AN ANALYSIS OF TRADITIONAL SPORTS STADIUM SECURITY AND FACIAL RECOGNITION BIOMETRICS TOWARDS THE PREVENTION OF CRIME AND VIOLENCE IN SPORTS ARENAS

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

DOCTOR OF PROFESSIONAL STUDIES

to the faculty of the

DIVISION OF CRIMINAL JUSTICE AND HOMELAND SECURITY

of

THE LESLEY H. AND WILLIAM L. COLLINS
COLLEGE OF PROFESSIONAL STUDIES

at

ST. JOHN'S UNIVERSITY
New York
by
Darnell R. Downes

Date Submitted 3/20/2024 Date Approved 3/20/2024

Darnell R. Downes

Dr. James O'Keefe

ABSTRACT

AN ANALYSIS OF TRADITIONAL SPORTS STADIUM SECURITY AND FACIAL RECOGNITION BIOMETRICS TOWARDS THE PREVENTION OF CRIME AND VIOLENCE IN SPORTS ARENAS

Darnell R. Downes

This qualitative descriptive study sought to determine how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast of the U.S. The problem that was addressed in the study is that despite the increase in violence and crime in sports stadiums and the use of biometric systems, it is not known how stadium security managers perceive and describe their experiences with biometric systems in mitigating crime and violence in and around sports stadiums on the east coast of the U.S. Interviews with 20 security managers representing major sports arenas located on the east coast of the U.S. were included. The interviews demonstrated that facial recognition technology is a significant and effective strategy for enhancing security systems at sports stadiums by security managers. Understanding security managers' perceptions and attitudes may help implement facial recognition strategies in safeguarding sports stadiums. While crime and violence can never be eliminated, we can take additional steps to counter it.

DEDICATION

Praise be to God who orchestrated my path to the road it is today. Sometimes, I doubted if becoming a doctor was achievable; you led my path and kept me going. It is you, the alpha and omega of my life. For the many blessings bestowed upon me, I am grateful and humble.

I want to dedicate this dissertation to my mother, Gillian Downes. Her investment in me emotionally, spiritually, and at times financially, was formative for the person I am today. I would not be who I am today without her constant love and support. Education was always a priority in our home, and this dissertation would not have come to fruition without her encouragement and guidance.

To my entire family, I want to express my gratitude for your support throughout the years and your belief in me through all the ups and downs. To my uncles, Dion and Dexter Thomas, your work in academia is what initially inspired this career path. Your support and wisdom cannot be expressed in words. Thank you.

To my beautiful children Skylar, London, and Chase Valor. May this completion be a witness to the power of persistence, sacrifice, dedication, and faith. I pray that you all come to see that education is a means to serve those in the world, not a means to make you feel above the world.

ACKNOWLEDGEMENTS

I would first like to express my sincere appreciation to my chair, Dr. James O'Keefe, for his academic guidance and enthusiastic encouragement throughout my course of study in the DPS program. Further, without his continuous support, this dissertation would not have been completed. I am blessed to have Dr. O'Keefe as my chair and feel honored to have had a chance to work with him. Thank you, Dr. O'Keefe.

I would like to thank my committee members. Dr. Christopher Mercado for guiding and supporting me over the last four years. I greatly appreciate his insight and input throughout my DPS program. I would also like to thank Dr. Andrew Costello for his constant enthusiasm. I deeply appreciate his valuable discernment in completing my DPS program and this dissertation.

Lastly, I would like to thank Dr. Bernard Jones for providing any assistance requested. Your discussion, ideas, and feedback have been invaluable. Thank you, Dr. Jones, for your patience throughout the entire process. I wish you all continued success!

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Research on the prevalence of crime and violent acts during sports activities in and outside of sporting events has been associated with the aggressiveness of fans and the opportunistic behavior of criminals. Lange and Young (2019) examined gender-based violence and crime in sports activities and found that gender-based violence and vandalism of property during sporting events were associated with male masculinity and the assumption that violence was an important culture in sports. Similar findings were reported by Vandeviver et al. (2019), who stated that engaging in violent activities that often paved the way for criminal activities such as theft and burglary was partly due to the assumption that violence was part of the male orientation. Other researchers have found that gender is a common issue in male violence (Marganski, 2019; Van Valkenburgh, 2021). Researchers have also delved into the widespread global misogyny and male supremacy in patriarchal society to explain violence (Brandt, 2023; MacKenzie, 2023). Misogyny is intertwined with male domestic violence because it is common for mass murderers to commit femicide before mass murders (MacKenzie, 2023; Marganski, 2019).

Violence and crime in sporting events taint sporting activities and interfere with sports' value to a community and areas surrounding sporting stadiums and complexes. Brosnan (2019) demonstrated that sporting activities and sports stadiums improved the economy and economic value of the people in the surrounding areas. Brosnan (2019) reiterated that sporting activities increased commercial activities that created employment for people and subsequently improved the economic activities of the surrounding areas.

Crime and violence associated with sports discourage the development of commercial and economic activities in the areas surrounding the stadiums. Moreover, criminal and violent activities discourage fans from participating in sports activities, reducing government funding and constructing resources such as stadiums to support sporting activities (Vandeviver et al., 2019).

Therefore, given the negative impacts of crime and violence on sports and surrounding communities, this study explored how stadium management has employed technology to mitigate crime and violence in and outside the stadiums. The following sections will be covered in this chapter: background to the problem, problem statement, purpose statement, research questions, theoretical framework, nature, and significance of the study.

Background of Study

The need to mitigate crime and violent attacks in sports stadiums in the United States is informed by violent occurrences during sports activities across the world and in the United States. Among the key occurrences, the researcher cited the research conducted by Yusoff et al. (2020), who examined the impacts of the Munich attack in 1972, where Israeli athletes were attacked and killed. In 1972, the Munich massacre was an attack during the Summer Olympics in Munich, West Germany, by eight members of the Palestinian terrorist group Black September. After killing two more athletes, Black September took nine members of the Israeli Olympic team hostage. It was called "Operation Iqrit and Biram" (Sylas, 2006), after two Palestinian Christian villages whose inhabitants were expelled by Israel Defense Forces (IDF) during the 1948 Arab-Israeli War. The Black September's commander was Luttif Afif, the negotiator. West German

neo-Nazis gave the group logistical assistance. Shortly after the hostages were taken, Afif demanded the release of 234 Palestinian prisoners in Israeli jails and the West German-held founders of the Red Army Faction, Andreas Baader and Ulrike Meinhof. Five of the eight Black September members were killed during a failed attempt to rescue the hostages. A West German police officer was also killed in the crossfire.

