as well as having negative impacts on image quality. (Careless, 2011)

With the advancements of digital video technology, the investigator has to download the video evidence onto an external recording device, requiring very detailed procedures, witnessing, and documentation to prove that the evidence is unedited, and an exact copy of the original. The investigator must establish how the video was recorded, what impact the recording process had on the captured video, whether the exporting of the video has further compromised the reliability of the images, and whether all relevant video has been obtained of the incident in question. If the investigator lacks the technical expertise and training to explain this authentication process, the video evidence may not be admissible. (Careless, 2011)

In Hollywood films and television programs like CSI, the American public has an expectation that law enforcement can professionally enhance video beyond what is actually possible. This phenomenon is known as the CSI effect: An assumption on the part of the juries that grainy video evidence can be infinitely resolved down to the smallest detail. In real life however, it is only possible to enhance the brightness, contrast, and color of an image to display better detail by using special computer programs. This type of video enhancement comes with a risk: The more the video is enhanced, the more likely the video is no longer accurate or fair since the evidence has been altered from the original form. (Careless, 2011)

An investigator cannot simply walk into a court and push play and assume the jury will fully understand the contents. The courts will rely on one or more expert witnesses to explain what the jury is viewing. This testimony is necessary to explain the impact of technical issues such as frame rates, multiple camera views, aspect ratios, compression, video tracking, and the alignment of audio and video images in relation to real time. A properly trained and qualified expert can explain the overall events that are depicted as well as the fine details that are often overlooked since the investigator will have spent several hours examining the footage. Video evidence has been compared to nitroglycerin: Properly handled, it can demolish a defendant. Carelessly managed, it can blow up in your face. (Careless, 2011)

Mobile Phone Evidence:

The development of cellular technology has changed the way people communicate. While initially designed to be a simple form of communication, cellular technology has developed to allow a cellular device to act much more like a personal computer. Cellular devices enable users to email, send photographs, videos, they are capable of storing information, provide a means for paying for goods, and they provide a means of enabling criminal activity. Technology manufacturers have taken note of this trend, which has led to increased security measures and encryption on memory chips. These security measures provide a security blanket for customers, but has become increasingly more difficult for law enforcement investigators to gain access to the devices. From a law enforcement point of view, having the ability to search for photographs, internet history, GPS, and location services is essential to investigating criminal activities.

As previously described, digital evidence can have a profound impact in court and requires handling in a secure manner with a proper chain of custody. While law enforcement investigators face challenges defeating security measures to access mobile device evidence, the first challenge they likely face is the collection of the device itself. Limited training is provided to law enforcement investigators when it comes to recovering the device, potentially exposing the case to unnecessary scrutiny or the loss of data altogether. A guide for first responders issued by the USSS lists a set of rules on whether to turn on or off the device. (USSS, 2006)

- If the device is "ON", do NOT turn it "OFF".
- Turning it "OFF" could activate lockout feature.
- Write down all information on display (photograph if possible).
- Power down prior to transport (take any power supply cords present).
- If the device is "OFF", leave it "OFF".
- Turning it on could alter evidence on device (same as computers).
- Upon seizure get it to an expert as soon as possible or contact local service provider.
- If an expert is unavailable, USE A DIFFERENT TELEPHONE and contact 1-800-LAWBUST (a 24 x 7 service provided by the cellular telephone industry).
- Make every effort to locate any instruction manuals pertaining to the device.

Once the mobile device is provided to a forensic examiner, the practitioner must have the ability to collect the evidence despite the passwords, protections, and encryptions. Commercial vendors such as Cellebrite, offer exclusive services to law enforcement agencies worldwide for device examination. The devices, whether unlocked or locked can be sent to Cellebrite for advanced unlocking services. For devices that are locked, Cellebrite can determine or disable the PIN, pattern or passcode screen lock (Cellebrite, 2018).

Some agencies opt to purchase and operate their own Cellebrite machines and software to download devices within their facilities in lieu of sending the devices out. The use of underqualified and rarely trained law enforcement investigators to forensically examine a device and testify about the procedures in court can present issues. Digital evidence is very complex and without the proper training, an entire case can be compromised in court. The Committee on Identifying the Needs of the Forensic Sciences Community has identified three challenges that face digital forensics:

- The digital evidence community does not have an agreed certification program or list of qualifications for digital forensic examiners.
- Some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity.
- There is wide variability in and uncertainty about the education, experience, and training of those practicing this discipline. (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009)

Methods

The purpose of this research was to identify whether or not an Electronic Evidence Recovery Technician would have utility to a General Offense Detective, and if so, to what extent. The data for this research was gathered through surveys which were distributed to District III General Offense Detectives at the Hillsborough County Sheriff's Office.

