Caught on Bodycam Video:

Exploring Issues of Preservation, Privacy, and Access

By Caroline Z. Oliveira

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Arts

Moving Image Archiving and Preservation Program Department of Cinema Studies

New York University

May 2018
# Table of Contents

Acknowledgments ................................................................................................................................................. 2

Introduction - Brief History of Video Surveillance ......................................................................................... 3

Chapter 1: Recording the Video ..................................................................................................................... 16

Chapter 2: Preserving the Video ................................................................................................................... 32

Chapter 3: Privacy and the Camera ............................................................................................................... 49

Chapter 4: Access .......................................................................................................................................... 68

Chapter 5: What Does the Future Look Like? ............................................................................................ 80

Closing Thoughts ............................................................................................................................................. 90

Glossary ............................................................................................................................................................ 92

List of Figures ................................................................................................................................................ 93

Bibliography .................................................................................................................................................... 94
Acknowledgments

I would like to thank Snowden Becker for being a brilliant thesis advisor. Her constant support, reassurance, and guidance made me feel confident and able to write about a very intimidating topic.

I would also like to thank Howard Besser, my MIAP advisor, for his constant encouragement and support since day one in this program.

Finally, I would like to thank my family for their support and Tony Mango for not only helping me with proofreading but also for cheering me on and not letting me give up.
Introduction - Brief History of Video Surveillance

Body-worn cameras, just like any other technology, did not appear out of anywhere, but resulted from a series of developments in a long history of crime prevention and audio-visual materials. Film photography started being used as a crime control tool almost as soon as cameras were invented, and by the 1850s, James Gardner, governor of Bristol Gaol, was already photographing prisoners in his custody for what he called his *Rogues’ Gallery* – an attempt to identify habitual criminals. In fact, this activity, which was being officially encouraged both in France and Britain, tried to address individual and statistical classifications:

- Individual classification addressed the concern of identifying habitual criminals in order to eliminate them from society, which at the time was done by imprisonment or transportation of the individuals to a British colony. However, with the demise of the Victorian transportation system and the creation of laws and financial circumstances limiting how long recidivist offenders could be kept incarcerated, these photographic records allowed law enforcement to monitor criminals who had been released.

- Statistical classification, on the other hand, was about cataloging physical characteristics recidivist criminals were believed to have in common. Francis Galton, who was also the father of the eugenics movement, believed this type of identification could help decrease crime in future generations by preventing these individuals from having children.¹

Although photographic cameras assisted with the monitoring and control of the incarcerated during the nineteenth century, they were yet to realize their full potential as crime deterrent tools,

---

since they were only able to take still images of subjects, which then had to be processed and developed.

Despite being a slow and not so practical process, Britain continued its tradition of photographing prisoners and, in 1913, Scotland Yard made use of what is considered to be the first modern photographic surveillance, “marking a new era of surveillance and intelligence gathering.”2 When members of the Women’s Social and Political Union (WSPU), more popularly known as suffragettes, kept evading police officers’ attempts to take their photographs during their incarceration at the Holloway Prison, British officials realized they needed a new strategy. Files from the Home Office – United Kingdom’s “lead government department for immigration and passports, drugs policy, crime, fire, counter-terrorism, and police”3 – which were uncovered at the National Archives in Kew in the early 2000s, document how officers first tried to photograph these political activists, including:

A remarkable picture of Evelyn Manesta (...), a young woman from Manchester (...) She has the arm of a prison warder around her throat to restrain her and she is grimacing in an attempt to distort her face. The somewhat grotesque result was used in a wanted poster of Manesta circulated by Scotland Yard but the image was doctored to hide the warder's arm around her throat [with a scarf] and the embarrassment of the police at their brutal treatment of the women.4

---


Purposely distorting or hiding their faces and moving constantly were effective tactics employed by this group of 18 inmates and since film speeds were much slower, officers were not able to obtain identifiable pictures of them. In an attempt to solve the problem, the Home Office issued the order that pictures should be taken “covertly, from far away, and without the inmates’ knowledge or consent.” Following a series of unsuccessful first attempts, the home secretary himself authorized the purchase of a Wigmore Model 2 reflex camera that was to be fitted with an 11-inch-long Ross Telecentric lens, at the time state-of-the-art equipment that not only was

---

portable but was also able to take close-up photographs from a considerable distance. Armed with the new gear, the expert commissioned photographer, Mr. A. Barrett, sat inside a van parked near the exercise yard at the prison and successfully snapped photographs of the women.⁶ The results were images similar to modern-day paparazzi shots, and it allowed detectives to compile “photographic lists of key suspects, [in an attempt] to stop arson attacks, window-smashings or the dramatic scenes of women chaining themselves to Parliament's railings.”⁷

Film cameras continued to evolve through the years, but it was not until the “invention of the television, which became commercially viable in the 1930s,”⁸ that this equipment became potentially able to execute surveillance of remote sites, although the process was limited and time-consuming as film still had to be developed in order to be viewed. In 1942 Germany, engineers developed a rudimentary camera that was able to transmit live feeds, allowing them to safely monitor the launch of a V2 rocket from a safe distance. By the end of World War II, Americans were also using similar devices to monitor test launches from their Atomic programme.⁹

With the advent of the Videocassette Recorder (VCR) in the 1960s, it became possible to capture moving images cheaper and faster, with the added possibility of instant playback. As early as 1965, cameras started being installed in public spaces, and with the commercial release of videocassette tapes, video surveillance became commonplace around the world, with its use

---

ranging from traffic control to divorce proceedings. This system became known and Closed-Circuit Television (CCTV).

As the name implies, CCTV is a closed system where all the elements are connected. For this reason, it is unable to pick up signals from airwaves like broadcast television does. As the years passed and technology improved, CCTV cameras were able to provide clearer image, some mobility (some cameras are able to rotate 360 degrees, move vertically, and horizontally), and the ability to create digital files of the recordings, instead of relying on analog tapes. Nowadays, the cameras in these systems can be:

- Static, or able to pan, tilt, and zoom, which can either be controlled by operators or programmed to move a certain way.
- Fixed to one single location, re-deployable (moved around power points within an area), or mobile (placed in vehicles and transported to where they are needed.)
- Able to transmit analog or digital images, via cable or wireless links.

Although this camera system was first marketed as a game-changing crime prevention tool, CCTV schemes, similarly to other private crime prevention strategies such as alarm systems in residences, often offered “selectively targeted and selectively experienced” benefits, since only areas where they were installed could see any advantages. In fact, various studies have been conducted over the years and none of them have been able to ultimately prove these cameras produce results in crime displacement or crime reduction, especially since the success of this

---

technology also depends on types of crime (acquisitive, drug-related or alcohol-related, violent crimes, etc.), nature of the area where the system was installed (CCTV systems tend to be more successful as a crime prevention tool in small, contained areas), size of the security systems, types of cameras employed, available light, the way control room technicians communicate with the police, and management of the schemes. Nonetheless, these systems have become popular all over the world: According to a 2011 survey, there are over 1.9 million cameras in the United Kingdom, one for every 32 U.K. residents, and since the 9/11 terrorist attacks, large U.S. cities like Chicago and New York have employed CCTV systems on public transit, business areas, and high-end residences.

Dashboard cameras (dashcam) are portable cameras that, as the name suggests, are mounted directly onto a car’s dashboard or windshield with an adhesive tape or suction cup mount. These are “single, dual or multi-channel [specialized cameras] purposely built and used to capture and record visual events that occur outside and (some instances) inside your vehicle (depending on model.)” Nowadays, videos are recorded and stored within an SD or MicroSD memory card and files can be played back on a computer with the appropriate software, television, streamed wirelessly to a smartphone, or on the camera itself.

However, dashcams have been used by police officers for decades and the first models were very rudimentary. Possibly the first mention of a dashcam is found in a 1939 edition of the Popular Science magazine, where a small article details how an officer from the California Highway Patrol used his personal film camera inside his patrol vehicle to capture images of

---

traffic violations that could be later used in court.\textsuperscript{17} There is also a report on a 1940 issue of the LA Times of 35mm film cameras being attached to police cars through a hole cut on the roof that would record traffic violations.\textsuperscript{18}

Figure 2. “Movie Camera in Police Car Puts Evidence on Film,” \textit{Popular Science}, September 1939.

Similarly to CCTV systems, the invention of the VCR in the 1960s brought some advantages to the in-car camera system but still did not solve the problem of how to best mount the cameras inside the vehicles. By the 1970s, some police agencies had adopted systems that secured “videocassette recorders (VCR) in the trunk of a patrol vehicle, with a camera hard-wired to it, of course, mounted on the dash.”\textsuperscript{19}

\textsuperscript{17} “Movie Camera in Police Car Puts Evidence on Film,” \textit{Popular Science}, September 1939.
The development of more portable cameras and the foundation of Mothers Against Drunk Drivers (MADD) in the 1980s helped catapult the popularity of in-car cameras among police officers, who would mount their recording systems onto their dashboards or on the passenger seat and record illegal behavior on VHS tapes, since “recordings came to be viewed as the most effective method of providing the necessary evidence to support a conviction”\(^{20}\) in cases of substance-induced impaired driving. Among the earliest pioneers was retired detective Bob Surgenor from Ohio’s Berea Police Department, who, in 1988, was able to capture one of the world’s first police car chases with the help of a camera mount he created himself, which secured the camera to the passenger seat.

In the 1990s, the war on drugs and an exponentially growing number of racial bias and profiling allegations against police officers pushed legislators to require extensive documentation of every traffic stop. Dashcams had officially become a necessary instrument for gathering evidence, disproving false allegations, increasing officers’ safety, and potentially increasing public trust in the police. Solidifying its usefulness, on January 23, 1991, a camera mounted to Nacogdoches County Constable Darrell Lunsford’s patrol car captured his own brutal murder. The 47-year-old officer turned his camera on just before approaching a suspect car he had stopped near Garrison, Texas, and ended up being beaten and stabbed to death by three men. The tape, which is considered to be the first time a camera captured an officer’s death in the line of duty, not only helped in the identification and arrest of the suspects but also became a teaching tool for police departments to this day.\(^{21}\)


However, this technology was not cheap, and many departments struggled to fit such expenditure in their budgets, which led the Office of Community Oriented Policing Services (COPS Office) – a sector of the United States Department of Justice – to launch the In-Car Camera Initiative Program. In 2000, the program started delivering funds to agencies throughout the country, and by 2007 “sixty-one percent of local police departments used video cameras in patrol cars.”

Dashcams and CCTV systems have been undoubtedly important tools to law enforcement over the years, but recent events have intensified public scrutiny of police officers, adding more tension to what has often been a volatile relationship. Two noteworthy instances of this were the deaths of Eric Gardner and Michael Brown—two entirely unrelated cases which motivated departments all over the United States to employ body-worn cameras, more commonly known as bodycams or BWCs, in an attempt to restore confidence and trust in police officers. These portable and wearable video and audio recording devices seemed to be the next logical step since the vast majority of the public have access to smartphones and live streams. According to Scott Greenwood of the American Civil Liberties Union (ACLU):

> The average interaction between an officer and a citizen in an urban area is already recorded in multiple ways. The citizen may record it on his phone. If there is some conflict happening, one or more witnesses may record it. Often there are fixed security cameras nearby that capture the interaction. So the thing that makes the most sense—if you really want accountability both for your officers and for the people they interact with—is to also have video from the officer’s perspective.

In other words, BWCs can be used by law enforcement to build transparency, trust, and accountability by documenting interactions between the public and officers, as they are able to capture unprofessional or illegal behaviors by both parties.

---

However, are BWCs really effective? In 2012, a study took place in the Rialto Police Department, California, where police officers were randomly assigned BWCs based on their shifts. A year later, the results showed a decrease in use-of-force incidents and a meaningful reduction in the numbers of complaints filed by civilians against officers when compared to the previous year.\footnote{The Rialto Police Department’s Body-Worn Video Camera Experiment: Operation ‘Candid Camera,’” April 29, 2013, ccjs.umd.edu/sites/ccjs.umd.edu/files/Wearable_Cameras_Capitol_Hill_Final_Presentation_Jerry_Lee_Symposium_2013.pdf.} Needless to say, this study had great impact on the sales of BWCs and has been used as an inspiration to other pilot programs, including the one implemented in the New York City Police Department.\footnote{Amanda Ripley and Timothy Williams, “Body Cameras Have Little Effect on Police Behavior, Study Says,” The New York Times, January 20, 2018, sec. U.S., www.nytimes.com/2017/10/20/us/police-body-camera-study.html.}

Several other studies followed Rialto’s, and the results have not been consistent. In October 2017, the Lab @ DC, a team of scientists in Mayor Muriel Bowser's administration,\footnote{The Lab @ DC, The Lab @ DC, accessed May 5, 2018, thelab.dc.gov/.} released the results of a seven-month study, where “just over a thousand Washington, D.C., police officers were randomly assigned cameras — and another thousand were not.”\footnote{Amanda Ripley, “A Big Test of Police Body Cameras Defies Expectations,” The New York Times, November 9, 2017, sec. The Upshot, www.nytimes.com/2017/10/20/upshot/a-big-test-of-police-body-cameras-defies-expectations.html.} The study, which was done with a partnership with the Metropolitan Police Department (MPD) and focused on the “documented use of force, civilian complaints, officer discretion (as measured by arrests for disorderly conduct), whether a case was prosecuted, and case disposition,”\footnote{“About the Results,” Randomized Controlled Trial of the Metropolitan Police Department Body-Worn Camera Program, accessed May 5, 2018, bwc.thelab.dc.gov/results.html.} showed that there was no significant difference between the interactions with the public carried by the officers equipped with BWCs and those who were not.

If matters were not confusing enough already, another study, conducted by Cambridge University in 2016, suggested the use of BWCs can increase the rates of assault against police by...
members of the public. After averaging the results of ten trials administered in police departments both in the United Kingdom and the United States, Ariel et al., state that when officers did not inform the public they were being recorded by a BWC and when the cameras were only activated after a situation escalated, incidents involving the use of force increased.29 Although both scientists and officers involved were surprised with these results, Ariel et al. argue that this study shows the importance of improving BWC policies around the world: “Cameras should remain on throughout the entire shift—that is, during each and every interaction with citizens—and should be prefaced by a verbal reminder that the camera is present.”30 Activation policies will be discussed in more depth in “Chapter 1: Recording the Video.”