The three surviving perpetrators, Adnan Al-Gashey, Jamal Al-Gashey, and Mohammed Safady were arrested. The next month, however, following the hijacking of Lufthansa Flight 615, the West German government released them in a hostage exchange. The Israeli government launched Operation Wrath of God, which authorized Mossad to track down and kill those involved in the Munich massacre. Two days before the start of the 2016 Summer Olympics, in a ceremony led by Brazilian and Israeli officials, the International Olympic Committee honored the eleven Israelis and one German who were killed in Munich. In the United States, the attacks during the 1996 Atlanta Olympics and the 2013 Boston Marathon bombing necessitated heightened security around the stadiums to mitigate against such violent attacks and preserve the lives of fans attending the sporting events.

Besides the massive bombing attacks on stadiums in Munich, Atlanta, and Boston, research also suggests that other forms of violence and crime, such as mugging, theft, burglary, and hooliganism, support the need for enhanced stadium security. Ristea et al. (2020) conducted a spatial analysis of criminal activities in football stadiums using georeferenced tweets. Employing exploratory and inferential analysis, the researchers identified criminal damage, violence against other fans, theft, and mishandling via tweets that often occurred in sporting stadiums (Ristea et al., 2020). Engelberg and Moston

(2020) investigated crime and misconduct in sports by reviewing published literature. The findings revealed that many hardcore football fans engaged in violent and aggressive behaviors inside the stadium, including fist-fighting and threatening players and other fans. Though the incidences are rare, they are often considered criminal, hence the need for enhanced security.

Sporting activities are regarded as sources of crime in cities with stadiums. Pyun and Hall (2019) investigated whether professional football increased crime in Pontiac, Michigan. In the quantitative comparative research, Pyun and Hall (2019) demonstrated that football games increased cases of vandalism and larceny in Pontiac. Mares and Blackburn (2019) investigated the relationship between Major League Baseball and crime at St. Louis Cardinal games in the United States. They found increased cases of motor vehicle thefts, vandalism of property, minor assaults, and robbery inside and around the immediate vicinity of the stadium. In a different study, the impact of game day on crime reported that game day was associated with heavy alcohol consumption that increased the likelihood of students engaging in criminal activities such as vandalism, violence against persons and property, and traffic offenses (Menaker & Sheptak, 2020). Thus, based on the reviewed studies, sporting events have increased crime rates in and around the stadium's immediate vicinity.

The findings that sporting events have increased cases of crime in and around stadiums have led to research on crime mitigation strategies in stadiums. Stadiums have adopted a multifaceted strategy to ensure security and spectator safety to lessen fear and anxiety associated with violent crimes (Rakhmanova et al., 2022). Stadiums have

deployed physical security measures like metal detectors, wands, and CCTV to monitor visitors' actions (Rakhmanova et al., 2022).

Copus and Laqueur (2019) investigated whether entertainment during sporting events prevented crime during Chicago sports games. Supporting the preceding findings of Copus and Laqueur (2019), Kurland (2019) investigated arena-based events and crime during sports and found that arena-based sports activities such as basketball games, boxing, and mixed-martial arts reduced cases of robbery and associated crime.

Kurland (2019) found evidence of a shift in crime and security incidents on Hockey game days compared to non-game days in the region around the Prudential Center in Newark, New Jersey, and in locations (and street segments) approximately 5km distant. The results indicate aggravated assault, robbery, theft, and car theft. Citywide and downtown games and vehicle theft and burglary crimes varied greatly on game days compared to non-game days. Event security plan developers should conduct a venue-specific study on crime and security issues to strategically allocate resources because, without empirical evaluations, they risk jeopardizing the lives of spectators (Kurland, 2019). These findings coincide with Block and Kaplan's (2022) and Mares and Blackburn (2019) findings.

The first major-league baseball club research reveals considerable spikes in crimes on home game days for the St. Louis Cardinals (Mares & Blackburn, 2019). After adjusting for attendance and game length, this study revealed increased crime during game days, including thefts, assaults, disorderly behavior, and property damage. This is especially true surrounding the stadium, but citywide violence has also increased. This study also compares game times and games against its traditional adversary, the Chicago

Cubs (Mares & Blackburn, 2019). Furthermore, while investigating the impacts of sports on young people, it was found that sports transformed their behaviors and discouraged them from engaging in crime (Morgan et al., 2019).

The security of sports stadiums is a significant concern, especially with increased crime and violence inside and around the sports stadiums. To prevent crime and violence, technology and digital inventions are of significant use in stadiums and sporting complexes as effective in deterring crime and violent behaviors (Hutchins & Andrejevcic, 2021). In the digital mitigation of crime in stadiums, cameras are frequently used because they are readily available and less costly. Cameras are also considered less intrusive and more effective than physical security, which is why many stadiums have adopted them in the United States and around the world.

Modern and innovative security systems, such as closed-circuit television (CCTV) and facial recognition, have also been adopted to increase security in and around stadiums while mitigating crime. Biometrics technologies offer a very effective and practical solution to this problem. Facial Recognition enables real-time checking of all spectators entering or leaving at any time without stopping the activities inside the facility (Hutchins & Andrejevcic, 2021). Evidence of biometric use in stadiums has also been captured by Flicker (2019), who reported that using biometric technology at stadium entrances in arenas such as Madison Square Garden increased the safety of spectators and athletes. However, Flicker identified issues associated with the risks of data breaches, privacy, and inaccuracies related to facial recognition technology. Additional evidence of biometric technology use in stadiums was reported by Dauvergne (2022), who investigated the globalization of facial recognition technology. Facial recognition

technology enhanced the security of stadium fans and athletes by deterring crime and other violent behaviors (Dauvergne, 2022).

Although researchers have evidence of the use of cutting-edge technology, such as biometric systems in sports stadiums as a means to enhance security, there is a gap in the literature concerning how stadium managers describe and perceive the use of biometric technology systems to mitigate crime in stadiums on the east coast of the U.S., which will be the primary research area to address the research question.