The survey questions were designed to determine the level of usefulness that an Electronic Evidence Recovery Technician could provide. Questions also inquired about the amount of training detectives have received and the frequency of electronic evidence collection. The survey also provided an open text field allowing the participant to provide thoughts and opinions which were not covered in the designed questions. The questions in this survey were specifically designed to illicit relevant data to determine whether or not an EERT would be a viable option for a District level General Offense Detective.

The survey was anonymous in order to encourage truthful answers and to decrease participant suspicion. A weakness in the data collection instrument is that it relies on participant opinions, estimation of time, and estimation of usefulness. In addition, the survey results are being collected by a commanding officer which could create a lack of candor.

Results

The survey was printed out and provided to 16 detectives assigned to the Hillsborough County Sheriff's Office Investigative section at District III. All 16 detectives completed the survey for a 100% response rate. Each survey was completed in its' entirety, and only 4 respondents opted to provide additional comments on the form. The survey offers a 1-5 Likert scale where the respondent can select:

5 = Strongly Agree,
4 = Agree,
3 = Neither Agree/Nor Disagree,
2 = Disagree,
1 = Strongly Disagree.

The first survey item indicated the extent to which the respondent agreed or disagreed with the statement that they were formally trained to recover video evidence.

4 indicated that they strongly disagree (25%),
5 indicated they disagree (31%),
3 indicated they neither agree nor disagree (19%),
2 indicated they agree (12.5%), and
2 indicated they strongly agree (12.5%).

The second survey item indicated the extent to which the respondent agreed or disagreed with the statement that they do not encounter software issues while recovering video surveillance.

8 indicated that they strongly disagree (50%),
6 indicated they disagree (37.5%),
1 indicated they agree (6.25%), and
1 indicated they strongly agree (6.25%).

The third survey item indicated the extent to which the respondent agreed or disagreed with the statement that video surveillance is important to their case work.

All 16 respondents indicated they strongly agree (100%).

The fourth survey item indicated the extent to which the respondent agreed or disagreed with the statement that a significant portion of their job function involves collecting video surveillance.

11 respondents indicated that they strongly agree (68.75%).
The remaining 5 respondents indicated they agree (31.25%).

The fifth survey item indicated the extent to which the respondent agreed or disagreed with the statement that a civilian assigned to the unit to recover/enhance video surveillance would be useful.

All 16 respondents indicated they strongly agree (100%).

The sixth survey item indicated the extent to which the respondent agreed or disagreed with the statement that they often use evidence collected from mobile device technology.

11 respondents indicated that they strongly agree (68.75%).
The remaining 5 respondents indicated they agree (31.25%).

The seventh survey item indicated the extent to which the respondent agreed or disagreed with the statement that they do not wait long for the results of a phone download.

5 indicated that they strongly disagree (31%),
8 indicated they disagree (50%),
3 indicated they neither agree nor disagree (19%).

The eighth survey item indicated the extent to which the respondent agreed or disagreed with the statement that the challenges of collecting and downloading mobile device evidence is causing them to sacrifice investigative leads.

1 indicated that they strongly disagree (6.25%),
1 indicated they disagree (6.25%),
8 indicated they agree (50%), and
6 indicated they strongly agree (37.5%).

The ninth survey item indicated the extent to which the respondent agreed or disagreed with the statement that a civilian assigned to the unit to download phones on site would be useful.

15 respondents indicated they strongly agree (93.75%), and
1 indicated they agree (6.25%).

The tenth survey item provided an open text field for any additional comments.

4 respondents (25%) added comments.

Two of the comments stated that a civilian assigned to the unit would be beneficial to allow detectives to focus on the case and how time consuming phone downloads could be. One comment indicated that having software to view videos would be beneficial, and the final comment indicated a civilian position would be a tremendous asset to the unit.

Discussion

The survey, although basic in form, illustrated the importance of collecting electronic evidence. All of the respondents (100%) strongly agreed that video surveillance is important to their case work and that a civilian assigned to the unit to recover/enhance video surveillance would be useful. Additionally, all of the respondents (100%) either strongly agree or agree that they often use evidence collected from mobile device technology.