Studies aside, police officers cannot deny the cameras, if anything, have a definite effect on them: “You gotta remain professional, because, God knows who’s going to watch [the BWC video]. A lawyer, my boss, it might end up on Facebook one day, and I don’t want to look like a savage.”31

Although some similarities can be drawn between this tool and other forms of police video surveillance, BWCs are fundamentally different from CCTV systems and dashcams. Since bodycams are attached to the uniform, they are able to move with the officer, capturing what he or she sees, unlike dashcams and CCTV, which tend to be mostly stationary and only able to provide limited camera angles. If a BWC is operating properly, it is able to record both video and audio, providing what many consider an indisputable account of events.

BWCs are also unique in the sense that they solely produce digital-born media. While in the past, officers had to manage film prints and videotapes, BWC generated video files and

30 Ibid.
31 Interview with Officer A, interview by Caroline Oliveira, Phone, April 6, 2018.
accompanying metadata require a certain amount of storage many departments are not able to afford.

In 2015, the Major Cities Chiefs and Major County Sheriffs, in a partnership with the U.S. Department of Homeland Security’s Office of Emergency Communications (OEC), sent a survey to 67 major cities and 76 major counties in the United States, with “the purpose of gathering information on the technological and interoperability challenges involved in implementing BWC programs.”

Seventy law enforcement agencies completed the research, and the results showed:

- About 19% said that their BWC programs were “fully operational.”
- Nearly 77% either “intend to implement,” were in the piloting phase, or have completed the pilot but have not yet started a program.
- The data indicated that many local agencies are moving forward with implementation, despite of a lack of IT infrastructure and technical solutions to fully support these programs.
- Only 5% of respondents said they either did not intend to implement a BWC program, or had completed a pilot but chose not to proceed.

A year later, another study showed that 95% of police departments in the United States had already or had the intention to implement a BWC program.

There is no doubt video-recording technology has advanced over the years, and police departments all over the world have been using it to increase public safety, solve crimes, and as training tools. In fact, technology has progressed so much that police departments everywhere have to continually make decisions related to acquiring and implementing new systems, such as:

- Automated license plate readers,
- Gunshot detection systems,
- Facial recognition software,
- Predictive analytics systems,
- Communications systems that bring data to officers’ laptops.

---

33. Ibid.
or handheld devices, GPS applications, and social media to investigate crimes and communicate with the public.\textsuperscript{35}

However, swift employment of such progresses can lead to underwhelming or even controversial effects if it is not accompanied by the proper policies and legislations.

Body-worn cameras are considered an important tool in increasing transparency and bettering public trust in law enforcement agencies, but an analysis of current policies reveals there are still many questions regarding privacy, video preservation, and access that still need to be answered in order to make the best use of these technologies.

Chapter 1: Recording the Video

The choice of body-worn camera technology adopted is one of the most defining factors when developing a framework of procedures officers need to follow during their shifts. Currently, there are over 60 BWC models especially designed for law enforcement available in the market, and their features vary greatly. Some of the factors that can influence a department’s decision of which camera system better meets its needs include battery life length, event marking, weight, camera placement, camera size, quality of video, vision type, field of view, playback capacity, charge time, pre-event recording or buffering, video and audio format, video safeguards, upload capability, and cost.\(^{36}\)

**Event Marking and Metadata**

At the most basic level, BWCs employed by a police department (PD) should be able to record time and date. Some models are able to produce screenshots of recorded video for easier retrieval and playback. Officer A, who was interviewed for this dissertation, also emphasizes the importance of tagging the video with case numbers for identification purposes.\(^{37}\)

**Pre-Event Recording or Buffering**

The pre-event recording or buffering feature allows officers to capture from 30 seconds to up to two minutes of footage before the “record” button is activated.\(^{38}\) This way, a pre-event

---


\(^{37}\) Interview with Officer A, interview by Caroline Oliveira, Phone, April 6, 2018.

recording is created in a memory buffer. Basically, this means the camera is always recording the same loop over and over in the same small sector of its memory. When a recording is triggered, it also captures the buffer in the file. For a BWC, this pre-event recording might actually be an attack on the officer, which could be critical in justifying an officer using force on a subject. Axon (formerly known as Taser International) BWCs, for instance, have a buffering mode that allows 30 seconds preceding a recorded event (or as Axon explains, the Event mode is activated) to be captured. This happens because the cameras are recording all the time, but not saving data to their permanent memory. These 30 seconds of pre-event recording are video only, and buffering mode only works if the camera is switched on.

WatchGuard has developed an in-car and BWC system, which allows the camera to capture an event even if the officer does not activate the record button. The system, entitled Record-After-the-Fact (RATF) provides the ability to retrieve video that was not officially recorded, days after the event took place. This is made possible because the 4RE in-car system and VISTA body-worn cameras can be configured to convert buffering background video into recorded video. The technology works by having the cameras constantly recording video, but unlike the regular pre-event recording, it actually writes data into the memory. As long as the data is not overwritten, WatchGuard’s software can retrieve it.

Although pre-event recording seems to be beneficial to officers, it also raises certain issues. One of the main problems this feature causes is the reduction of battery life. According to a Colorado-based law enforcement agency, the pre-event recording function cuts the camera’s battery life to less than 25% of what is advertised, and as often as every two hours, officers have

to charge the BWC for use. Other implications related to this feature will be further discussed in “Chapter 3: Privacy and the Camera.”

**Battery Life Length and Charge time**

According to a market survey published in 2016 by the U.S. Department of Justice, where an overview of 66 BWC technologies available and four data collection systems was presented, the standby battery lifetimes of the analyzed cameras “ranged from [eight] hours to 216 hours, while recording battery lifetimes ranged from 2.5 to 23 hours.” As mentioned previously, pre-event recording and even department policies related to camera activation affect battery life.

**Weight**

The weight of the BWC can be an important factor when a department is deciding on a brand and a model. The weight can range from 0.53 ounces, like the Taser Axon Flex (camera alone, not counting its controller) to about eight ounces, like Law System’s Witness BWC, and it affects where the camera can be safely mounted while remaining comfortable to the officers. Weight is also directly related to the battery life of a BWC: lighter cameras, shorter battery life.

---

Camera placement

The placement of the cameras varies depending on their models. Common mounting places include lanyard, duty belt, glasses, epaulet, chest, bike handlebar, helmet, in-car dashboard, shirt or jacket, helmet, lapel, pocket, bicycle, motorcycle, shoulder, head, hat, kickfast adaptor, and specific mounts.

Most cameras are sold with mounting systems that allow officers to attach and detach a BWC to and from various places. Mounting itself is a critical issue departments have to consider when selecting a camera since camera placement can greatly impact how the video is recorded. Although chest placement is the most preferred among law enforcement agencies, head and sunglasses have also been popular, especially since these options allows cameras to capture images that are closer to the officer’s point of view. However, such placement also has its disadvantages. Aside from producing discomfort, cameras that are placed on the officer’s head raise safety concerns since a suspect could potentially attempt to destroy the camera, consequently harming the officer.

Another popular camera placement is mounting the BWC to the officer’s shoulder or uniform. Although this placement is able to provide a good perspective, the camera can be easily blocked by certain gestures: “One agency, for example, lost valuable footage of an active shooter incident because the officer’s firearm knocked the camera from his shoulder.”

---

46 Michael D. White, “Police Officer Body-Worn Cameras - Assessing the Evidence” (OJP Diagnostic Center, 2014).
Regardless of camera placement, no BWC currently available in the market will “capture 100% of the action.”

Quality of Video

Video quality has improved greatly over the years. Currently, the video resolution found in BWCs range from 576 pixels to 5MP (2560 pixels by 1920 pixels) and the frame rate varies from 25 to 60 fps (frames per second). Although higher quality and higher frame rate are desired by all departments, these aspects require larger storage capacity and bandwidth, which can become costly especially if the police department has a long video retention policy:

At [video graphics array] (VGA) resolution (640x480) and a frame rate of 30 frames per second, an hour of video recording would take approximately 550-1,100 MB of storage. High definition (HD) resolution, also called 720P, is 1280x720; an hour of recording would take approximately 1,650-3,325 MB of storage.

Frame rate also has an impact on the size of the video files. A higher frame rate of 60 fps, for example, will result in more frames, causing the video file to be larger. Consequently, this aspect of video recording has a direct impact on storage. If a system has a large storage capacity and bandwidth, and one needs to record extremely clear video with fast motion, increasing the frame rate may be an option.

Vision Type (day or day/night)

---

Vision type can also be indicated by the LUX rating, which refers to “a camera’s ability to see in various degrees of darkness.”\textsuperscript{51} Although it might seem logical for a department to choose a camera with lower LUX rating – stronger performance in low light situations – if deciding to forgo the option of night vision, some surveillance experts warn agencies to exert caution. Aside from not following measuring standards (numbers are established by each camera manufacturer), extremely low LUX ratings produce practically useless noisy images.\textsuperscript{52}

**Field of View**

Field of view (FOV) refers to how much information the camera lens is able to fit in a frame, or “simply what [the] lens together with the camera can see and capture from left to right, to top to bottom.”\textsuperscript{53} Consequently, it is essential to consider this aspect because:

For a given resolution, a larger FOV will encompass more objects but in less detail, while a smaller FOV will include [fewer] objects, but in greater detail. Furthermore, certain types of lenses (e.g., fisheye) used to increase FOV may result in some distortion, especially near the edges of the video. Such distortion may complicate efforts to determine distances and may pose a challenge for analytics software.\textsuperscript{54}

**Playback Capacity**

Certain BWC models have small LCD displays, which allow officers to review a recording while on duty. Other models, which do not have a display, offer the option of connecting the camera to the officer’s smartphone through an application. Axon, for instance,
offers Axon View, which is compatible with Android and Apple devices and allows instant video playback and GPS tagging.55

**Video and audio format**

BWCs should “support a non-proprietary, standards-based video format [since] investigations [could] be hampered and slowed by the need to convert the footage to a standard format, which [could] also impact the actual video detail.”56

Not all cameras available in the market capture audio, and sometimes the “placement of the microphones on the BWC may impact the quality of the recording, especially for head or shoulder-mounted systems.”57 Some camera systems allow the audio function to be turned off without affecting video capture, and this feature, in particular, has been mentioned in the media several times, but not for any positive reasons.

In March 2018, officers from the Sacramento Police Department fatally shot Stephon Clark after mistaking his white iPhone for a gun.58 Once the BWC videos were released to the public, the case gained national attention and fueled concerns regarding Sacramento PD’s lack of transparency, since the video shows a police sergeant instructing the officers to mute their

---

cameras. After the sergeant “is heard saying, ‘Hey, mute,’ (...) the audio of both of the officers standing with him [goes] silent, [but the] video shows they remained at the scene.”

Although BWCs are considered first and foremost a visual medium, audio capture and preservation should not be overlooked.

Video Safeguards

For obvious reasons, BWC videos need to be protected against unlawful use, unauthorized access, and cyber attacks. Safeguards need to be put in place to protect all BWC videos, not just the ones with evidentiary value since almost every recording:

Is likely to also contain information that while not crucial to an investigation could still be considered sensitive in nature. If any of the recorded information is accessed by an unauthorized third party then this could not only compromise a police investigation but also cause considerable intrusion into a person’s privacy at a time of vulnerability. An obvious form of intrusion that could cause considerable harm is the unintentional identification of a person.

Encryption, “a mathematical function using a secret value — the key — which encodes data so that only users with access to that key can read the information,” is a valuable tool for data protection, but far from being the only one. In fact, encryption is only effective “if access codes and authentication systems are correctly managed” and if it is being used in conjunction with appropriate camera activation, storage, and access policies.

---

The PD should also make sure its chosen camera has some sort of tamper resistance in order to prevent videos from being edited, overwritten, or deleted before being transferred to a storage system:

Systems that can export a hash value of files being transferred may provide an enhanced capability to demonstrate tamper resistance. Standard encryption such as AES can be employed to protect data and improve the management of lost devices and memory cards.63

**Upload Capability**

BWC systems can connect to a data management and storage system by cable connection, wirelessly, and docking station. Docking stations tend to be a popular choice since they are able to upload video files and data to the chosen storage system and, at the same time, charge the cameras.64

**Cost**

According to the U.S. Department of Justice market, costs for the cameras vary greatly from $2,000 to $199.65 However, BWC costs are not so clean cut. In fact, Axon conducted a year-long free trial of some of their equipment, including one Axon Body 2 per officer, year-long license to Evidence.com Unlimited Pro, two mounts for the BWC, docks for the station, deployment support, and access to their e-learning system, Axon Academy.66 However, many experts believe the true costs related to this technology lie in storage, which will be explored in “Chapter 2: Preserving the Video.”

---

To Record or Not to Record?

Although PDs have to consider financial limitations, certain design features are considered critical to law enforcement, according to a market survey conducted by DOJ’s National Institutes of Justice. They include “durability (despite a heavier weight), resilience of the docking station, strong mounting clip (for fear of BWCs falling off), and video retrieval.”67

As of this date, there are no federal laws dictating how the police in the United States of America should use BWCs. In fact, although the Bureau of Justice Assistance (BJA) – part of the Department of Justice’s Office of Justice Programs (OJP) – has provided over $41 million in grants from 2014 to 2016 alone to the Body-Worn Camera Policy and Implementation Program,68 the federal government is still hesitant to deploy this technology in its own law enforcement agencies. Since federal laws of operation always prevail over local laws, federal agencies are currently not allowed to engage in joint task force operations with local police departments in which body cameras are utilized.69 On March of 2017, U.S. Congressman Adriano Espaillat introduced the ICE and CBP Body Camera Accountability Act, which would require U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) officers to wear BWCs when on duty.70

The lack of federal laws causes policies to vary greatly from department to department, with some agencies having more detailed and effective protocols than others. The Leadership

---

Conference on Civil and Human Right and Upturn – a nonprofit organization which focuses on research and analysis of topics related to technology and social justice – created a policy scorecard to examine BWC related policies. When it was first released, the scorecard examined 25 police departments (PD) in the U.S., but in November of 2017, it expanded to 75 agencies, including all major cities where BWCs are in use or about to be in use, departments that have received more than $500,000 in grants from the DOJ, cities that have received national attention, such as Baton Rouge (LA) and Ferguson (MO), and Parker (CO) due to their propitious policies.71

Among the eight criteria used to evaluate PDs, the report sheds light on the lack of concrete policies that address privacy concerns. Of all the departments analyzed, only 18 have specific policies regarding when the BWC should not be recording. These include:

- During sensitive situations (bathroom, shower, lockers, etc.)
- To protect vulnerable individuals (sex crime victims, child abuse victims, domestic violence victims) if they wish to not be recorded.
- During strip searches.
- Recording without victims’ and witnesses’ knowledge and/or consent. In most policies, officers are encouraged but not required to inform the general public a BWC is recording.
- Inside medical facilities.
- In certain policies, such as the ones found in place at Baltimore County, officers are allowed to determine when the camera should be or should not be recording, especially during “situations where a heightened expectation of privacy exists.”72

---

72 James W. Johnson, “Addendum to Special Order #2016-03” (Baltimore County Police Department, January 9, 2017), resources.baltimorecountymd.gov/Documents/Police/2017pdfs/bwcspecialorder.pdf.
• Unless there is a crime happening, individuals in private areas (i.e., private homes) should not be recorded without a warrant. (Chicago)

• During interactions with juvenile victims or witnesses, if a parent or legal guardian refuses to have the child recorded. (Cleveland)

• If someone, who is wishing to help with the investigation or report a crime, requests anonymity, the BWC might be switched off, as long as the safety of the officer and others are not being threatened. (Denver)

• Cameras can be switched to buffering mode during private conversations with an officer, paramedics, doctors, etc. or if the information to be conveyed is not part of the investigation. (Denver)

• Denver PD also requires officers to activate the camera audible alert signal, which lets the public know they are being recorded. Officers are able, however, to turn the mute button on during tactical situations.