Theoretical Framework

Grant and Oslanoo (2014) described the theoretical framework as the blueprint that guides how the ideas of a study are related. Furthermore, McChesney and Aldridge noted that the chosen theoretical framework must be reflected in the methods and overall decisions of the specific study (McChesney & Aldridge, 2019). The theoretical framework used for this study is the Technology Acceptance Model (TAM) developed by Davis et al. (2023). TAM emphasizes users' perceptions of a particular technology influenced by perceived usefulness and ease of use. TAM will be useful in the study as it will help the researcher describe and understand the perception of sports stadium security managers regarding using biometric facial recognition software to deter crime and violence during sporting activities using TAM's major concepts of perceived usefulness and perceived ease of use. Perceived ease of use asserts that individuals will accept and use technology if they perceive it to be easy to use (Davis et al., 2023). Davis et al. (2023) established that individuals would use technology if limited effort is required to use technology. The second concept, perceived usefulness, examines individuals' perception of the technology being effective and enhancing job performance (Davis,

2023). Individuals will adopt and use certain technology if they perceive it to improve their performance and productivity. Thus, TAM will be useful in understanding security managers' perceptions and the use of biometric facial recognition software.

Statement of Problem

The problem that was addressed in the study is that despite the increase in violence and crime in sports stadiums and the use of biometric systems, it is not known how stadium security managers perceive and describe their experiences with biometric systems in mitigating crime and violence in and around sports stadiums on the east coast. Biometrics is nothing new to professional sports teams and their home stadiums, arenas, and ballparks. Currently, the most common form of biometrics used in sports arenas is fingerprint biometrics. This is driven in large part by the recent 2018 partnership between Major League Baseball ("MLB") and biometrics technology vendor CLEAR—whose biometric screening technologies are also commonly seen in airports around the world. At the same time, other professional sports franchises have also started integrating facial recognition systems into their home venues' operations.

Previous researchers have reported that sports activities have been associated with increased cases of crime and violent behaviors. Menaker and Sheptak (2020) found that game day in universities elevated cases of crime and vandalism of property within and around the university stadiums. Similar findings were reported by Mares and Blackburn (2019), who demonstrated that Major League Baseball games increased crime cases, including motor vehicle thefts and vandalism of properties. Jakar and Gordon (2022) who reported consistent findings, said that increased police checks and patrol during major leagues in the United States were associated with the possibility of crime and

violent behaviors from fans.

With the increased probability of crime due to sports activities, several mitigation strategies have been adopted by managers and caretakers of sports stadiums. Copus and Laqueur (2019) demonstrated that including entertainment during sporting events reduced cases of crime and violent behaviors from young people.

Copus and Laqueur (2019) investigated whether entertainment during sporting events prevented crime during Chicago sports games. Supporting the preceding findings of Copus and Laqueur (2019), Kurland (2019) investigated arena-based events and crime during sports and found that arena-based sports activities such as basketball games, boxing, and mixed-martial arts reduced cases of robbery and associated crime.

The notion that mass media might be accountable for aggressive and illegal conduct is pervasive. Copus and Laqueur (2019) stated its diversionary role has received very little study. The authors examined the impact of television entertainment on crime rates by using the inherent unpredictability in the scheduling of athletic events. A comparative analysis was conducted of crime reports in Chicago during the half-hour when Chicago's sports teams are engaged in games, as opposed to the same time, day, and month when the teams are not playing. Identical analyses were conducted for the Super Bowl, National Basketball Association Finals, and Major League Baseball World Series. Copus and Laqueur (2019) found a continuous decline in criminal activity during the occurrence of games. Short-term crime displacement is negligible or non-existent.

Kurland (2019) found evidence of a shift in crime and security incidents on Hockey game days compared to non-game days in the region around the Prudential Center in Newark, New Jersey, and in locations (and street segments) approximately 5km

distant. The results indicate aggravated assault, robbery, theft, and car theft citywide and downtown games and vehicle theft and burglary crimes varied greatly on game days compared to non-game days. Event security plan developers should conduct a venue-specific study on crime and security issues to strategically allocate resources, as without empirical evaluations, they risk jeopardizing the lives of spectators (Kurland, 2019). These findings coincide with those of Block and Kaplan (2023) and Mares and Blackburn (2019).

The first major-league baseball club research reveals considerable spikes in various crimes on home game days for the St. Louis Cardinals (Mares & Blackburn, 2019). After adjusting for attendance and game length, this study revealed an increase in crime during game days, including thefts, assaults, disorderly behavior, and property damage. This is especially true surrounding the stadium, but citywide violence has also increased. This study also compares game times and games against its traditional adversary, the Chicago Cubs (Mares & Blackburn, 2019). Furthermore, while investigating the impacts of sports on young people, it was found sports transformed the behaviors of young people and discouraged them from engaging in crime (Morgan et al., 2019).

McGovern (2023) examined the potential correlation between different types of crimes and days when the Boston Red Sox had home games. This study did not yield substantial evidence, similar to the findings of Mare and Blackburn (2019), indicating that home games lead to a rise in anticipated property crimes. However, the researcher did establish a significant correlation between home games and an increase in expected minor assault charges, specifically Disorderly Conduct and Simple Assault. Boston had a

far lower anticipated rise in general criminal activity in contrast to the research conducted by Mare and Blackburn (2019) on St. Louis (15%) (McGovern, 2023).

McGovern (2023) recommended policy aimed at mitigating the influence of MLB games on crime should largely concentrate on managing the crowd near the stadium to decrease instances of Disorderly Conduct and Simple Assault charges in the surrounding region. Implementing regulations about alcohol sales during sports is expected to decrease the probability of minor assault charges. McGovern (2023) concurred with Mare and Blackburn's (2019) suggestions to enhance the monitoring of stationary cars since they seem particularly vulnerable during sporting events. Notifying onlookers to park their vehicles in places with strong supervision and conceal their things might potentially reduce property crimes during game days (McGovern, 2023). While further investigation is required, the absence of a rise in property crimes in Boston on game days is likely due to the presence of robust surveillance measures for personal belongings. This successful outcome should be pursued as a model for other large cities (McGovern, 2023).

Mass events, especially noteworthy soccer matches, can lead to stadium violence (Gardocka & Jagiełło, 2022). Crimes involving these activities often use ambiguous language (e.g., another dangerous tool, similarly dangerous behavior) and prioritize prohibitions over societal harm. In the stadium or during organized transport to the event, it is illegal to carry a knife or machete, move between crowd sectors, or cover your face. Fan registration and stadium entry photos are stored for identification. Stadium crimes and petty offenses result in a ban on participation and a forced appearance before the police unit at specific sporting events (Gardocka & Jagiełło, 2022).