The survey also made it apparent that a significant portion of the respondent's job function involves collecting video surveillance, with 100% either agreeing or strongly agreeing, and 81.25% of respondents strongly disagreeing or disagreeing that they do not wait long for phone downloads.

The literature described in detail the importance of having a properly trained and qualified expert to testify to the overall events in a video as well as to explain the impact of technical issues such as frame rates, multiple camera views, aspect ratios, compression, video tracking, and the alignment of audio and video images in relation to real time. The survey revealed that over half (56%) of the respondents indicated they strongly disagree or disagree that they were formally trained to recover video evidence.

One limitation of this survey is that it allowed the respondent to simply circle the 1-5 responses on the Likert scale. A recommendation for a future survey would be to force the respondent to write in the answer in lieu of circling the number. By writing the answer, it would likely reduce the chance of accidental misinterpretations of the scale.

Major Craig Timko was born and raised in Warren, OH. He is a veteran of the US Army, where he served until 1999 as an infantry soldier and member of the Old Guard in Arlington, VA. He was hired by the Hillsborough County Sheriff's Office in 2000, where he patrolled the streets of District III. Craig spent the majority of his career serving as a member of the SWAT team, eventually serving as the SWAT team leader. He has worked a variety of assignments including detective, Recruitment and Screening, General Offense, Homeland Security, and served as the deputy division commander for the Criminal Investigations Division until being promoted to Major. He currently serves as the district commander for District III, which services the northwest portion of the county. He earned a Bachelor of Arts Degree and a Master of Science Degree in Criminal Justice from Saint Leo University and is an active member of the Tampa Kiwanis club.

References

Careless. J. (2011, April 21). Video evidence. *Canadian Bar Association.* Retrieved from http://www.cba.org/Publications-Resources/CBA-Practice-Link/2015/2011/Video-Evidence

Cellebrite. (2018). *Advanced unlocking services*. Retrieved from https://www.cellebrite.com/en/services/advanced-unlocking-services

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. (2009). *Strengthening forensic science in the United States: A path forward.* Retrieved from https://www.nap.edu/read/12589/chapter/1#iv

Edwards, R. (2009, January 1). Seven of ten murders solved by CCTV. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/uknews/law-and-order/4060443/Seven-of-ten-murders-solved-by-CCTV.html

Perkins, R. (2018, March 9). Caught on camera: the CCTV challenges facing police forces. *NICE.* Retrieved from https://www.nice.com/protecting/blog/Caught-on-camera-the-CCTV-challenges-facing-police-forces-657

Pew Research Center. (2018, February 5). Demographics of mobile device ownership and adoption in the United States. Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

USSS. (2006). *Best practices for seizing electronic evidence.* Retrieved from http://www.ustreas.gov/usss/electronic_evidence.shtml

Vlahos, J. (2009, October 1). Surveillance society: New high-tech cameras are watching you. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/military/a2398/4236865/

Appendix A

<u>Detective Survey Instructions:</u>

Research is currently being conducted to evaluate the utility of an Electronic Evidence Recovery Technician (EERT). This new civilian position would be assigned to your squad to recover/enhance surveillance video, and to process mobile devices. The information gained from this survey will be used to evaluate the need for an EERT. Your candid responses to this survey will be anonymous. It should take approximately 5 minutes to complete this confidential survey. Please select the extent to which you agree or disagree with the statements below using the provided scale.

1 2 3 4 5 *I have been provided formal training on how to recover video evidence.*

1 2 3 4 5 *I do not encounter any software issues while attempting to recover/view video surveillance.*

1 2 3 4 5 *Video surveillance is important to my case work.*

1 2 3 4 5 *A significant portion of my job function involves collecting video surveillance.*

1 2 3 4 5 *A CSA would be useful if assigned to my unit to recover/enhance video surveillance.*

1 2 3 4 5 *I often use evidence collected from mobile device technology.*

1 2 3 4 5 *I do not wait long for the results of a phone download.*

1 2 3 4 5 *The challenges of collecting and downloading mobile device evidence is causing me to sacrifice potential investigative leads.*

1 2 3 4 5 *A CSA would be useful if assigned to my unit to download phones for me on site.*

1 2 3 4 5 *I have additional comments regarding these topics that I would like to share. (Use space provided below for comments)*

5 = Strongly Agree, 4 = Agree, 3 = Neither Agree/Nor Disagree, 2 = Disagree,

1 = Strongly Disagree.