• Las Vegas PD requires officers to obtain explicit permission from victims and witnesses before they are recorded.

• According to Montgomery County PD policies, officers are required to inform individuals when they are being recorded, except when exempt by law. They do not determine what laws.

Aside from these specific policies from the 18 police departments that address personal privacy concerns, the great majority of other departments on the scorecard only mention the importance of this issue, but do not establish when the BWC should be recording and when it should not. More interestingly, Fort Worth, Los Angeles County, Pittsburg, and Portland PDs do not address privacy issues at all.
The report also analyzes if the studied departments contain policies regarding officer discretion. Forty-two departments in the scorecard mention specific situations where cameras needs to be recording, and require any officer to justify and document any time he or she fails to record or interrupts the recording of a required event. Chicago PD lists several scenarios where the camera needs to be activated, and they include:

- Calls for service
- Investigatory stops
- Traffic stops
- Arrests
- Foot and vehicle pursuits
- Use of force incidents
- Seizure of evidence
- Interrogations
- Searches, including searches of people, items, vehicles, building, and places
- Statements made by individuals in the course of an investigation
- Any other instance when enforcing the law.

Columbus PD has a similar list of specific contacts that need to be recorded and in some departments such as Albuquerque PD officers are investigated if they repeatedly and intentionally stop or fail to record required events. However, having such policies written does not guarantee they are being implemented. Albuquerque PD, for example, is among the 42 departments that have policies detailing when officers should have their cameras recording. In fact, they have a list of required events similarly to Chicago PD’s, but there is no mention of

---

punitive actions towards officers who intentionally fail to record an event. In a city where the rate of fatal shootings involving the police is eight times that of New York City, officers face no consequences. In an interview, American Civil Liberties Union (ACLU) legal director of the New Mexico branch, Alexandra Smith, notes:

There have been police shootings where the cameras simply [were not] turned on. There was one case—Christopher Torres—where police shot an unarmed man in the back, in his backyard, while he was in his pajamas. In that case, they simply [did not] turn the footage in. And that was just valid and acceptable to them. And there was the case of Mary Hawkes, a 19-year-old unarmed girl who was shot in back by a police officer, who didn’t turn on the camera in that case.

And there are many, many cases like this, where the cameras simply weren’t turned on, or the officers said they weren’t turned on, or the footage wasn’t turned in. But of course in criminal cases, when the footage is good for them, they’ll use that footage (...) Just having the cameras isn’t enough: policies need to be enforced. If officers actually knew they were going to face strict sanctions for not using their cameras, I think it would be a very different picture. Right now in Albuquerque they face [no] consequences for it.\(^{75}\)

There are many other reasons why officers do not activate their BWCs, and they are not always a conscious decision. It is not unusual for situations to escalate without any warning, and for instance, if a regular encounter with a civilian turns into an on-foot pursuit, the officer might not have time to turn the recording mode on. Lack of intensive training and confusing policies are the main culprits for recording failures, and this is not something that only occurs in Albuquerque. In fact, in 2017 an ABC affiliate, local television station KSTP, uncovered that “Minneapolis police officers with body cameras recorded less than 20 minutes of footage for every eight-hour shift – or a total of five or six hours of footage a month.”\(^{76}\)


Several organizations created policy models in an attempt to help PDs draft their own set of guidelines. The ACLU Model Act for Regulating the Use of Wearable Body Cameras by Law Enforcement, which states on section 1(b):

Both the video and audio recording function of the body camera shall be activated whenever a law enforcement officer is responding to a call for service or at the initiation of any other law enforcement or investigative encounter between a law enforcement officer and a member of the public, except that when an immediate threat to the officer’s life or safety makes activating the camera impossible or dangerous, the officer shall activate the camera at the first reasonable opportunity to do so.77

In comparison, the International Association of Chiefs of Police (IACP) Body Worn Cameras Model Policy states “officers shall activate the BWC to record all contacts with citizens in the performance of official duties.”78 The joint Police Executive Research Forum (PERF) and U.S. Department of Justice Office of Community Oriented Policing Services (COPS) publication “Implementing a Body-Worn Camera Program” establishes that:

[As] a general recording policy, officers should be required to activate their body-worn cameras when responding to all calls for service and during all law enforcement-related encounters and activities that occur while the officer is on duty.79

Some might argue that the best way to avoid confusion around when the camera should and should not be on would be to have it on during an officer’s entire shift, especially since certain cameras can record for up to 12 hours. However, this suggestion would never be practical. Police officers also have the right to privacy and should be able to engage in regular human activities without fearing the footage would be made accessible if requested by the

public. If BWCs were required to stay on during the entirety of a shift, they could potentially capture:

- Private conversations of anyone (civilians and officers) within the BWC’s microphone range.
- Moments when officers are discussing sensitive investigation techniques and tactical operations.
- Victims, witnesses, and suspects inside their private homes, which is a problem if the officers do not have a warrant.
- Confidential conversations with informants, attorneys, and vulnerable individuals, including victims of domestic abuse, children, and sexual crime victims.
- Officers during their breaks, using the restroom, and having private phone conversations not related to ongoing investigations.80

Capturing these types of footage would not help increase transparency and improve the relationship and trust between the public and law enforcement. Furthermore, the amount of useless and even potentially damaging footage would require additional work and effort to be analyzed and eventually discarded. Although this could work in larger and better-funded departments like the New York Police Department (NYPD), such endeavor would not be feasible in smaller ones. It would also intensify ever-growing storage challenges, which will be better discussed in “Chapter 2: Preserving the Video.”

---

Chapter 2: Preserving the Video

One of the most important questions that need to be answered regarding body-worn cameras is: how long should videos be kept? Those who watch police procedural shows or movies have grown accustomed to seeing a homicide detective entering the evidence vault, a warehouse-like facility with aisles and aisles of metal shelves filled with brown cardboard boxes with case numbers written on them. Inside these boxes, the detective finds photographs, old videotapes, cassette tapes, and properly bagged physical evidence, like bloody clothes, a gun, and so on. Everything looks neat and well maintained.

The reality, however, is quite different. Many underfunded departments struggle to keep their vaults operational and most often have to deal with lack of storage space and proper management. In fact, all sorts of evidence, including DNA samples, which revolutionized investigations and crime-solving techniques, arrive at police departments all over the country often in overwhelming quantities, causing lost and destruction of many critical elements. Furthermore, these “vaults,” which are most frequently just basements, are managed by clerks that might not have the proper training, and it is not unusual for evidence to be purged prematurely. In 2003, for example:

The Denver Post examined purges in [ten] states and found that authorities destroyed biological evidence in nearly 6,000 rape and murder cases during the past decade, rendering them virtually unsolvable. Over the past three decades, the loss or destruction of DNA evidence in 28 states has undermined efforts by at least 141 prisoners to prove their innocence.81

Policies determining the retention of evidence vary from state to state, since there are no federal laws governing the issue, and unsurprisingly, policies addressing the retention of BWC

videos also vary from jurisdiction to jurisdiction. In 2016, the Office of the Secretary of State (SOS), a section of the Washington State Archives, re-issued a document in which some guidelines were detailed on how long video evidence should be kept by local law enforcement agencies. According to the report, if the camera captures an incident where unlawful behavior or criminal act is observed, the video should be kept until the matter is resolved or the perpetrator has exhausted his or her appeals.\(^{82}\) The document also states that if no unlawful incidents were recorded, videos, also known as non-evidentiary, should be kept either for 90 days or 60 days\(^{83}\) from the date of its recording and then destroyed. This approach to can be defined as *evidentiary*, since it establishes retention periods according to the evidentiary value of a video.

Another approach that can be used to determine video retentions guidelines is called *instructional*. According to this point of view, BWC videos have an educational value and can, therefore, aid in police training. According to a United Kingdom Home Office guide:

> [A BWC] has been used by Professional Development Units as a training aid for student officers. The ability to review their performance in detail after an incident is a powerful tool for officers to highlight effective and ineffective actions. When reviewing their evidence, experienced officers who have used the equipment have also been able to assess their behavior and can professionalize their performance accordingly.\(^{84}\)

In the U.S., the Miami PD, which has been using BWCs since 2012, has adopted this approach. According to Ian Moffett, chief of Police and District Security for Miami-Dade Schools PD, a

---


BWC video “allows [the] officer to go back, the supervisor to go back, and review it, and determine if something was done wrong.” 85

Another argument in favor of this approach is that BWC videos can be used as an officer performance review tool, especially “during investigations of critical incidents, such as use of force.” 86 Police officers constantly find themselves in situations where they are asked to act fast, without much time to rationalize and carefully plan out a course of action. BWC videos allow a supervisor to analyze an event in slow motion, literally frame by frame, and help determine if an officer acted in compliance with his or her training. Although more studies are yet to be made to definitely indicate the effectiveness of this instructional approach, Officer C believes BWCs act as an independent witness, and can help “disprove the many demeanor and internal affairs complaints.” 87

In reality, the number of days a video should be kept for varies greatly, and the retention policy is typically dictated by state evidentiary laws and regulations. While some jurisdictions follow SOS suggestions, other departments believe videos should be kept longer, others believe they should be kept for a shorter period of time. Based on the information collected by Upturn and the LCCHR, out of the 75 law enforcement agencies surveyed, only eleven had clear and concise footage retention policies, determining how long videos should be kept and reinforcing deletion of the files after that period has expired. Charlotte-Mecklenburg, for instance, has footage not related to any criminal charges or investigation deleted after 45 days:

The BWC system automatically deletes recordings from the server when the retention period for the categorized recording has elapsed. The retention period is set by the system

87 Interview with Officer C, interview by Caroline Oliveira, email, April 2018.
according to specific categories assigned to the video by the officer, supervisor or authorized user.88

Similarly to other departments where clearer policies on footage retention are in place, videos related to criminal incidents, such as homicide and other felonies, are to be kept for years, in case of Charlotte-Mecklenburg PD, 20 years.

In order for these systems to work, officers are required to input the proper metadata before the video gets transferred to their final storage system. Officer A explains that it is an important part of an officer’s workflow to assign a case number and a category to each BWC video captured.89

On the other hand, there are departments where not only there is no explicit retention policy, but deletion of BWC is not reinforced. Oakland, California, PD, for instance, is said to retain video files for a minimum of two years and has no deletion requirement.90 In addition, if a BWC video becomes evidence in an ongoing investigation or court case, it might be kept for an even longer period of time. There is also a not-often-voiced paranoia that seems to accompany any type of evidentiary law, including the previously mentioned DNA evidence. What happens if a video becomes evidence in an appeal many years, if not decades, in the future? It is not uncommon for DNA evidence to exonerate individuals after years of being in prison, or even years after their execution. Could the same be the case with BWC videos? Many could agree with Shirley Clemons, whose fiancé, Willie Grimes, was unable to appeal his rape conviction

88 “Interactive Directives Guide - Body Worn Camera (BWC)” (Charlotte-Mecklenburg Police Department, April 29, 2015).
89 Interview with Officer A, interview by Caroline Oliveira, Phone, April 6, 2018.
due to evidence destruction by a court clerk: “It’s like that, I guess. One man’s garbage could be another man’s salvation.”

However keeping all video files and related metadata indefinitely might be unrealistic. Storage and data management are considered to be two of the biggest challenges involving BWCs, and although many BWC vendors offer cloud services, such as Axon’s Evidence.com, which also facilitates data management and file sharing, the amount of data can be cumbersome to PDs, especially smaller-sized ones:

When the Chula Vista, Calif., Police Department started giving body worn cameras to a handful of police officers, they quickly learned that a 30-minute video took about 800 MB of storage space. The department crunched the numbers and realized that if it equipped every one of its 200 sworn officers with cameras, they could potentially generate 33 terabytes of data every year.

Since audio-visual technology keeps evolving constantly, cameras are becoming increasingly less costly. Consequently, agencies are aiming to acquire those with better video resolution and higher frame rates, both of which also increase the file size. The metadata associated with each video file also needs proper storage space, since it is vital for establishing the chain of custody and for auditing processes. When Police Executive Research Forum (PERF) interviewed 40 PDs to write “Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned,” it learned that the majority of agencies used either “an in-house server (managed internally) or an online cloud database (managed by a third-party vendor)” to store BWC videos. Regardless of the chosen system, PERF recommends that the PD:

---

- Consult with prosecutors and legal advisors: Police departments can get assistance from experts to make sure the employed storage system is compliant with evidence retention laws.

- Explicitly prohibit data tampering, editing, and copying: BWC footage needs to be kept unadulterated, unless redaction has been authorized and deemed necessary before a video is made available to the public.

- Include protections against tampering with the data prior to downloading: Especially in departments where officers are allowed to watch the footage before filing reports, it is essential to implement safeguards that protect videos from being altered and deleted.

- Implement an auditing system: Although some BWC storage systems already come with a built-in audit trail, providing an auditing system is still not considered a requirement. It is of immense importance for a PD to implement such system in order to document who is accessing the footage, when, and why.

- Explicitly determine who will be authorized to access the data: In most cases, supervisors are able to access BWC footage. According to many policy books, officers are able to also re-watch captured footage before filling out reports of incidents. This aspect will be addressed in more depth on the “Access” chapter of this dissertation.

- Ensure there is a reliable backup system: BWC data needs to be backed up to avoid accidental deletions, which could hinder criminal investigations and destroy evidence.

- Determine who will be responsible for downloading videos from the camera to the storage system and when: In most departments, officers are responsible for connecting the camera to a docking station or to a computer, and transferring the footage to the storage system. According to Officer A, for example, after the video gets transferred to
the storage system, officers are unable to re-watch them.\textsuperscript{94} PERF also recommends PDs determine who should be responsible for this process in case an officer is involved in a shooting or another serious incident.