To enter the stadium, individuals must agree to restrictions on their own freedom. In these cases, criminal rules should consider a careful description of the criminalized act and the potential to prove its commission (Gardocka & Jagiełło, 2022). Due to the presumption of innocence, extensive forensic recognition procedures are used in such cases, and the stadium audience is fully monitored. However, expedited recognition reduces trial time and limits court evidence. Fans understand that entering the stadium consents to a privacy breach. According to the concept that no harm is done to the willing, the proven success of the legal measures implemented does not warrant constitutional questioning (Gardocka & Jagiełło, 2022).

Unlike Copus and Laqueur (2019), Rakhmanova et al. (2022) established that stadiums adopted a multifaced security approach that included technological and physical surveillance to increase security and deter crime. The standard technologies adopted were closed-circuit television (CCTV) and biometric security systems. While investigating the use of technology in improving stadium security, biometric security systems deter crime by increasing surveillance and recognition of perpetrators through facial recognition software (Hutchins & Andrejevcic, 2021). In previous research, Flicker (2019) established that despite the risks associated with data security, biometric security systems improved security in sports arenas.

Although researchers have evidenced the use of biometric systems to secure sports stadiums and arenas, they have yet to investigate how stadium managers perceive and describe their experiences with biometric security systems to mitigate crime and violent behaviors in their respective stadiums. For example, in Europe, soccer fans who throw their drinks or otherwise disrupt games are sometimes banned. If they try to sneak

in, they may have to contend with a facial recognition system at the stadium (Janofsky, 2019).

Danish club Brondby IF installed security cameras and software developed by Japan-based electronics firm Panasonic Corp. in mid-July at its stadium on the outskirts of Copenhagen. The club uses the system to spot banned fans from a blacklist of about 50 to 100 people each game in a crowd that can reach 25,000. In 2017, Danish authorities issued criminal charges against 44 people following violent clashes during a match between FC Copenhagen and Brondby IF at the stadium. The club uploads photographs of banned visitors into a computer before a game and stations one person in a security room to watch for alerts. The system uses machine learning to spot guests whose faces match the uploaded photographs. If a match is detected, a security guard is sent out to ask the guest to leave (Janofsky, 2019).

Investigating how security managers of sports stadiums describe the use of biometric systems will help its widespread adoption and use to prevent crime and violence in and outside sports stadiums. However, failure to mitigate against crime and violent behaviors in sports stadiums following sporting activities will impact not only the proliferation of sports but also commercial and economic activities in the areas around sports stadiums.

Purpose of the Study

The purpose of the qualitative descriptive research was to explore how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast of the U.S. A convenience sampling technique was

used to recruit 20 participants for the qualitative study. The data sources were semi-structured interviews that will help the researcher collect data critical to reporting security managers' perceptions and experience with facial recognition software to prevent crime and violence in sports arenas. Braun and Clarke's (2006) thematic analysis steps will analyze the collected data.

Research Questions

The following questions were used to address the identified study problem and the purpose of the study:

RQ1: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the east coast of the U.S.?

RQ2: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the east coast of the U.S.?

RQ3: *Perceived Ease of Use (PEU)* Will learning to operate facial recognition technology in stadiums be challenging for security managers?

RQ4: *Perceived Usefulness (PU)* How will this technology at stadiums improve security managers productivity?

Nature of the Study

This study used a qualitative research methodology with a descriptive research design. Researchers use qualitative research methodology to investigate a phenomenon or problem using participants' experiences, views, and perceptions (Yin, 2015). Qualitative researchers collect and analyze non-numerical data to gain an in-depth understanding of a

particular problem. Qualitative research was appropriate for this study because the researcher sought to understand how security managers at sports stadiums described their experiences and perceptions of biometric facial recognition software in preventing crime and violence in and around sports stadiums. While it is anticipated that many of the managers might not have the necessary expertise or experience with cutting-edge technology, exploring how they perceive the effectiveness of biometric systems will aid in deciding the state of technology on east coast stadiums. Alternative research methodologies, including quantitative and mixed-methods research, will also be explored for suitability and use in achieving the purpose of the research.

In terms of research design, a descriptive research design was used to address the problem and purpose statements. Researchers use descriptive research designs to systematically and accurately describe facts and characteristics associated with a particular phenomenon of interest (Dulock, 1993). Researchers use descriptive research to account for situations and phenomena being investigated. In the study, descriptive research design was used to provide a clear and in-depth description of crime and violence in sports stadiums as well as security managers' perception and description of the effectiveness of biometric facial recognition software to mitigate crime and violence in sports stadiums on the East Coast of the U.S.

The target population for the study was 20 security managers in sports stadiums on the east coast. A purposive sampling technique was used to recruit 20 sports stadium security managers. Semi-structured interviews were used as sources of data. The interviews were expected to last 60 minutes. The collected data was analyzed using thematic analysis.

Significance of the Study

This qualitative study aimed to explore the effectiveness of facial recognition security protocol in deterring crime and violent behaviors in and around sports stadiums on the East Coast. Thus, researching the perceptions and attitudes of security managers regarding the use of facial recognition at sports stadiums may assist the security personnel in offering the most excellent level of security and distributing government funding and resources, such as facial recognition software, to safeguard sports stadiums during various gaming activities. Pistone et al. (2019) established that understanding the perceptions and attitudes of security managers on using facial recognition technology may assist law enforcement officials in creating policies and allocating resources for adopting facial recognition technology.

Facial recognition technology is still developing, giving law enforcement and the private sector, such as sporting stadiums, further applications (Hutchins & Andrejevcic, 2021). Law enforcement officers can use the research findings to understand the use of technology in tracing and detecting terrorism activities to protect the people in sports stadiums (Hutchins & Andrejevcic, 2021). The research results will help security managers implement policies in adopting and using facial recognition to safeguard sports stadiums. In enhancing stadium security, the security managers could use the research findings to guide the security operations around the sports stadiums. Police enforcement may better prevent and investigate crime, violent acts, and improve stadium safety using facial recognition software technology (Tóth, 2021). Facial recognition is the most potent and relevant AI biometric technology (CyberLink, 2022). It has vast abilities and can carry out several tasks beyond face detection and recognition. The more robust and

feature-forward a facial recognition platform, the more benefits and fewer biases it brings. Facial recognition biometrically identifies facial vectors and features, matching them with pre-enrolled individuals. The technology leverages proprietary AI algorithms and mathematical equations to create an individual's template by measuring facial variables – nose depth and width, forehead length, and eye shape (CyberLink, 2022). Facial recognition then compares the generated template with existing templates in a database. If there is a match, it can confirm an individual's identity.

By drastically shortening the time required by first responders and investigators to yield leads and identify suspects, the research findings on facial recognition technology can be employed by security managers in circumstances where a suspected criminal act is about to occur or is already in progress, especially at sports stadiums with a huge gathering of spectators watching the games (Tóth, 2021). This can speed up response times, prevent or lessen the damage caused by such attacks, and ultimately save lives at sports stadiums.

Understanding security managers' perceptions and attitudes may help implement facial recognition strategies in safeguarding sports stadiums. The research regarding security managers' attitudes and perceptions about facial technology triggers the need for its adoption and implementation at sports stadiums (Lynch, 2020). Given the widespread issues regarding violence at sporting events and stadiums, the research findings may help to understand whether extreme violence may be decreased through enhanced crowd control techniques mixed with the latest in surveillance and security technologies.

CHAPTER 2: LITERATURE REVIEW

This chapter includes a review of the existing academic literature that provides a foundation for the relevance of this project's topic. This chapter addresses questions related to sports stadium security methods (generally) and the specific use of facial recognition biometric technology. It will facilitate a better understanding of the nature and extent of the person-to-person violent threats and crimes facing sporting arenas. It will specifically discuss facial recognition and how it may play a role in stadium security in large venues. Sporting events, like any major gathering, have no choice but to monitor fans in the name of safety. A big stadium can fit 100,000 people, and global events such as the World Cup and the Olympic Games draw far more visitors—they are explicit targets. With such big crowds, violent outbreaks and acts of terror could have nightmarish consequences. This chapter presents literature on sports arenas, crime, and violence in sports arenas and related security systems installed to ensure fans' and athletes' safety.

Sports events are integral to most cultures, and millions of spectators attend such events annually. Providing a safe, secure environment for patrons and fans is critical. Subsequently, individuals, agencies, and private contractors face the significant challenge of providing a safe environment and enjoyable experience for fans paying to attend and watch such games from sports arenas. The sports industry has embraced best practices and technological tools to aid their efforts. Still, law enforcement recognizes that professionals in the field lack access to new knowledge and experience using the latest technology in the field of sports to ensure security and safety in different sporting events.

Theoretical Framework

Since the development of the Internet and subsequent advancement in technology, security has become a major concern at personal and corporate levels around the world. Research has demonstrated that as much as technology is a security threat, technological and digital developments are critical in enhancing security. Miraz and Ali (2020) investigated the integration of the Internet and blockchain technology to enhance digital security. Blockchain technology is a way of storing and sharing data securely and transparently across a network of computers. It uses cryptography and consensus to create a shared, immutable ledger of transactions and assets. The analysis of merging the two forms of technology revealed an enhanced security system with limited security risks. Similar findings were reported by Choudhary et al. (2019), who investigated the convergence of blockchain and IoT in systems security. Integrating blockchain technology and IoT has positively influenced individual adoption and use of technology to enhance systems and data security. In sports stadiums and sporting activities, Yang and Cole (2020) investigated smart stadiums in the United States, focusing on technology and sports. The analysis of the collected data revealed that smart stadiums employed a wide range of technologies to enhance the security and protection of fans and security personnel.

Technology Acceptance Model

The technology acceptance model can best describe the significance of technology in promoting stadium security (Davis, 2023). TAM, proposed by Davis et al. (2023), identifies and describes two key factors influencing individual acceptance and potential use of a particular technology. The two factors include a) perceived usefulness

and b) perceived ease of use. Researchers use the TAM model to describe and explain the perception of individuals regarding their potential use of technology. While describing the model, Davis et al. (2023) noted that for technology to be accepted and used by a potential user, both the developer and user must share the belief that the developed technology is useful and easy to use.

As illustrated, the key concepts of the technology acceptance model are perceived usefulness and perceived ease of use. The perceived usefulness of the technology acceptance model is defined as the extent to which individuals or organizations believe that using a given technology would improve their productivity and job performance (Davis et al., 2023). The second concept of TAM is the perceived ease of using a particular technology. Davis et al. (2023) described perceived ease of use as the extent to which a person believes using a particular technology would be effortless. Users are likely to accept and use technology systems that are easy, less complex, and require minimal effort to install and use. In the current study, security managers of the selected sports stadiums on the east coast are likely to accept and allow the installation and use of biometric facial recognition systems to enhance stadium security based on the ease of the use of systems and perceived usefulness (Davis, 2023).

Different studies in extant literature have reviewed the usefulness and perceived ease of use of TAM. In one such study, Mailizar et al. (2021) examined the behavioral intention of students to adopt e-learning during the Covid-19 pandemic. Using a student sample of 109, the study revealed that many students were guided by the perceived educational benefits a specific technological software will have. Unlike Mailizar et al. (2021) but with similar results, Su and Li (2021) investigated the application of TAM by

new entrepreneurs in online entrepreneurship education. The results indicated that entrepreneurs' attendance of online education was influenced by perceived ease of use and perceived usefulness of the online technology and software used.

Concurrent with the current qualitative study, Norfolk and O'Regan (2020) investigated biometric technologies at music festivals using TAM. The results indicated that the system's privacy, compatibility with other security systems, and convenience influenced biometric systems' perceived usefulness and ease of use. Comparable findings were reported by Liu et al. (2021), who researched face recognition and privacy using data from 518 questionnaires. The quantitative data analysis revealed that while perceived ease of use had no significant impact on individual decision to use face recognition software, perceived usefulness associated with accuracy and perceived enhanced security influenced the positive use of facial recognition systems. Therefore, besides helping the researcher describe the perception of security managers regarding facial recognition software, TAM will help formulate questions for semi-structured interview discussions. This will ensure an extended understanding of security managers' perceptions, experiences, and use of biometric facial recognition software for enhanced stadium security on the East Coast.

Review of Literary Themes

Overview of Violence Among Football Fans

Both verbal and physical violence are reported in many football and soccer games. Yusoff et al. (2020) and Leitner and Richlan (2021) said that violent activities among football fans include beating others, intimidation, and other terrorizing activities. The violence perpetrated by football fans results from drug and alcohol abuse, conflicts in

an individual's family, and sometimes poverty (Van Ham et al., 2019). Yusoff et al. (2020) defined aggression or aggressive behavior in sports as disrespectful to fans of the opponent team, match officials, or athletes.