- Consider third-party vendors carefully: Since many PDs do not have designated personnel to manage their storage system, it is common for law enforcement agencies to employ the services of third-party vendors. Not all vendors are the same and not all are compliant to FBI’s security guidelines, so agencies must make sure they offer safeguards, backup, audit trail, etc.\textsuperscript{95}

Unsurprisingly, storage costs are weighing heavily in certain departments. In 2012, Clarksville, Indiana, equipped its 50 full-time officers and 25 reservists with BWCs, just to have the implementation program suspended months later, after Indiana passed a new evidence retention law requiring videos to be stored for at least 190 days. In an interview with Aljazeera, Chief Mark Palmer said:

His department's video storage and camera maintenance costs had been between $5,000 and $10,000 a year under its 30-day video storage policy. But the new law that took effect July 1 would have raised those costs to $50,000 to $100,000 for the first year, he said, by requiring videos to be stored more than six times longer. Palmer said the department would have had to buy new servers and may have had to buy new cameras and software and to train someone to use it, and that although the cost would have been lower in subsequent years, it still would have been high.\textsuperscript{96}

Video retention laws are most likely to keep evolving so many agencies are opting for cloud storage. Although many cloud data management services have yet to meet FBI’s Criminal

\textsuperscript{94} Interview with Officer A, interview by Caroline Oliveira, Phone, April 6, 2018.
Justice Information Services (CJIS) certification standards, many PDs are going with Evidence.com or VIEVU’s VERIPATROL and Solution, both which maintain they are safe, secure and CJIS compliant. However, FBI’s CJIS is not the only standard a cloud service storing BWC videos should be compliant with. In situations where a video is related to an investigation on child abuse, for example:

Standards such as IRS 1075 Encryption Requirements, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Risk and Authorization Management Program (FedRAMP), and others may also come into play. A cloud service provider should be able to confirm compliance with all necessary standards, including the ability to keep up with changes to these requirements, and be willing to attest to this in writing.

Currently, there is no concrete information on Axon’s, VIEVU’s, or Azure’s websites about working with any other standards aside from CJIS.

Evidence.com is Axon’s cloud-based system that is able to store “all [police] data — from body-worn cameras to audio records — while streamlining data management and sharing.” According to its website, this system allows video and audio files to be uploaded automatically from hardware, both Axon devices and hard drives, facilitates file-share, by creating secure links and by granting access to approved personnel. Evidence.com can also be integrated to the department’s Computer-Aided Dispatch (CAD) and Records Management System (RMS), which allows files to be tagged with the proper metadata. Axon states this feature:

- Improves Accuracy

---


- Automatically adds Incident ID, Category, Location and other tags to videos
- Avoids the misspellings and incomplete information of manual entry
- Makes it easier to search and retrieve Axon videos later

- Save Time
  - Frees officers from manual video tagging
  - Requires minimal involvement from agency IT staff
  - No need to involve CAD or RMS providers.¹⁰⁰

Axon offers two types of Evidence.com plans – basic and pro – and two different bundle options. Each plan varies in price and types of services offered:

Figure 3. Axon’s Plans and Pricing. From axon.cdn.prismic.io/axon%2F1d7bf35d-31cf-4817-999b-e55e72cc1e11_02072018+-+product+card+-+us+axon+plans.pdf

<table>
<thead>
<tr>
<th>PLANS</th>
<th>BASIC</th>
<th>PRO</th>
<th>UNLIMITED</th>
<th>OFFICER SAFETY PLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCLUDED STORAGE</td>
<td>10GB</td>
<td>30GB</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Evidence Sync</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dock-Automated Video Upload</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure File Storage</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Axon Capture App &amp; Axon View Apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GPS Mapping of Captured Media</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File &amp; Case Sharing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Video Clips &amp; Markers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Custom User Roles &amp; Categories</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automatic File Deletion Schedules</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bulk Reassign, Share, Edit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Single Sign-On (SSO)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Video Redaction</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Group Monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agency Usage Reports</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Device Analytics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Axon Device Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Human Paid Transcription</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Multicam Playback</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restricted Evidence</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Axon Citizen 1:1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Standard Redaction Studio</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Two Axon Camera Upgrades</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Full Axon Camera Warranty</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unlimited HD Storage*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>One Smart Weapon*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Full Smart Weapon Warranty</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Axon Signal Sidearm</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**ENTERPRISE ADD-ONS**

- **Advanced User Management** [+$10/user/month]
  - Bulk user account creation and management via API

- **CAD/RMS Integration** [+$15/user/month]
  - API and Development Support for 3rd Party Systems [+$10/user/month]
  - Automated user account creation and management from Active Directory (SCIM)

Figure 4. Axon’s Plans Details. From //axon.cdn.prismic.io/axon%2F1d7bf35d-31cf-4817-999b-e55cc722c1c11_02072018+-+product+card+-+us+axon+plans.pdf
A small asterisk at the bottom of the page states discount prices will expire on December 31st, 2018, but there is no information on how much these numbers will change.

Some experts believe that Axon is aiming to establish an empire similar to Apple’s by creating an ecosystem of hardware and software co-dependency:

Once police have bought the hardware, they'll be reliant on Taser to manage and store the terabytes of daily video streaming back from officers. Storing and managing that video requires a monthly fee, which gets higher as you share it across more departments, or purchase features like redaction and simplified editing tools.

According to Sydney Siegmeth, an Axon spokesperson, video is uploaded to Evidence.com every 1.6 seconds, equaling 2.1 petabytes (one petabyte equals a million gigabytes) and “in the third quarter of 2015, [Axon] saw $36.9 million in storage sales, up from just $5.9 million in the first quarter of 2014.” This number will keep growing exponentially since more storage demands will keep increasing and prices will keep going higher. Recently, Axon has migrated 20 petabytes of data to Microsoft Azure in what the company billed as one of the largest cloud migrations.

VIEVU’s Solution is also a Microsoft Azure government-based cloud system. Similarly to Evidence.com, Solution also allows the user to “easily manage and analyze video and case file evidence, add metadata and securely share with users or non-system users” and videos can be uploaded from smartphones or computers. It has Pro and Premium plans, with storage space varying from 50GB, 200GB, to unlimited. Their thirty dollars plan only allows videos to be kept

---

for up to 370 days and CAD/RMS Integration only comes with the more expensive unlimited plans.

VIEVU also has an on-site storage option called VERIPATROL, which allows law enforcement agencies to control their own video storage systems. This system also "includes several layers of security to keep (...) data secure and utilizes a FIPS 140-2 compliant Digital Signature process to prove that video has not been altered."¹⁰⁶ Unlike VIEVU’s Solution, VERIPATROL only has a one-license fee per camera of $300. This system is required if the PD uses LE5 LITE BWCs.¹⁰⁷ Finally, this company also has a hybrid option, which combines on-site video and cloud-based storage. There is no price information on this option on VIEVU’s website.

Cloud-based storage, although it has many advantages, is still something some people do not trust fully. After all, BWC data does not need only to be stored, it needs to be secured. As mentioned previously, not all cloud-based storage systems are CJIS compliant, but “since the videos could contain highly sensitive information, law enforcement agencies need to ensure that the data [is not] hacked, intentionally or unintentionally.”¹⁰⁸ Although Microsoft Azure Government has implemented several new security measures in early 2018,¹⁰⁹ Microsoft Azure has a commercial-facing cloud and that could give hackers so insight on how to hack the system. Cybercriminals have done it before. In 2016, Eastern Europeans hackers attacked several U.S. law enforcement agencies, hospitals, and even schools with ransomware, a virus that “seize

control of a computer system's files and encrypt them.” Agencies were then forced to pay in Bitcoins in order to get a decryption key that would unlock the system and allow files to be retrieved. Although some of the attacked agencies were easier targets for running ancient computer systems, the damage was done:

In Maine, cybercriminals took over the computer system shared by five police agencies for about two weeks last year until the departments paid the crooks $300. In Los Angeles, a large hospital shelled out $17,000 this year to regain access to its electronic medical records that criminal hackers took hostage. And in eastern Ohio, Columbiana County was forced to pay more than $2,800 in ransom in June after computers in its juvenile court system became infected.

There are no guarantees a service such as Microsoft Azure Government will not be able to protect sensitive data, but not every police department will be able to afford or keep affording a secure system such as this, especially since storage demands will continue to increase. That is another reason why implementing specific retention policies should be one of the priorities for PDs with BWCs. Knowing what videos can be deleted after a certain time would save storage space and ultimately cut costs.

It is also important to make sure these videos are not erased before their deletion date. Just like many other storage systems, human error can cause irreversible damage. In 2014, one-quarter of all BWC footage from the Oakland, California, PD was accidentally deleted when an IT employee accidentally unchecked an option to preserve videos during a software update. A similar case happened in Seattle in 2016, when over 2,000 dashcam videos were deleted. In both cases, backup storage was not being implemented at the time. Problems like this can not

only impact an ongoing investigation (due to potential evidence loss or impeding an officer from being investigated through footage captured by his or her BWC) but also might raise issues regarding trust in law enforcement, something BWCs are believed to be able to help fix. As Brian Hofer, chair of the City of Oakland Privacy Advisory Commission, states:

The revelation that we mistakenly deleted all this body camera data tracks a concern we raised during the Domain Awareness Center debate—can the City of Oakland be trusted with our data? (...) As law enforcement moves to collect more and more info about our lives, how do we ensure accuracy, security, and preservation of data when necessary, such as exculpatory evidence? (...) A single mistake can land someone’s profile on a No Fly List or in the CalGang database, with devastating consequences.\textsuperscript{114}

Since many retention policies are not very clear or do not reinforce the deletion of videos, there is a strong possibility issues related to storage will continue to become more difficult to resolve. The longer the videos remain stored, the more chances the public has to request them, which can be a good thing and a bad thing. BWCs were first employed as a tool to better relations between law enforcement and the public since civilians see it as something to promote transparency, even before it being a technology to gather evidence and aid investigations. This can put law enforcement agencies in a difficult position: “If police departments withhold footage, the public is likely to interpret this as betraying the point of the cameras.”\textsuperscript{115} The preservation of BWC videos directly affects issues of access, where many questions are still left unanswered. Access issues will be explored in another chapter of this dissertation.

No one can predict if BWC storage policies will ever reach a point where all the questions have been solved and every situation will have been addressed, but if it happens, it will allow these videos to be used not only as evidence, but also as instructional elements, as

\textsuperscript{114} Cyrus Farivar, “Police IT Staff Checked Wrong Box, Deleted 25% of Body Cam Footage,” Ars Technica, September 16, 2016, arstechnica.com/tech-policy/2016/09/police-it-staff-checked-wrong-box-deleted-25-of-body-cam-footage/.

previously discussed. Developing a framework where specific videos could be used as examples of proper (or even improper) conduct would allow agencies to “study patterns of behavior, train police officers, establish better relationships with citizens, and possibly to prevent crimes.”

Although it would be still counterproductive for a PD to assign personnel to watch countless hours of video in order to determine which files could be helpful with officers’ training and instruction, criminal justice experts at Washington State University’s (WSU) Complex Social Interaction (CSI) Laboratory are using scientific tools and techniques, including biometrics and artificial intelligence, to attempt to answer that question. Launched in 2017 and led by Dr. David Makin, an expert in police training and technology, the program is designing software that analyzes interactions between officers and the public captured in BWC videos. In the process:

The [laboratory] has analyzed more than 2,000 police–community interactions and numerous records from law enforcement incidents to identify, code and catalog key variables associated with a range of outcomes, positive to negative. Location, lighting, time of day, number of people present, gender, race, verbal and physical stress, and intensity of the interaction are among the contextual factors assessed. Makin’s main goal is to turn all the countless hours of BWC footage into data PDs can use to improve “police-community relations, reduce conflict, cost and liability, and enhance the health and well-being of law officers and their communities.” He elaborates:

What I envision for this research is that we will get to a point where we will be able to automate the analysis of the footage and leverage it to inform risk management. In this way, the footage is about improving the delivery of services, and we retain this footage only when it is needed for evidentiary purposes. I believe that through automated analysis, we will be able to reduce the volumes of video generated by agencies, which are becoming more concerning to the community. However, one of the pressing challenges

---


we will face is not the technology, it will be [in] the legislature, which will inform retention and access.119

Currently, the CSI lab has partnered up with Axon for the research, who has supplied the team of researchers with 60 BWCs and access to Evidence.com free of charge. These BWCs are being used in WSU’s own police cadet training and the researchers are developing key performance indicators (KPIs), classifiers which tell computers what behaviors and actions (i.e., use of force) should be watched out for. The idea is that the software will be able to then flag videos where the use of force, for instance, is detected and allow police chiefs to determine if officers are acting in accordance to their training or if changes need to be made. Makin also states that such technology will help departments be more efficient with their time: “Being able to automate the analysis so at the end of the week a sergeant receives a notification that there are 20 videos to review instead of 400 is how we will move policing into the 21st century.”120

If this technology succeeds in its objective and becomes available to departments, only time will tell if it will indeed help with storage and training. Just like most issues surrounding BWCs, the problem is not if the technology is available or not, but if the policies governing its use exist and are being implemented successfully. There is a chance WSU’s artificial intelligence will be helpful. However it will be another additional cost that some departments might not be able to take on and if departments are not establishing a good video retention policy, to begin with, it will not end up being another technology that does not reach its full potential.

Dr. Makin has a good point about BWC. Currently, the majority of agencies are not using this technology as well as they could. Part of improving relationships between law enforcement

and the communities they serve and increasing transparency is to improve training. These cameras are able to capture interactions in a way dashcams and CCTV were never able to.

Although it is not an easy task, creating and implementing appropriate preservation plans for BWC videos is of the utmost importance. After all, these are not merely audio-visual materials, but data with evidentiary, social, and anthropological value: Not only it can help with police investigations and officer training, but it can also provide statistics and information for the study of human behavior.
Chapter 3: Privacy and the Camera

“Since a comprehensive privacy law may never be passed in the U.S. – and certainly not in the near future – law and legal principles must be developed or adapted to rein in particular new technologies such as surveillance cameras, location-tracking devices, and biometrics. Surveillance cameras, for example, must be subject to force-of-law rules covering important details like when they will be used, how long images will be stored, and when and with whom they will be shared.”

Defining privacy can be a daunting task. In 1890, Samuel D. Warren and Louis Brandeis wrote The Right to Privacy, which was published by Harvard Law and is considered the first publication in the United States to explore the right to privacy. In it, Warren and Brandeis define privacy as “the right to be let alone,” and they believed individuals had the right “to protect his or her psychological integrity by exercising control over information which both reflected and affected that individual’s personality.”