In sports, aggressiveness, and violence can be through physical or verbal altercations between or among fans. Newson (2017) stated that advancing toward the opponent or the referee to hurt or make them scared exemplifies some of the aggressive behaviors of football fans. Violent behaviors, including hooliganism, cause fan panic, as evidenced by the events in 1985 in England when Liverpool and Juventus fans fought against each other (Campbell, 2023). Hooliganism is disruptive or unlawful rioting, bullying, and vandalism, usually in connection with crowds at sporting events. The words *hooliganism* and *hooligan* began to be associated with violence in sports, in particular from the 1970s in the UK with football hooliganism. The phenomenon, however, long preceded the modern term; for example, one of the earliest known instances of crowd violence at a sporting event occurred in ancient Constantinople. Two chariot racing factions, the Blues and the Greens, were involved in the Nika riots, which lasted around a week in 532 CE; nearly half the city was burned or destroyed, in addition to tens of thousands of deaths. As a result of the violence, roughly half of the stadium was damaged, and 39 fans lost their lives.

Similar occurrences were witnessed in 1989 when Liverpool fans again clashed with Nottingham Forest fans, leading to the death of 96 fans (Campbell, 2023). Although hooliganism and violence among football fans are common in Western countries, similar instances have been reported in other parts of the world. In 2012, fighting between Al-Ahly and Al-Masry football clubs led to the death of 76 fans in Egypt (Thabet, 2022).

Thabet (2022) said the conflict has been ranked the worst in the country's football sports history. Violence and fighting have also been reported among football fans in Malaysia. Despite the negative outcomes of violence and hooliganism on the property and lives of fans, many people in Malaysia categorize such acts as soccer celebrations. To stem violence in soccer games, the Football Association of Malaysia (FAM) has punished different football teams and their management for failing to control their fans (Yusoff et al., 2022). Despite the punishment, some fans still engage in violent and aggressive behaviors during football games.

Misbehavior among fans occurs either through physical violence or verbal exchanges. In verbal misbehavior, fans do not engage in any form of violence; however, verbal misbehavior often leads to physical altercations. Yusoff et al. (2020) reported verbal misbehaviors, including shouting at opponents, yelling at opponents, or abusing each other. Verbal misbehavior occurs between female fans, while physical altercations are common among male fans (Yusoff et al., 2020). Conversely, physical attacks in football include lighting flares, damaging public property, throwing objects, and fighting with opponents (Yusoff et al., 2020).

Some researchers have argued that verbal altercations cannot be categorized as misbehavior because chanting, singing, and yelling are part of cheering in sporting activities (Herrera, 2018; Kossakowski, 2020; Yusoff et al., 2020). Regarding physical violence, Yusoff et al. (2020) demonstrated that provocations from players and opponents often led to fighting. Leitner and Richlan (2021) reiterated that physical violence in soccer games resulted from provocative words, actions, and behaviors from the opponent

teams. Herrera (2018) stated that masculinity was topped as the reason why male fans displayed aggressive behaviors and even engaged in violent activities.

Combating Violence and Aggressiveness Among Football Fans

Around the globe, countries have adopted different mechanisms to combat violence among football fans. Given the differences in culture, levels of fan misbehavior, and geographical location, the actions taken to mitigate violence in football might differ between countries. In Hungary, for example, Rakhmanova et al. (2022) investigated how Hungarian authorities combated sports violence and established that the government had implemented different mechanisms to discourage violence during major sports events. In particular, the country has invested in the police service, which has been mandated to use all available means and strategies to control fans and prevent acts of violence in the stadium (Rakhmanova et al., 2022). Atkinson and Murry (2021) stated that Hungary has also increased the number of uniformed and non-uniformed police officers in the stadium during football games to intimidate fans, thinking of causing chaos or seeking to start fights.

In addition to using police officers and guards to prevent violence, technology such as CCTV can discourage violence in stadiums. Given the significance of CCTV in preventing crime, Hutchins and Andrejevcic (2021) recommended the installation of numerous CCTVs to ease the monitoring and identification of offenders. Installing sufficient CCTVs around the stadium will improve security by helping the management monitor and identify fans causing violence and reminding fans that their behavior is monitored (Hutchins & Andrejevcic, 2021). Rather than using CCTV as the sole security

feature in stadiums, Yusoff et al. (2020) found that complementing the CCTVs with facial recognition software helped accurately identify and apprehend crime perpetrators.

The CCTVs and software used for surveillance should be monitored, maintained, and regularly serviced to ensure they are working properly (Piepiora et al., 2019). Other technologies other than CCTV have been considered for adoption to complement and enhance the effectiveness of CCTVs in stadiums. For instance, some countries have adopted Iris scanners to complement CCTVs in mitigating hooliganism and violent behaviors among fans. Football clubs advised their fans to purchase a club card fitted with a long-range radio-frequency identification (RFID) chip as a security measure. Additional security measures are adopted when fans are applying for club cards. First, the fans' biometrics will be taken; second, a clear passport photo of the fan will be taken and synchronized with the club's digital security systems (Piepiora et al., 2019).

To access the stadiums during matches, fans at the entrance will use their RFID-fitted club cards, while their biometrics and photographs will be assessed in the tunnel before they are allowed into the stadium. Only fans whose authentication is approved will be allowed into the stadium (Yusoff et al., 2020).

In European countries, the modesty on preventing hooliganism and violence in sporting events has been centered on cultivating some form of relationship between the fan and the club (Olszewski-Strzyżowski, 2018). Olszewski-Strzyżowski (2018) stated when using this approach, fans are encouraged to use football games as a socialization tool and a means to create a sense of belonging aimed at taming violence. Even though encouraging sportsmanship among fans has proved effective to some extent, many in the sports industry have criticized the approach as soft and ineffective in curbing crime and

violence in football (Tiell & Cebula, 2020). However, despite the success of using sports for socialization and developing a sense of belonging, some football stakeholders have advocated for stricter responses against hooliganism (Yusoff et al., 2020).

The problem surrounding the different preventative mechanisms and strategies put in place by countries is the difficulty in assessing the effectiveness of their implemented programs. Studying the prevention of football hooliganism in Turkey, Ekmekci et al. (2018) reported that some preventative actions have improved the relationship between clubs, fans, and the police, discouraging young fans from adopting violent behavior. As a preventive action, Loyens et al. (2021), in a qualitative case study of Dutch football, recommended the establishment of integrity programs aimed at teaching and training youths to act responsibly while at stadiums.

Security and Surveillance in the 21st Century

To avoid panic, fear, and destruction due to terror attacks, violence, and crime associated with sporting events, the United States has developed a robust security strategy involving all stakeholders, including members of the political class, media institutions, and the general public. With the risks of violence and criminal activities, the security of football stadiums has been enhanced through public risk management and the installation of security measures to counter any criminal activities (Ashwin, 2022). Besides risk assessment, the United States government has developed and passed several laws that mandate security agencies to conduct surveillance against threats (Deflemm & Chicoine, 2018). Other laws advocate for security agencies through media platforms to rally public and political classes' support in advising and maintaining security for mega-sporting events. Deflemm and Chicoine (2018) asserted that seeking political and public

support is meant to encourage public and sports organizers' acceptance, implementation, and adherence to new security measures.

During sporting events, physically identifying criminals, and hooligans is almost impossible, given the large number of spectators entering and sitting in the stadium. As a result, Faraji et al. (2018) asserted that adopting technology would help sporting organizers address the difficulties and enhance security during sporting events. Some of the technologies adopted included biometric identification devices, video surveillance, and satellite surveillance not only to identify criminals but also to monitor for suspicious activities that might qualify as a security threat. With the increase in security threats, security and counterterrorism strategies characterize the planning of huge sports activities such as football (Faraji et al., 2018).

Cleland and Cashmore (2018) stated that heightened security measures are always implemented weeks or even months before sports activities. Cleland and Cashmore (2018) particularly identified measures such as CCTV surveillance, satellites, drones, security patrols using uniform and undercover police guards, and the stadium's closure before the sporting event. Cleland and Cashmore (2018) conducted quantitative research with over 1,500 survey responses from the association of football fans in Germany, the United States, and France to investigate how highly publicized security events are secured. Cleland and Cashmore (2018) also sought to identify and report the impacts of security and counterterrorism strategies on people's civil liberties around the stadiums.

The study results indicated that the heightened security measures ensure the safety and security of the attendees. Moreover, with early preparation, the state ensures that the

public is involved in the planning and normalization of security against possible threats. As per Cleland and Cashmore (2018), the goal is to ensure a flawless experience with sporting events in terms of security and safety of the fans in the stadiums.

The events of 9/11 did not only influence the security and surveillance of Olympic events but also influenced how the security, surveillance, and counterterrorism strategies were implemented during the 2002 World Cup in South Korea. Ludvigsen (2022) stated that South Korea and Japan conducted extensive security checks, including counterterrorism measures, months before the tournament to ensure the attendees' safety. In previous research, Cleland (2019) explored how the football federation prepared security for the World Cup in 2010 in South Africa. In their qualitative study, Cleland (2019) stated that together with the South African government, the World Cup organizers deployed thousands of security agents through the stadiums, with over 40,000 uniformed police officers conducting patrols. Moreover, as a contingency, another 50,000 uniformed and specialized police units were put on standby.

In addition to the security measures in South Africa during the 2010 World Cup, Cleland (2019) also examined security preparations for the Rugby World Cup in 2003. Cleland (2019) explored fans' perceptions regarding the risks of terror attacks and how they felt about their security and safety while attending the rugby tournament. The results indicated that while heightened security gave the fans some sense of comfort, risks of insecurity, including terrorism threats, did not deter them from celebrating and enjoying the tournament. Therefore, this study will build on Cleland's (2019) findings to describe how football fans describe the impacts of security threats on their attendance of the

games and whether the security measures in place influence how they participate in mega sporting events such as the World Cup.

Technology, Crime, and Violence in Football Management

Stadiums have upgraded their security, evidenced by establishing security command and control centers within the stadium. The essence of having command and control centers in the stadium is to allow security personnel to monitor both sides of the stadium easily. Kowalska (2019) stated that the security control in the stadium housed the public address systems, fully integrated closed-circuit television system for surveillance, alarm systems, turnstile monitoring capabilities, and control systems for stadium entrances. In addition to the security systems in the control rooms, the stadium management has upgraded their on-site security system with a mobile command center fitted with CCTV and connected to the control room, allowing easy communication between security personnel manning the stadium (Hutchins & Andrejevcic, 2021). In previous research, Cleland and Cashmore (2018) reported that investment in technological security systems, including FaceTrac and CCTV, have eased the monitoring and identification of fans attending games inside and outside the stadium.

While investing in technology has enhanced the security of British stadiums, conducting risk assessments to identify vulnerabilities, risks, and threats has proved critical. Cleland and Cashmore (2018) stated that the British government conducted a financial risk assessment to establish how and what may disrupt the flow of resources meant for the stadium. The government also conducted a strategic risk assessment to identify the different ways planning may fail, the operational risks associated with the management and construction of the stadiums, and the human errors that might

exacerbate operational risks. In addition to financial and strategic risk assessments, operational risk assessments are also conducted for the British stadiums, including risks associated with the process and human errors.

Cox et al. (2020) extended Cleland and Cashmore's (2018) research on risk assessment, which is critical in promoting the security and safety of stadiums in the United Kingdom. Other than the already discussed operational, strategic, and financial risk assessments, organizers of football games, in conjunction with football authorities, performed match assessments. In match assessments, Cox et al. (2020) established that football authorities assessed football games based on provided intelligence, the history of the event between the playing teams, the anticipated number of fans, and the number of people the stadium can hold. Conducting match assessments regularly and periodically helps football authorities meet the security needs of the games flexibly based on the latest intelligence and confirmed reports. Match assessments advise on the levels of management needed, costs, and resources based on adjustments made before the match. The common security methods used are discussed below.

Biometrics

Biometrics is the scientific discipline concerned with measurements and metrics related to biological or behavioral human characteristics, which are commonly possessed by all human beings while also being highly representative of a person, thus allowing for the identification of individuals. Biometrics is used in various ways, including access control, identification, verification, and authentication (Hutchins & Andrejevcic, 2021). Such markers may be related to a person's physiological characteristics, such as finger or palm prints, DNA, facial, iris, or retina recognition (i.e., biological biometrics). Others

are linked to behavioral patterns, such as recognition based on a person's gait (behavioral biometrics or 'behavior metrics').

With the growing threats of violent cyber-attacks, more stadiums are looking to introduce biometrics in their security systems (Hutchins & Andrejevcic, 2021). As biometric identity attributes are unique to a person and stable over time, they provide a singularly useful tool for accurate and efficient identification and authentication. These characteristics also make such data particularly sensitive, thus creating a need for secure data storage and processing systems to mitigate the risk of unauthorized access. The biometric authentication system is a technology that measures a body's physical characteristics and uses the data for personal authentication. Biometric tools have become a staple for contemporary use by security sector actors. Automation has turned biometrics into an even more powerful instrument.