In 2000, Andrew von Hirsch further explored what privacy is by establishing three concentric circles of activities in which privacy is a factor, and the individual is afforded a different type of protection in each of these circles. The smallest circle concerns an individual’s personal and inner life, “where there should be a broad entitlement to resists demands for

disclosure of any kind: his intimate life is something he should be able to keep to himself or reveal only to chosen others.\textsuperscript{125}

The next concentric circle deal with social and work life, where the individual chooses to share some information to facilitate social and working life. In this circle, however:

Determining what information should be and should not be protected from disclosure is a difficult issue to resolve, both theoretically and practically, because this second circle concerns relationships with chosen working and social associates who have certain legitimate matters to transact with the person involved.\textsuperscript{126}

The third circle is about the individual in a public space, where he or she has the least control over who he or she meets and interacts with. Since the people around the individual in the public space might have different values, attitudes, and commitments, it is up to the individual to:

Limit the extent to which he may be called upon to respond to the expectations, or even to satisfy the curiosity, of such unchosen others. The entitlement of non-disclosure is more straightforward in this third circle, because it concerns \textit{strangers} – those with whom the person has not undertaken dealings of any kind.\textsuperscript{127}

\textsuperscript{126} Ibid., 63.
\textsuperscript{127} Ibid., 63.
Figure 5. Concentric Circles of Privacy, based on Andrew von Hirsch, “The Ethics of Public Television Surveillance,” in *Ethical and Social Perspectives on Situational Crime Prevention* (Hart, 2000), 63.

According to von Hirsch, privacy is one’s entitlement to non-disclosure; it is how one protects oneself from scrutiny by other people and how one controls whose expectations one has to satisfy.\(^\text{128}\) Consequently, privacy can be considered a form of self-ownership:

Privacy is concerned with the degree to which we can control access to ourselves, exclude others from participating in our lives and refuse to accept their attention. A person must have a say over how closely he wants to get involved with other individuals and how much of himself he wants to disclose, for making distinctions in the way we engage with others is of fundamental significance in human relations.\(^\text{129}\)

Furthermore, Nagel adds that privacy can be seen as a humanizing factor: “The boundaries between what we reveal and what we do not, and some control over that boundary are among the most important attributes of our humanity.”\(^\text{130}\)

Privacy is also heavily associated with the sense of self:


[An] autonomous person is to be capable of having privileged access to information about your psychological profile — your hopes, dreams, beliefs, and fears. A capacity for privacy is a necessary condition of autonomous personhood.\(^{131}\)

On the other hand, unwanted exposure, argues von Silva-Tarouca Larsen, is demeaning since one is unable to control how much, and when one is scrutinized and it takes away the right to only present to the public what a person is comfortable sharing with others. Although some critics, like Judith Jarvis Thomson, argue privacy is merely a right and should be discussed as other rights such as the right to liberty or right not be harmed\(^{132}\) and present society thrives on oversharing on social media platforms and live streams, privacy is still regarded as a valuable right. In fact, many closed institutions, such as prisons, strip this right from inmates as a way to assert control and punish.

In his book *Discipline and Punishment*, French philosopher Michel Foucault noted that by the mid-nineteenth century, "punishment had no doubt ceased to be centered on torture as a technique of pain [and] it assumed as its principal object loss of wealth or rights."\(^{133}\) Although there was still a level of corporal punishment (imprisonment, rationing of food, forced labor, etc.) it was understood that the most severe penalty was no longer addressed to one’s body, but it had been “replaced by a punishment that acts in depth on the heart, the thoughts, the will, the inclinations.”\(^{134}\) Foucault further explores these thoughts by illustrating how the “nature of crime control has shifted from using the threat of violence and the fear of being physically punished to control through surveillance – fear of being seen to be doing something wrong.”\(^{135}\)


\(^{134}\) Ibid, 16.

Thomas Jefferson once wrote: “Whenever you are to do a thing, though it can never be
known but to yourself, ask yourself how you would act were all the world looking at you, and act
accordingly.”136 Although there have been conflicting studies regarding the effectiveness of
BWCs, many experts believe the presence of images and/or objects related to vision can affect
people’s behavior. In 2010, a team of scientists at Newcastle University conducted a study where
posters containing images of eyes were hung inside a cafeteria “in conjunction with, and not
associated with, verbal messages to clear one's litter.”137 Ernest-Jones et al. found the presence of
staring eyes decreased the amount of litter left by the cafeteria patrons, implying that these
“implicit cues of observation”138 can affect human behavior, possibly influencing them to follow
rules and display more socially acceptable comportment. This effect can be connected to
people’s inherited inability to:

Inhibit responses to gaze even when instructed to. This makes sense, because there is
great evolutionary value in being able to quickly assess whether any predators are on the
prowl; neural activation of the gaze detection system is fast and automatic. Yet this also
means that [it is] possible to “trick” the system and this is exactly what the new
experiment has shown: objects that merely resemble human eyes are sufficient to trigger
human gaze detection and subsequently alter social behavior.139

Arguably, cameras have similar effect.

Control by surveillance was a concept first introduced by eighteenth-century social
theorist Jeremy Bentham and his idea of the Panopticon. Panopticon, which comes from the

April 30, 2018, avalon.law.yale.edu/18th_century/let31.asp.
137 Max Ernest-Jones, Daniel Nettle, and Melissa Bateson, “Effects of Eye Images on Everyday Cooperative
Behavior: A Field Experiment” (Centre of Behavior and Evolution, Newcastle University, October 23, 2010).
138 Max Ernest-Jones, Daniel Nettle, and Melissa Bateson, “Effects of Eye Images on Everyday Cooperative
Behavior: A Field Experiment” (Centre of Behavior and Evolution, Newcastle University, October 23, 2010),
https://www.staff.ncl.ac.uk/daniel.nettle/ernestjonesnettlebateson.pdf.
139 Sander van der Linden, “How the Illusion of Being Observed Can Make You a Better Person,” Scientific
you-better-person/.
Greek words *pan* (meaning “all”) and *optikón* (“sight” or “seeing”),\(^{140}\) was technically first introduced by the theorist’s brother, who:

> Was working in Russia on the estate in Krichev and he had a relatively unskilled workforce, so he sat himself in the middle of this factory and arranged his workforce in a circle around his central desk so he could keep an eye on what everyone was doing.\(^{141}\)

Bentham observed what his brother was doing and developed the idea for an architectural prison model, which “consisted of a circular, glass-roofed, tank-like structure with cells along the external wall facing toward a central rotunda.”\(^{142}\) A supervisor would stay inside the central tower, and although surveillance would not be continuous, the prisoners would not be able to see the guard on duty, inducing “in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power.”\(^{143}\)

Foucault states the Panopticon becomes “a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen.”\(^{144}\) This aspect is interesting because one could argue today’s society does not have one single tower, but various elements with disciplinary power. At its core, Bentham’s Panopticon principle is based on the idea of central inspection, which has obvious parallels to the use of CCTV surveillance, where the monitoring is done from a central location. In addition, cameras, both in CCTV systems and BWCs, arguably have the same effect as Bentham’s tower since they are visible and act as a reminder to the public that they are being watched.

---


\(^{144}\) Ibid, 202.
Active behaviors being observed is one thing, but another issue comes about when people feel as though even their thoughts are being subject to a lack of privacy. With current developments such as targeted advertising, Google’s predictive searches and Smart Replies, which read one’s email or messages and predicts possible replies, Facebook’s predictive photo editing and tagging, and Snapchat’s automatic GPS tracking, it is easy for one to feel their thoughts are already being read and their conversations being eavesdropped by technologies. Extreme surveillance only intensifies these feelings of invasion of privacy, and although it is heavily debated if cameras indeed have the power to stop or prevent crime, no one can deny their psychological effect on many members of the public, making them feel safer. There are also many who believe the presence of cameras changes people’s behavior: “Most people now obey the rules because they know they are being watched – they regulate their own [behavior] for fear of becoming the wrong kind of person.”

In his writing, von Hirsch relates how CCTV systems affect privacy in public spaces since it infringes on a person’s expectations of remaining anonymous. CCTV captures all sorts of behaviors, not limiting its recordings to criminal activities. In other words, anyone captured in those recordings can be under scrutiny. However, CCTV systems also create a certain distance between what a viewer looking at the footage sees and what the people captured in the footage experience and observe. For someone viewing the footage, the action is only seen from one angle and can come off rather removed from the overall scope of the situation, as different viewpoints and perspectives can shift how something is interpreted. Although technology and video quality

---

have improved greatly over the years, a lot of CCTV footage is still not very effective in objectives such as identifying criminals. This happens for mainly two reasons:

- Criminals have become used to CCTV cameras, so they frequently employ disguises – hoodies, bandanas, ski masks, etc. – to cover their faces and hide their identities.

  Although they are not always successful or prepared, the presence of cameras tends to not be seen as an insuperable obstacle, but just another challenge to overcome:

  One day in 1995, a large, heavy middle-aged man robbed two Pittsburgh banks in broad daylight. He didn’t wear a mask or any sort of disguise. And he smiled at surveillance cameras before walking out of each bank. Later that night, police arrested a surprised McArthur Wheeler. When they showed him the surveillance tapes, Wheeler stared in disbelief. “But I wore the juice,” he mumbled. Apparently, Wheeler thought that rubbing lemon juice on his skin would render him invisible to videotape cameras. After all, lemon juice is used as invisible ink so, as long as he didn’t come near a heat source, he should have been completely invisible.\(^\text{147}\)

- CCTV systems mostly use low video resolution and low frames per second (FPS) in order to maximize memory.\(^\text{148}\) If, for instance, a person of interest is cropped from CCTV footage and the image is enlarged, it results in a very grainy (noisy) picture where most details are blurry or lost altogether.

  Although more modern cameras have a powerful optical zoom and the ability to move vertically and horizontally, if individuals move out of its angle of view, their actions will not be captured.

  Aside from all of this, the presence of CCTV systems can make people feel uncomfortable. The famous phrase “Big Brother is watching you,” which first appeared in George Orwell's novel *Nineteen Eighty-Four*, tends to come to mind when people become aware of public surveillance, and that more often produces a certain anxiety of being watched.


However, it is possible this feeling of anxiety is not solely caused by the presence of cameras, but the presence of various security measures, such as gates and motion activated lights, used in conjunction with video surveillance. After all, “the more you secure a block or an estate, the more it gives a message that something is wrong with that estate.”

Many critics similarly believe body-worn cameras can easily intensify the feeling of a violation of privacy. After all, the camera is closer to the action: attached to an officer’s uniform or head, the camera gives viewers a sense of immersion since it captures images that are close to the officer’s point of view. It moves with the officer, it follows the event, and it can capture all of the intense emotions some of the interactions between law enforcement and civilians can produce. Sometimes, however, BWC footage can exaggerate the situation. Seth W. Stoughton, a law professor at the University of South Carolina, calls his effect *deceptive intensity*:

> Which refers to our tendency to overestimate the amount and speed of movement, and thus the intensity of the action, in body-worn camera footage. [It] results from a confluence of the camera’s location, the way BWCs move, and the way we perceive motion. With regard to the camera’s location, Hollywood directors have known for years that positioning the camera underneath the subject, so the upward angle of the show exaggerates the subject’s height and the breadth of their shoulders. A shoulder- or chest-mounted camera will duplicate that effect, particularly when officers are physically close to the subject being recorded (...) Whatever the body-worn camera attaches to, it is not so tightly connected to an officer’s body that it will mimic exactly her movements. Instead, it will bounce around, thrown about by the sway of an officer’s head or the jostling of an officer’s chest.

Advances in technology have allowed the majority of BWCs that are currently available in the market to have high video quality, allowing faces and other defining individual characteristics to be captured with remarkable accuracy. This capability creates the perfect setting for the implementation of facial recognition software and other video analysis tools.

---


By its most basic definition, facial recognition consists of a biometrical identification application which utilizes algorithms automatically “that analyze specific facial features, such as the relative position, size and shape of a person's nose, eyes, jaw and cheekbones”\(^{151}\) to identify individuals from video frames or other digital images. Unlike fingerprinting, blood samples, and retinal scans, it does not require an individual’s consent or knowledge, and its use preoccupies a great number of privacy and civil rights advocates.

In 2015, a coalition of over 24 organizations including the National Association for the Advancement of Colored People (NAACP) and the American Civil Liberties Union (ACLU) released a set of guidelines which:

- Ask police to develop policy with input from the public, to avoid using facial recognition and other biometric technology in examining the footage, to follow specific regulations on how long data is retained, make the footage available to the press and to prevent officers from viewing the footage before filing incident reports.\(^{152}\)

Still, facial recognition software is being developed and employed by many state and local law enforcement agencies, even though there are no comprehensive state laws regulating its usage, and very little is known about its accuracy.\(^{153}\) In fact, there is evidence to the contrary, and according to the ACLU, this technology has a “disproportionate impact on communities of color.”\(^{154}\) This happens because the algorithms used by facial recognition software are not immune to racial bias and the majority of people present in police databases are African American since they are disproportionately more likely to have interactions with law enforcement.

---


enforcement and are more likely to get arrested than any other racial group in the United States. Consequently:

Police face recognition may be overused on the segment of the population on which it underperforms. It also means that African Americans will likely be overrepresented in mugshot-based face recognition databases. Finally, when algorithms search these databases, the task of selecting a final match is often left to humans, even though this may only add human bias back into the system.

In addition, a study conducted at the University of Texas at Dallas, which analyzed state-of-the-art face recognition algorithms against databases with both Caucasian and East Asian faces, shed light on inherited racial bias computer programs can demonstrate. In the first phase of the study, it was concluded “the Western algorithm recognized Caucasian faces more accurately than East Asian faces and the East Asian algorithm recognized East Asian faces more accurately than Caucasian faces.” In other words, just like humans, algorithms work better recognizing their own than the other-race face, and it is unlikely companies are employing a diverse group of developers to work and test these biometric tools.

In the next phase of the study, researchers analyzed how both Western-designed and East Asian-designed algorithms performed with a database where the majority race was Caucasian. In this case, both algorithms performed better at identifying Caucasian faces. This bias can be explained by the fact that algorithms tend to perform better recognizing faces of the race they were trained with: “When those faces disproportionately represent one race, an algorithm will optimize its accuracy for that group at the expense of others.”

---

Another study conducted in 2012 suggests certain demographics are more difficult to be identified successfully by facial recognition algorithms. These demographics mainly consist of African Americans, since most software rely on color contrast to define facial features, and women, which hypothetically can be harder to identify due to the use of cosmetics and makeup.\(^{159}\)

Although experts have been vocal about these issues, many agencies that use facial recognition software do not run tests on their algorithms or audit searches for misuse and abuse,\(^{160}\) increasing the chances of misidentification or failure to identify the real perpetrators, which in turn “could result in innocent citizens being marked as suspects in crimes.”\(^{161}\) Unfortunately, for reasons previously stated, African Americans are more vulnerable to these “glitches.”

Facial recognition associated with BWC usage poses more risks to privacy because the camera is not confined to only one spot or angle, which is the case with dashcams and CCTV systems. In 2017, at least two big companies announced their efforts of integrating this technology to BWCs. Motorola partnered up with artificial intelligence software startup Neurala in order to create intelligent cameras “that can learn ‘at the edge’ and automatically search for persons or objects of interest—significantly reducing the time and effort required to find a missing child or suspicious object in environments that are often crowded or chaotic.”\(^{162}\)

---


Neurala’s “at the edge” learning capabilities help solve some of the biggest challenges that come with real-time applications of AI. Neurala’s patent-pending technology provides an alternative to lengthy training for the AI engine, so that, for example, the intelligent camera “learns” to identify the person or object of interest. This feature, known as incremental learning, also reduces the risk of “catastrophic forgetting,” which occurs when a neural network forgets its previous training. Incremental learning also enables enhanced accuracy and latency for real-time public safety applications of AI.\textsuperscript{163}

In that same year, Axon announced it had purchased two artificial intelligence companies, Misfit and Dextro, to form a new division, Axon AI. According to CEO and founder Rick Smith’s press release, Axon is very aware of all the complexities surrounding artificial intelligence and has been “finalizing a fully independent, public AI Ethics Board (...) comprising established thinkers from civil rights law, data privacy, AI ethics, and the community [to work] on a set of AI governing principles and publish the results.”\textsuperscript{164} Axon AI aims to implement the following features to Axon’s camera system:

- **Automated Redaction:** So officers can share footage with the public faster while protecting the privacy of individuals captured in a video.
- **Accelerated Review:** So supervisors can better understand compliance and provide feedback in order to improve training and police-community relations.
- **Automated Reporting Generated Directly from Video and Audio:** So officers can spend more time with the community instead of writing reports.\textsuperscript{165}

Before Dextro was bought by Axon, it had already raised some eyebrows due to its ability to identify objects while scanning camera footage. When it first appeared in the market, Dextro was advertised as a video analysis tool that was able to identify and tag objects (i.e.,

specific types of shoes, a gun), places (i.e., indoor and outdoors) and actions (i.e., a punch, handshake) during live stream videos. Its algorithms were said to “actually ‘watch’ the contents of the videos themselves to form the basis of [a] search.”

Just how Axon now aims to use this technology, Dextro engineers believe this software can help PDs go through a large quantity of video data and isolate only the moments and details that are of interest, consequently improving redaction. In an interview with Gizmodo, Marcus Womack, Axon’s former executive vice president, also detailed how this type of artificial intelligence can help with officer training by pinpointing errors of other officers acting improperly in certain situations, such as incidents of mistaking a cell phone for a gun. Ideally, this could also potentially help with storage concerns for a department where BWC videos were used as instructional tools in addition to serving as evidence.

However, many are concerned this type of technology would serve more as a surveillance tool and not so much as an accountability tool, as Axon and Dextro engineers state, especially since AI can be implemented to other police instruments including “surveillance footage access, drones, Stingrays, face recognition databases, [and] license plate readers.” In 2016, already half of American adults – more than 117 million people – were in a law enforcement face recognition network, regardless of their innocence, and this number has most likely been growing steadily over the years. According to Alvaro Bedoya, Executive Director of the Center on Privacy & Technology at Georgetown Law:

169 Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle, “The Perpetual Line-Up: Unregulated Police Face Recognition in America” (Georgetown Law, Center of Privacy and Technology, October 18, 2016).
By using face recognition to scan the faces on 26 states’ driver’s license and ID photos, police and the FBI have basically enrolled half of all adults in a massive virtual line-up. This has never been done for fingerprints or DNA. [It is] uncharted and frankly dangerous territory.\textsuperscript{170}

Face recognition databases, AI, and BWCs might decrease a person’s ability to remain anonymous. During an interview with Gizmodo, Jay Stanley, a senior policy analyst with the ACLU, remarked:

One of the big fears is that these cameras become roving surveillance cameras. We could have 30,000 officers with these cameras and a list of suspected terrorist with their photos, and now everybody who bears a passing resemblance is getting stopped by every police officer who enters their field of vision. I don’t think most Americans want to live in a world like that.\textsuperscript{171}

Public fears are also a very marketable, and companies are not wasting any time coming up with products aimed at those who are concerned about maintaining their privacy in the public space. Created by Scott Urban, “Reflectacles” are light-reflecting sunglasses and eyeglasses. One of its products, “Reflectacles Ghost” is designed to “reflect both visible and infrared lights,”\textsuperscript{172} a feature which prevents facial recognition systems from identifying those who wear it. Therefore, this product can be classified as an anti-facial recognition device. The sunglasses:

Are created with solid blocks of clear cellulose acetate and CNC machining was utilized for constructing the product instead of the conventional plastic mold injection. There is a metal wire core that runs across the temple to make it sturdier and allowing full customization so that the glasses fit your face. You can change lenses as well with the presence of a machines groove within the frame. The lenses are UV coated and created from high-grade CR39 plastic. Every pair comes with slightly tinted Active lenses or darkly tinted Sunglass Lenses. You can remove and replace these lenses with your prescription lenses at any time.\textsuperscript{173}

The Reflectacles Ghosts starts off at $125.00.174

There are also other eyeglasses and clothes, including “baseball caps, hoods and even a burqa”175 being sold that are lined with NIR LEDs. Just like the Reflectacles eyeglasses, these items also blind surveillance cameras, blocking facial-recognition systems from making positive identifications.

One of the most interesting (if not bizarre) anti-facial recognition products currently available on the market are the URME Personal Surveillance Identity Prosthetic Masks. The product, which resulted from a partnership between URME Surveillance and ThatsMyFace.com, is made “from a pigmented hard resin, this mask is both a 3D scan of artist Leo Selvaggio's face, as well as photorealistic rendering of his features, such as skin tone, texture and hair.”176 It is regularly priced as $299.00, but as of March 2018, it is being sold for $200.00.
As previously mentioned, facial recognition software has a difficult time identifying females, and that is most likely caused by the use of cosmetics and makeup. Consequently, one can purposely use makeup to foil the algorithms used in facial recognition. During his time as a student at New York University’s Interactive Telecommunications Program, artist, designer, and entrepreneur, Adam Harvey, for example, created patterns with makeup that are able to confuse facial recognition algorithms. These patterns, called Computer Vision Dazzle (or CV Dazzle), are based on a simple concept:

Facial recognition algorithms look for certain patterns when they analyze images: patterns of light and dark in the cheekbones, or the way color is distributed on the nose bridge—a baseline amount of symmetry. These hallmarks all betray the uniqueness of a human visage. If you obstruct them, the algorithm [cannot] separate a face from any other swath of pixels.  

Figure 7. Some of Harvey’s CV Dazzle patterns. From: cvdazzle.com/

Privacy laws in the United States, especially those related to video capture, are very confusing. While video recording is forbidden during legal proceedings in the Supreme Court and various state courts, restricted during live performances, and deemed controversial when citizens record police officers (which became a hot topic after videos of Staten Island officers putting Eric Garner in a chokehold during his arrest and Walter Scott being fatally shot by a
police officer during a routine traffic stop were heavily disseminated online),\textsuperscript{178} the U.S. “only [has] a patchwork of largely inadequate”\textsuperscript{179} laws regarding privacy.

Aside from the policies mentioned in the Recording the Video chapter, there are still many issues that have yet to be discussed regarding privacy and BWC videos. Most civil rights groups focus on the privacy of civilians when these issues, but the privacy of police officers who wear these cameras is also valuable and many times, completely ignored. Some experts, including Kevin Angell, believe the pre-event recording function in BWCs is a threat to officers’ privacy, and it is rarely discussed in depth. He states a “camera that uses pre-event recording is [always] recording. It doesn’t know that you have entered a restroom, your child’s bedroom to kiss them [goodnight] or that you are receiving a ‘be safe’ hug from your spouse.”\textsuperscript{180} Although cameras with pre-event recording feature do not save all the footage recorded in the camera’s memory, problems can and did happen. In 2016, police officers in Round Lake Park, Illinois, filed a federal lawsuit for nearly $10 million after video of them engaging in private activities was captured by their own BWC.\textsuperscript{181} In the suit, officers state they had a two-hour training session on the then newly acquired VISTA BWC from Texas-based Enforcement Video, known as WatchGuard Video and although a manual for the cameras was provided, there were no mentions of continuous video recording.\textsuperscript{182} Not surprisingly, WatchGuard states this feature has helped law enforcement tremendously, that it can be disabled by the department’s administrator, and the “system only saves video to the server if it is marked as evidence, otherwise, it typically


\textsuperscript{180} Kevin Angell, “Your Invitation to the Pre-Event Disaster Party…Please RSVP,” \textit{BWC Expert} (blog), September 29, 2016, bwcexpert.com/category/privacy/.


\textsuperscript{182} Lepe, Colon, Izzo, Lyons, Reuter, Vela, Rodriguez, Segreti, Shepard, and Valle v. Village of Round Lake Park and Filenko (n.d.).
gets recorded over in a day or two.” The plaintiffs argue that they were unaware of this feature and for a period of seven months, their BWCs captures them using the bathroom, with their genitals and buttocks exposed, changing in the locker room, and “performing other private and personal acts.” Officers were humiliated after they finally viewed the footage.

In the suit, it is also stated that the plaintiffs believe both their chief and deputy chief were aware of the videos, which had been recorded even when the cameras were in “off mode” and “sleep mode.” They also believe the chief deleted these videos, thus violating Illinois State “Law Enforcement Officer-Worn Body Camera Act,” which states any video recorded by a BWC needs to be kept for at least 90 days before being deleted or altered.

---


Chapter 4: Access to the Footage

Who gets to watch the videos captured by a body-worn camera? Access to BWC videos is determined by state laws that are not specific to them, but involve public records. However, since BWC videos are unlike any other police record, state legislatures are debating new bills to address privacy and security issues. While that is being determined, police departments have to create policies to keep these records safe and at the same time be responsive to the public when video is requested. According to the LCCHR and Upturn:

Increasingly, departments are establishing explicit procedures that allow recorded individuals — like those seeking to file a police misconduct complaint — to view the footage of their own incidents. Four departments we analyzed — in Cincinnati, Las Vegas, Parker (CO) and Washington DC — now appear to provide special access to recorded individuals. These special access rights, tailored specifically for body camera footage, exist alongside state-level public records laws.186

For the most part, BWC footage is not part of public records, and to make matters more complicated, the definition of public records tends to be very broad.187 In the United States, public records fall under the Freedom of Information Act (FOIA), which generally provides any person with the statutory right, enforceable in court, to obtain access to Government information in executive branch agency records.188 However, Congress has established nine categories of information that are exempt from being released to the public, in order to “protect interests such as personal privacy, national security, and law enforcement.”189

---

Releasing BWC footage to the public is a tricky subject because it involves privacy issues, investigation and evidence handling, and public interest. If a video depicts a victim of sexual abuse giving her account of her or his traumatic experience, and the public requests the release of the video, what should be considered priority: the victim’s privacy or the public’s request (if, for instance, they argue that BWCs are –before anything else – a transparency tool?) What if the police department argues the release of a video can impair an ongoing investigation? Certainly, it is a valid reason not to release a video, but it will not appease the public’s distrust on law enforcement.

Another relevant point to consider is that many state laws allow police departments to charge a fee to those who request access to the videos, “for the time it takes to locate, review and produce records.”190 Louisville Metro Police Department (LMPD), for example, states in its policy book that “recordings provided to persons or agencies outside of the LMPD shall be duplicated on new tapes or discs and will be provided by the department for a reasonable fee,”191 but does not specify what the actual fee is. Other departments, such as the Las Vegas Metropolitan Police Department (LVMPD), are more transparent in regard to this issue, informing the public on its website that a fee of $50.00 per hour “will be charged for the processing of a recording to redact confidential information.”192

Currently, most of the existing state laws regarding BWC footage and access have a few exemptions based on FOIA. Generally speaking, a video will most likely not be released if it:

• Compromises someone’s privacy: According to FOIA’s sixth exemption, the disclosure of information that could result in a clear “unwarranted invasion of personal privacy,”\textsuperscript{193} such as medical or personnel files, should be avoided. However, Marshall argues that with BWC videos, public interest might speak louder than privacy concerns and sometimes footage will be released on that basis.\textsuperscript{194}

• Relates to personnel files and/or disciplinary records: Sometimes, BWC videos will capture officers behaving inappropriately, and certain departments might be resistant or purposely stall the release of such videos. Marshall adds:

> It is not uncommon for states to withhold certain types of information about employees, whether it relates to sensitive data (such as Social Security numbers and home addresses) or performance evaluations. Generally, however, these exemptions do not allow agencies to withhold records that indicate employee wrongdoing, which is important to note when requesting access to videos that may show police misconduct. In Oklahoma, bodycam videos that show law enforcement personnel under investigation may be temporarily redacted to obscure their identity, unless the investigation lasts for an unreasonable amount of time.\textsuperscript{195}

In fact, in January 2018 the Patrolmen’s Benevolent Association, New York City’s largest police union and “the largest municipal police union in the world,”\textsuperscript{196} filed a lawsuit in the State Supreme Court in Manhattan to prevent BWC videos depicting critical incidents, such as police-involved shootings, from being released to the public. Union lawyers argue that these videos, both in their raw and edited versions, “are personnel records shielded from public disclosure by Section 50-a of the state Civil Rights law, a statute that also protects officers’ performance evaluations and disciplinary

\textsuperscript{195} Ibid.
records.” For that reason, they argue, the release of these videos can endanger police officers’ safety and the public’s right to privacy.

- Impairs an ongoing investigation: According to FOIA, if a requested material has the power to potentially impair a criminal investigation, it should not be released to the public. However, just as mentioned above, this matter is not so straightforward when it comes to BWC videos since state laws have also to consider privacy issues and public interest.

No matter what the access policy is, mistakes are bound to happen and videos might get leaked to the public. On January 3rd of 2018, Sahleem Tindle was fatally shot by a Bay Area Rapid Transit Police Department (BART) officer in West Oakland, California. Tindle’s death was captured by the officer’s BWC and the video was later shown to members of Tindle’s family, who then released a portion of said video to the media without the police department’s authorization since they believed it depicted illegal use of force. This “leak,” according to Oakland Police Department’s Captain Roland Holmgren, could have jeopardized the investigation if investigators did not manage to interview a key witness before the clip started circulating through the media:

If the witness had seen the unauthorized version of the video before making a statement to OPD, it would have raised questions about whether the witness was recalling what he actually saw during the shooting or whether he simply “regurgitated” what he saw on the news.

---


The family stated they released the video in an attempt to get justice for Tindle. The officer involved in the shooting “was cleared and has returned to full duty after passing drug and alcohol tests and psychological exams”\(^{200}\) a little over two weeks after the incident. Oakland PD has since released the full video.

As of May of 2018, only 24 states in the U.S. have legislature regarding access of BWC footage. Most of these existing laws address if BWC videos are considered public records, how and who should be able to access them, and give an idea of how each state tries to balance an individual’s privacy with public interest:

- Certain states, such as New Hampshire and North Carolina, establish that BWC videos are not public records. However, a video may be released to the public if there is “a compelling public interest.”\(^{201}\)
- States where BWC footage is considered to be public record, Oklahoma and Kansas, for example, also list situations in which videos should not be released to the public, such as circumstances where a person has a reasonable expectation of privacy (i.e., inside a private home or in medical facilities). In addition, some states include examples of situations when a video should be redacted prior its release: when there is depiction of nudity, death, or the identity of a minor. It is worth noting that these exemptions are congruent with the activation policies listed in “Chapter 1: Recording the Video.”
- Other states define who is able to request access to a video and establish specific procedures one must follow in order to do so. In Indiana, for example, those allowed to


view a recording, which the statute defines as *requestors*, must fit into one of these four categories:

1. A person depicted in a recording, or if the person is deceased or incapacitated, the person’s relative or representative.
2. An owner or occupant of real property depicted in a recording.
3. A crime victim, if the depicted events are relevant to the crime.
4. A person who suffers a loss due to personal injury or property damage, if the depicted events are relevant to the person’s loss.\(^\text{202}\)

- On the other hand, Missouri, which is nicknamed the “Show Me State,”\(^\text{203}\) allows any person to request BWC data, but also establishes that the court can prevent a video from being released if it:

> Contains information reasonably likely to disclose private matters in where the public has no legitimate concern or will bring shame or humiliation to a person or was taken in a place where a person has a reasonable expectation of privacy.\(^\text{204}\)

Creating laws and policies that address the issue of access is like walking a fine line between giving the public the transparency they want and protecting the privacy of those depicted in the videos. On March 20, 2018, the Los Angeles Police Commission voted and approved a new policy that requires the Los Angeles Police Department (LAPD) to “publicly release video from police shootings and other ‘critical incidents’ within 45 days of when they occur.”\(^\text{205}\)

---


The Los Angeles Board of Police Commissioners constitutes critical incidents as:

- Officer-involved shootings, regardless whether a person was hit by gunfire. It does not include unintentional discharges and officer-involved animal shootings.
- A use of force resulting in death or serious bodily injury resulting in hospitalization.
- All deaths while an arrestee/detainee is in the custodial care of the Department unless there is no evidence of misconduct, use of force, or an act committed by an arrestee/detainee that appears to cause injury or death.
- Any other police encounter where the Commission or the chief of police determines the release of video is in the public interest.²⁰⁶

When addressing privacy concerns, the policy states that the law or court orders can keep a video from being released to the public. If there are minors or victims of “certain crimes” (possibly sexual and/or domestic abuse victims) captured in the video, the image will be edited or redacted to protect their identities. If it is not possible to edit or redact the video enough to protect individuals, the video will not be released. The policy is scheduled to take effect within 30 days after its approval date.

Other departments in other states have different approaches. The New York Police Department (NYPD) releases BWC videos on a case-by-case basis when the public or press file open-records request, but the process is lengthy and it can take months.²⁰⁷ On a survey conducted by the NYPD in 2017, civilians and officers were asked their opinions on several matters regarding BWCs, including public access to videos. To the statement “If a person has an

interaction with an officer wearing a body-worn camera, the NYPD should be required to show
that person the footage upon request,” the majority of the public interviewed strongly agreed the
footage should be released, while the majority of the officers interviewed disagreed.208

Figure 8. Release of BWC footage, Graph 1. From:

To the statement “If a person has an interaction with an officer wearing a body-worn camera, and
a news reporter or advocacy group requests the footage, the department should be required to
give it to them,” the results were different:209

208 “NYPD Response to Public and Officer Input on the Department’s Proposed Body-Worn Camera Policy” (New
York City Police Department, April 2017), www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-
worn-camera-policy-response.pdf.
209 “NYPD Response to Public and Officer Input on the Department’s Proposed Body-Worn Camera Policy” (New
York City Police Department, April 2017), www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-
worn-camera-policy-response.pdf.
In contrast, the Seattle Police Department (SPD) started a YouTube channel called “SPD BodyWornVideo” in 2015 where BWC videos would be uploaded and, consequently, accessible to the public. In order to protect the privacy of those depicted in the videos, SPD organized a “hackathon” bringing together three dozen computer experts to help develop a fast and inexpensive way to redact sensitive images from countless hours of footage.\(^{210}\) Hacker Tim Clemans developed a software that is able to redact over four hours of footage in half a day, which is effective in speeding up the redaction process, since “a simple manual redaction in a one minute video, for example, can take specialists upwards of half-an-hour, whereas more complicated edits –like blurring multiple faces or pieces of audio – can take much, much longer.”\(^{211}\)

---


However, critics are not pleased with the ending result. Clemans’ redaction software blurs the entire image, making “most of the videos look like that moment in movies when someone who's been knocked out slowly regains consciousness.”

Figure 10. Over-redacted preview of AXON_Body_Video_2015-02-18_0533, SPD BodyWornVideo Channel, Oct 6, 2016. From: www.youtube.com/watch?v=kqh_y1zhNPk

The videos are also devoid of audio. Although the blurriness is supposed to protect the privacy of the individuals captured in the videos and allow SPD to upload these images online for all to see, some members of the public pose the question: is it worth to release a video to the public if no one can really see anything? On one of the comments left on a The Verge article about SPD redaction endeavors, user Syvergy states:

I’m wondering what the actual point of this footage is. You can’t see anyone, hear anything, or have an understanding of what is going on. In effect, as a tool for public transparency, this footage is utterly pointless. Sure, spend some time and money blurring out faces, beeping out personal details/changing voices, but if you’re making something for the public it needs to be actually useful. This footage is a complete waste of money, and if I lived in Seattle it would make me annoyed that someone is wasting money on it. If this is the best they can do, don’t bother. Keep the cam footage private and only use it in court.

SPD’s YouTube channel was last updated on October 6, 2016.

Access inside a police department is also something that needs to be discussed. According to Upturn and LCCHR’s Scorecard, many departments with BWC policies (59 out of the 75 surveyed) allow or sometimes even encourage officers to review the footage before they file their reports. This practice has the obvious advantage of allowing officers to make sure their reports are accurate and even notice things they were not able to see during the recording of the video.

As Officer A explained during his interview, his department uses a BWC system that connects to an application in the officers’ phones. Before the footage gets sent to the cloud for storage, this application allows the officer to review, yet not save the video. This, Officer A argues, allows officers to be as specific as possible while filing reports and allows them to make notes of details that at first do not seem that important or relevant. If, while filing a report on a DWI (driving while intoxicated) for example, the officer does not remember if the person who got stopped “wobbled on step three or five” and is not accurate with that detail on the report, a defense attorney can use that to argue the officer is lying and potentially have the case dismissed in court. Officer A believes that some defense attorneys are against officers re-watching BWC footage because now reports can be so precise that it creates problems for the defense.214 However, it is also creates opportunities for ill-intended officers to fabricate details. Dunn and Lieberman advise:

Finally, other than situations in which video will be used to resolve a complaint, in a criminal prosecution or in a disciplinary proceeding, videos should be destroyed as quickly as possible (recognizing that videos that are altered so individuals cannot be

214 Interview with Officer A, interview by Caroline Oliveira, Phone, April 6, 2018.
identified may remain in the public realm). After all, the best way to minimize abuse is to minimize the size of archives.\textsuperscript{215}

It is also important to note, “many of the police departments that use BWCs participate in fusion centers, joint information-sharing efforts between local, state, and federal government and the private sector.”\textsuperscript{216} While the sharing of evidentiary videos between law enforcement agencies can be beneficial from an investigation standpoint, it can also, unsurprisingly, raise more privacy issues, and currently there are not enough guidelines in place to control this activity.

Providing access to BWC footage is a controversial topic. The cameras were first adopted as an accountability tool, but the confusing patchwork of state laws and the sheer nature of the videos make the question of “who gets to see the footage?” very challenging to answer.


Chapter 5 - What Does the Future Look Like?

“Do we want to police in the future the way we are policing today? I don’t think so. How did we get to where we are today? We looked; we listened; we learned; we changed; we grew with the times. That’s our job as leaders today.”—Jim Fox, Chief Newport News, Virginia, Police Department.

For decades, Hollywood movies and television shows have predicted many scientific advances in every aspect of human life. Years before Black Mirror, a British science fiction anthology series first released in 2011, explored a dystopian future where implants, surveillance, virtual reality, and other innovations collide with the dark side of human nature, motion pictures like Minority Report (2002) and RoboCop (1987) introduced viewers to technologies that at the time felt highly fantasized, if not entirely fictional tools used in crime fighting, prevention, and suspect identification. In Minority Report, a team of specialized police officers is able to predict felonies before they happen and arrest the future perpetrators, virtually eliminating crime from Washington D.C. Some of the technologies in the film, including iris recognition, robots that are deployed to explore dangerous areas, and some restraints tools, have since become a reality and have been used by police departments and the military for years. Interestingly enough, even crime predicting CCTV cameras, which work by emitting alerts to its operators when suspicious behavior such as loitering and unusually slow walking are spotted, were introduced in

---

Portsmouth, Britain, in 2008.\textsuperscript{218} In \textit{RoboCop}, a fatally wounded officer is brought back to life when his brain and parts of his face are implanted into a humanoid robotic body, which is outfitted with state-of-the-art weapons, facial recognition, predictive analytics software, and even the ability to record and live stream videos. Although 21st century society might not be building such cyborgs anytime soon, many of RoboCop’s technologies are being used by law enforcement all over the world and have been the subject of intense debates, especially since police departments have been increasingly adopting body-worn cameras as a new crime-fighting tool.

Body-worn cameras are growing in popularity among PDs all over the United States and this trend does not show any signs of slowing down. Trying to guess what new technologies will be adapted in conjunction to these cameras, but there are a few tools that are already being used in certain places and situations that could possibly make their transition to law enforcement activities.

\textbf{Weapon Detection}

On October 1, 2017, Stephen Paddock opened fire on concertgoers attending a country music festival from his room at the Mandalay Bay Hotel in Las Vegas, Nevada. Armed with 10 AR-15 rifles, Paddock took 58 lives and injured over 800 people. Soon, surviving victims filled several lawsuits against MGM and the Mandalay Bay Hotel, arguing both companies did not take proper preventive measures to stop Paddock’s plan.\textsuperscript{219} Since gun control laws in the U.S. might never become a reality and “there are no common security standards across the hospitality


industry [and] the trend has been to prioritize convenience, not increased security," it is becoming apparent that private institutions and companies have to create their own security measures.

Shortly after the Mandalay Bay incident, the Westgate Las Vegas Resort and Casino started testing a weapon-detecting system called Patscan Cognitive Microwave Radar (Patscan CMR) from Canadian security outfit PatriotOne Technologies Inc. The Patscan CMR is “an automated alert system capable of covertly screening moving individuals for on-body concealed weapons (handguns, knives, grenades, explosive vests, etc.),” which combines “short-range radar with machine learning algorithms.” It is safe to say weapon detection systems are no longer a military-exclusive tool.

PatriotOne says that since Patscan CMR does not retain images or data and solely scans individuals, there are no privacy concerns. However, it could arguably raise some privacy issues protected by the Fourth Amendment, which protects individuals from “unreasonable searches and seizures.”

Considering this technology is already available commercially, it would not be unrealistic for companies similar to PatriotOne to start developing a feature or an accessory that could be used with police BWC. If a weapon detection system were to be implemented by the police to work in conjunction with BWC technology and it started saving data, it would require PDs to

---

revise (and in some cases figure out a better strategy) their storage programs and retention policies. A recording of these weapon detection scans would create more video data and metadata that would need to be preserved. State laws would also have to determine if the retention period for such data would be similar to the ones in place for BWC and it would undoubtedly require departments to be more responsible for file deletion.

**Automated Analytics and Predictive Policing**

Automated analytics refers to “instantaneous data retrieval and assessment in the field.” Perhaps the best visualization of this concept was depicted in a scene in 1991’s *Terminator 2: Judgment Day*, where the Terminator (played by Arnold Schwarzenegger) arrives naked at a motorcycle bar. Upon scanning his surroundings, his built-in automated analytics points him to a biker, whose clothes would fit his body. The Terminator then pronounces: “I need your clothes. Your boots. And your motorcycle.”

Predictive policing, which “tries to harness the power of information, geospatial technologies and evidence-based intervention models to reduce crime and improve public safety,” is nothing new. The concept has been around since 2009, when the National Institute of Justice, in partnership with the Bureau of Justice Assistance and the Los Angeles Police Department, held a symposium “to discuss this emerging idea and its impact on the future of policing.” In 2012, the results of a survey conducted by PERF — with the support of Target Corporation and the Office of Community Oriented Policing Services (COPS Office) — showed

---

38 percent of the responding 200 police departments were already using predictive policing, and
70 percent expected to implement a system within the next two to five years.\textsuperscript{230}

PredPol, one of the most popular predictive policing software among police departments
in the United States,\textsuperscript{231} “uses a machine-learning algorithm to calculate its predictions.”\textsuperscript{232} The
algorithm studies information about crime location, type, date, and time present in police datasets
in order to predict high-risk areas for each day of the week.\textsuperscript{233}

Although both automated analytics and predictive policing have raised concerns due to
potential civil liberties implications, software is still being developed and programs are already
being implemented in cities, even if citizens are not aware. An example of such case has been
happening in the city of New Orleans since 2012, where the local police department created a
partnership with Palantir Technologies, one of the most powerful data-mining companies in the
world, to implement a predictive policing program, unbeknownst to the public, city council
members, and attorneys.\textsuperscript{234} Although there is evidence the partnership could have expired in
February 2018,\textsuperscript{235} the current status of the program is unknown.

With such developments already taking place, it would not be surprising if BWC data
started to be implemented in the datasets used by predictive policing software. If so, one can only

\textsuperscript{230} Police Executive Research Forum, “Future Trends in Policing” (Office of Community Oriented Policing
\textsuperscript{231} Ellen Huet, “Server And Protect: Predictive Policing Firm PredPol Promises To Map Crime Before It Happens,”
\textsuperscript{233} Ibid.
\textsuperscript{234} Ali Winston, “Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology,” The
\textsuperscript{235} “Amendment NO.3 to Data Sharing Agreement and License and Service Agreement Between City of New
hope the algorithms used are not as prone to racial bias and inaccuracies as the ones used in facial recognition.

**Biometrics for Data Security**

DNA, retina scans, and fingerprints have been used to identify persons of interest for years, however it is possible that in the future similar biometric information can be used to access restricted data inside a police department. Many private companies, such as Apple, are already using fingerprints and facial recognition in their products, especially with smartphones and tablets. The same technology could be more largely implemented in PDs to increase security around BWC videos stored as evidence and to also facilitate an audit trail. As Maxine Most, a principal at Acuity Market Intelligence, states, with biometrics “you know that the individual accessing secure areas or information is not just an individual holding the proper credential, but is in fact the person who has been granted access.”

As previously mentioned, biometrics are also used for identification purposes. HELIX—a security application for smartphones—locks and unlocks the device by scanning and identifying its owner by his or her ear. Michael Boczek, the President and CEO of Descartes Biometrics, the company behind HELIX, believes biometrics are more stable and reliable than facial recognition, as ear recognition technology has been tested by police departments in Washington state to be used with BWC. "A police officer with a body-mounted camera that sits mid-chest [could] capture images of someone's ear to scan when they approach a driver's window.”

---

The FBI already has a facial recognition database in place and the popularity of people being identified in public if they cross a live-feed video camera is increasing among police departments. In the near future, this practice might become even more commonplace.

Currently, at least five major police departments, including departments in the cities of Los Angeles, Chicago, and Dallas, “have either already used the technology, bought it from a vendor, or have said they’re interested in acquiring it.” However, there are no guarantees these departments are even testing their software for accuracy and this type of surveillance is mostly done in the dark, without a lot of restrain.

It is apparent technology is evolving at lighting speed and legislature is not keeping up with such developments. In an ACLU report, Stanley and Steinhardt state:

In the past, new technologies that threatened our privacy, such as telephone wiretapping, were assimilated over time into our society. The legal system had time to adapt and reinterpret existing laws, the political system had time to consider and enact new laws or regulations, and the culture had time to absorb the implications of the new technology for daily life. Today, however, change is happening so fast that none of this adaptation has time to take place – a problem that is being intensified by the scramble to enact unexamined anti-terrorism measures. The result is a significant danger that surveillance practices will become entrenched in American life that would never be accepted if we had more time to digest them.

Real-Time Face Recognition

“For many of these systems, the inclusion of real-time face recognition is just a software update away,” Harlan Yu.

---

In 2016, a Russian software developer named Andrey Mima announced he had been able to identify people by using a facial recognition application called FindFace, which he called "Shazam for people."\textsuperscript{242} This application, developed by NTechLab, allows people to be identified in real time, something that for many years was considered to be a technology only present in science fiction movies: "It can determine not just who someone is, but where they’ve been, where they’re going, and whether they have an outstanding warrant, immigration detainer, or unpaid traffic ticket."\textsuperscript{243}

If this statement is indeed a representation of what FindFace can do, it would have to be implemented and used in conjunction with local police, state, and federal datasets, which would allow even more possibilities for misidentification and possible indictment of innocent people. Furthermore, its described ability to track where a person has been and where they are going might imply this facial recognition application would also have to rely on cameras installed inside private buildings. As a result, private companies would potentially be able to capitalize on the data they gathered, privatizing information and raising privacy concerns even more.

Still similar technology is already being paired with BWCs and being tested in other parts with the globe. In early 2018, Chinese media from the city of Zhengzhou confirmed the local police has been testing sunglasses and BWCs with built-in facial recognition technology. The sunglasses, which require the officer to "actively take a photograph of a ‘suspicious individual’ in order to run their face through [a facial recognition] database [have] already resulted in the

\textsuperscript{242} Ethan Chiel, “This Face Recognition Company Is Causing Havoc in Russia—and Could Come to the U.S. Soon,” Splinter, April 26, 2016, splinternews.com/this-face-recognition-company-is-causing-havoc-in-russia-1793856482.

apprehension of seven suspects wanted for alleged crimes, and 26 people alleged to have been using false identification.\textsuperscript{244}

Although there are concerns these tools could be used to profile ethnic minorities and track political protesters, China, who is already is a world leader in facial recognition technology, has been determined to build “the world's biggest camera surveillance network.”\textsuperscript{245}

The South China Morning Post reported again in early 2018 between three and four thousand police officers in the country are currently part of a pilot program where BWCs with a built in facial recognition software and 720 degrees field of view are being used.\textsuperscript{246} The cameras are provided by Nebula Science and Technology, a Beijing-based startup founded in 2017, which has also developed 720-degree CCTV cameras, and are “equipped with 4G and Wi-Fi connectivity to link to a central database of facial images,” allowing law enforcement to utilize almost real-time facial recognition.\textsuperscript{247} Shi Pengfei, chief executive of Nebula and a former cameraman for the state broadcaster China Central Television, states these cameras are able to capture higher quality images than the average BWC since it can be attached to the officer’s shoulder avoiding possible blocking from arm movements and once 5G technology becomes more widely available, these cameras will allow the live uploading of video streams. After having its products exhibited during the Technology Consumer Association (CES) 2018


conference in Las Vegas, Pengfei adds: “Soon you won’t need three cameras to monitor an area, you’d just need one camera.”

Rise of Anti-Facial Recognition Devices

Although there are already anti-facial recognition products being sold, if facial recognition does become even more commonplace, there will be an increase in the availability and popularity of these products. Items like the previously mentioned Reflectables eyeglasses and the URME Mask might become staples during protests, especially since some activists already use clothing and hats to protect their faces.

Aside from products designed to foil facial recognition tactics, it is possible for “resistant kits” to also become more popular. Even though it is currently being used as an attempt to spark a debate about resistance, the Backslash kit has caught the attention of many social media users. The kit, which was originally created by Pedro G. C. Oliveira and Xuedi Chen as a Masters thesis at the Interactive Telecommunications Program at New York University, is made of “functional devices designed for protests and riots of the future;” including “a smart bandana for embedding hidden messages and public keys, independently networked wearable devices, personal blackbox devices to register abuse of law enforcement and fast deployment routers for off grid communication.”

In this case, BWC footage would also become a cataloguing tool of future resistance strategies used to fight against surveillance and injustice.

---

Closing Thoughts

Audio-visual technology has greatly advanced over the years and has been used as a vital tool for law enforcement since the 1800s. After the invention of the VHR, video cameras started being installed in public places and even mounted inside police patrol cars, creating respectively CCTV systems and dashcams. As the years went on, technology kept advancing, and in an effort to better the relationship between public and law enforcement, many departments started implementing body-worn cameras to their arsenal.

Although many believed BWCs would be able to build transparency, trust, and accountability by documenting interactions between the public and officers, departmental policies and state legislatures still need to be further developed. My intention with this dissertation was to gather as much information as possible and explore various issues related to video preservation, privacy, and access that still need to be addressed by law enforcement agencies, lawmakers, and even the public.

In “Chapter 1: Recording the Video,” I explored several factors that can influence a law enforcement agency when deciding which BWC brand and model better fits its needs. I also studied several policy handbooks, focusing on the presence, and sometimes omissions, of specific activation and deactivation policies. By doing so, I was able to get a better understanding of how these cameras work and how such policies have a direct effect on storage and privacy.

For “Chapter 2: Preserving the Video,” I focused on retention policies and storage concerns, especially those pertaining to cloud-based services, such as Evidence.com and VIEVU’s Solution. “Chapter 3: Privacy and the Camera” allowed me to explore various aspects of this technology and their direct effect on privacy. Trying to define the idea of privacy alone
was a challenging task and describing how BWC technology can potentially affect one’s sense of self and safety was an exercise in paranoia control.

The “Chapter 4: Access to the Footage” was equally challenging, since state legislations vary greatly. While some states have very specific guidelines determining who has the right to access a BWC video and what processes one must undertake to do so, others leave it up to the courts to decide on a case-by-case basis, while trying to find a balance between public interest, privacy, and investigation needs. Finally, “Chapter 5: What Does the Future Look Like?” gave me a chance to look at other technological advances and hypothesize how they could be implemented with BWCs.

Writing this dissertation was a challenging undertaking. Not a day goes by where a new article or study on BWC technology is released to the public, and sometimes they generate new ideas or even weaken a previous argument. Part of me wanted to answer all questions, but it soon became clear that, currently, not even experts and lawmakers can do so. In fact, I am not even sure we will ever figure out the most appropriate way to handle the preservation, access, and privacy issues surrounding BWCs. However, one thing is for certain: technology will keep advancing and it necessary for policies and legislation to catch up. Nobody wants to be living inside a real-life episode of *Black Mirror.*
Glossary

ACLU: American Civil Liberties Union

BJA: Bureau of Justice Assistance

Bodycam: Body-worn camera

BWC: Body-worn camera

CAD: Computer-Aided Dispatch

CBP: U.S. Customs and Border Protection

CJIS: Criminal Justice Information Services

COPS Office: Office of Community Oriented Policing Services

Dashcam: Dashboard camera

DOJ: Department of Justice

FOIA: Freedom of Information Act

IACP: International Association of Chiefs of Police

ICE: U.S. Immigration and Customs Enforcement

LCCHR: Leadership Conference on Civil and Human Right

NAACP: National Association for the Advancement of Colored People

NIJ: National Institutes of Justice

OJP: Office of Justice Programs

PD: Police Department

PERF: Police Executive Research Forum

RMS: Records Management System

SOS: Office of the Secretary of State, a section of the Washington State Archives
List of Figures

Figure 1. Evelyn Manesta by Criminal Record Office...........................5
Figure 2. “Movie Camera in Police Car Puts Evidence on Film”....................9
Figure 3. Axon’s Plans and Pricing.........................................................40
Figure 4. Axon’s Plans Details...............................................................41
Figure 5. Release of BWC footage, Graph 1........................................51
Figure 6. Release of BWC footage, Graph 2........................................64
Figure 7. Over-redacted preview of AXON_Body_Video_2015-02-18_0533......65
Figure 8. Concentric Circles of Privacy..................................................75
Figure 9. URME Personal Surveillance Identity Prosthetic........................76
Figure 10. Some of Harvey’s CV Dazzle patterns....................................77
Bibliography


https://www.axon.com/info/offer.

“A Model Act for Regulating the Use of Wearable Body Cameras by Law Enforcement.”


“ACLU Urges Justice Department to Investigate Police Use of Face Recognition.”


washington-state-university-to-further-ground-breaking-research-on-police-community-interactions-300477257.html.


https://www.washingtonpost.com/posteverything/wp/2017/06/01/bodycams-are-key-for-police-accountability-we-cant-let-them-erode-privacy-rights/.

Dwyer, Terrence P. “To Record or Not to Record: When Should Cops Turn on Their Body Cameras?” PoliceOne, September 21, 2017. https://www.policeone.com/policing-in-the-video-age/articles/421461006-To-record-or-not-to-record-When-should-cops-turn-on-their-body-cameras/.


https://www.staff.ncl.ac.uk/daniel.nettle/ernestjonesnettlebateson.pdf.


Goudie, Chuck, Barb Markoff, and Christine Tressel. “Officers File Lawsuit After Body
Cams Record Them Non-Stop.” ABC7 Chicago, June 23, 2016.
http://abc7chicago.com/1399056/.

Greene, Susan, and Miles Moffeit. “Room for Error in Evidence Vaults.” The Denver Post,
vaults/.

February 24, 2018.
http://www.policemag.com/channel/technology/articles/2016/04/the-body-cameras-
police-use.aspx.

http://www.policemag.com/channel/technology/articles/2017/04/lessons-learned-from-
body-cam-users.aspx.

“’Hackathon’ Asks Techies to Aid SPD on Sensitive-Video Issues.” The Seattle Times,
December 14, 2014. https://www.seattletimes.com/seattle-news/lsquohackathonrsquo-
asks-techies-to-aid-spd-on-sensitive-video-issues/.

“Hackers Hijacked These Law Enforcement Computers for Ransom.” PBS NewsHour,
October 13, 2016. https://www.pbs.org/newshour/nation/hackers-hijacked-law-
enforcement-computers-ransom.

“Half of All American Adults Are in a Police Face Recognition Database, New Report
https://www.law.georgetown.edu/news/press-releases/half-of-all-american-adults-are-


Horton, Alex. “After Stephon Clark’s Death, New Videos Show Police Muted Body

http://www.predpol.com/how-predictive-policing-works/.

Huet, Ellen. “Server And Protect: Predictive Policing Firm PredPol Promises To Map Crime

Hung, Vivian, Steven Babin, and Jacqueline Coberly. “A Market Survey on Body Worn


“Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned.”
2014/body_worn_camera_program.asp.

“Interactive Directives Guide - Body Worn Camera (BWC).” Charlotte-Mecklenburg Police
Department, April 29, 2015.

Interview with Officer A. Interview by Caroline Oliveira. Phone, April 6, 2018.
Interview with Officer C. Interview by Caroline Oliveira. Email, April 7, 2018.


McKee, Stuart. “Is the Cloud Ready for Body-Cam Video? (Industry Perspective).”

McMullan, Thomas. “What Does the Panopticon Mean in the Age of Digital Surveillance?”


Mire, Sam. “Chinese Police Testing Facial Recognition Body Cameras, Glasses.”

“Movie Camera in Police Car Puts Evidence on Film.” Popular Science, September 1939.

http://eprints.lse.ac.uk/62319/1/_lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Mulcahy,L_Docile%20suffragettes_Mulcahy_Docile%20suffragettes_2015.pdf.


Newman, Lily Hay. “Cops Have a Database of 117M Faces. You’re Probably In It.”


“NYPD Response to Public and Officer Input on the Department’s Proposed Body-Worn Camera Policy.” New York City Police Department, April 2017.


Southall, Ashley. “New York Police Union Sues to Stop Release of Body Camera Videos.”


http://spdblotter.seattle.gov/2015/02/25/spd-launches-youtube-channel-for-bodyworn-video/.


Stanley, Jay. “Lessons From the Minnesota Shooting Body Camera Activation Failure.”


Zercoe, Cole. “When Should Police Departments Release BWC Footage to the Public?”