Metal Detectors

Metal detectors are a standard security tool used at airports, sports arenas, and other security areas. They are also used in war zones to search bodies for explosives. These devices often safeguard essential areas and valuable items (Diaz et al., 2019). A walk-through metal detector is "a free-standing screening device having an electromagnetic field within its portal structure (aperture) for detecting metallic objects, including some nuclear shielding materials, carried by persons walking through the aperture."

Walk-throughs tend to be less invasive than wands for patron screening and quite a bit faster to screen patrons than with wands, which would appeal to those emphasizing the fan experience for stadium venues. Walk-throughs also can change the amounts of

metal they detect, compared with wands, many of which do not have this capability. These machines effectively detect metallic objects, such as knives and guns (Diaz et al., 2019). People often bring these items with them when they travel. A metal detector's loud buzz stops people from getting inside a building; it alerts security guards that someone may be carrying a dangerous item.

Additionally, people often pass false metallic objects off as others when bypassing metal detectors. This means a metal detector is necessary but not always 100% accurate (Diaz et al., 2019). When violent people plan an attack, they often use metallic materials to create deadly explosives. They need something that can destroy objects without being noticed by authorities. Metal detectors help find these devices when used correctly. These machines alert security personnel to unusual signals when triggered near metallic material (Diaz et al., 2019).

Metal detectors can secure a sports stadium by helping security personnel detect and prevent weapons smuggling into the stadium. The metal detectors used in the stadium are portable and lightweight, making them easy and quick to install in any event area (Diaz et al., 2019). Metal detectors use electromagnetic fields that can accurately detect any metal objects in the area. It works by measuring the electromagnetic field in front of an object and gives the response to your scanner. Metal detectors are a necessary addition to the security systems of major sports venues. These systems help prevent bomb attacks in major football matches and provide peace of mind to fans as they enter the venue. Using metal detectors helps eliminate customer delays, reduces theft rates, and provides greater security at the stadium. As such, walk-throughs can be used in large venue situations, targeting whatever amounts of metal the venue prefers to target (e.g., based on

a risk assessment). Obviously, the smaller the quantity desired to be detected, the slower the screening would take.

Facial Recognition

Facial recognition, also known as computer vision, is a collection of techniques that allow computers to recognize patterns in the human face very robustly. The most critical feature is the geometry of a face, such as the distance between a person's eyes and the distance from their forehead to their chin. This then creates what is called a "facial signature." It is a mathematical formula compared to a database of known faces. Face recognition has recently attracted attention as terrorism is one of the most severe security threats today, and this technology could provide an important tool to counter these threats (Nijholt, 2020).

Facial recognition systems are crucial steps in securing the sports stadium from criminals entering the stadium. It is a technology that uses Artificial Intelligence and deep learning to capture features of the human face and analyze characteristics such as age, gender, race, ethnicity, and appearance to detect suspicious behavior (Nijholt, 2020). Facial recognition can assist in identifying prohibited persons entering a sports stadium, such as criminals and troublemakers. Facial recognition systems can detect suspected criminals when they enter the stadium.

Using cameras has increased individuals' feelings of safety and security. Studying the psychological perspectives on individual perception of safety, Eller and Frey (2019) found that people perceived safety and experienced real safety differently. Using camera surveillance to increase security gives people a feeling of being safe; however, their perception of safety is short-lived as the cameras are operated by people who might be

compromised (Jansen et al., 2018). However, Welsh et al. (2019) argued that despite the feelings of safety, the impacts of camera surveillance are limited.

Another effect of using cameras for surveillance is that rather than promoting security, people will act according to the fact that they are being watched via security cameras. Jansen et al. (2018) asserted that people acted as required or conformed to the laws and powers present out of the knowledge that their behaviors and conformity would be spotted on surveillance cameras. Bicchieri and Dimant (2019), while studying the risks and benefits of social information, established that people conform to power because it is expected of them. However, both Jansen et al. (2018) and Bicchieri and Dimant (2019) stated that given the opportunity, many would act contrary to the instructions. Piza et al. (2019), in a systematic review of the literature, established that given the opportunity, the individual would recognize security but would not consider its value nor appreciate the value of power in surveillance.

Cameras may discourage an act of crime in an area, but the crime might shift to areas not covered by cameras. However, Eck and Clarke (2019) reported that the offenders would move to a new area without cameras and commit the offense due to being deterred by the presence of surveillance cameras. Thus, rather than preventing crime or deviant behaviors, surveillance cameras displace them to uncovered areas (Rossmo & Summers, 2019). Comparably, Piza et al. (2019) found that with cameras, criminals moved to uncovered areas not surveilled to commit the offense. Similarly, Robin et al. (2020) and Circo et al. (2022) concurred that camera surveillance displaced and postponed crime rather than stomping out crimes. However, despite the minimum

crime prevention, surveillance cameras have reduced crime and criminal activities in covered areas.

The emergence of automated facial recognition as a security technology must be understood as part of post-9/11 security hysteria and as the profound post-Cold War identity crisis of the national security state. The post-9/11 tech nostalgia assertions made by Senator Feinstein and others not only efface the technology's muddy history and reify automated facial recognition as "hi-tech," they also frame the problem of security as one of recognition or identification, the need to accurately and reliably identify the enemy. While this framing enabled the biometrics industry to capitalize on the hyper-paranoia of the post-9/11 moment, the preoccupation of the national security state with identifying new enemies and problems to legitimate itself intensified a decade earlier, following the fall of the Berlin Wall and the breakup of the Soviet Union.

Sports stadiums are prime sites for deploying and developing facial recognition technology. They are used to envision and model a spectator experience governed by automated surveillance and sensor-based monitoring systems, which promise greater security and enhanced consumption opportunities. Law enforcement focuses on the sports stadium as a site for considering how biometric surveillance is introduced, implemented, and normalized. The immense popularity of mega-events and the pleasures of live sports erode the contestability of this framing, drawing attention away from the biases, inaccuracies, privacy concerns, and inequalities perpetuated by highly invasive systems that exercise social control in and beyond the stadium. Facial recognition systems use a camera to capture an image of a person's face as a digital photograph. In the most common form of facial recognition, this image is manipulated and reduced to a series of

numbers representing the image of the "average" face. These numbers are often referred to as a template, which is then instantly searched against a "watchlist," or computerized database of suspected terrorist templates. This search looks to answer the question, "Is this person in the watchlist database?" A computer-generated match or "hit" alerts the authorities to a potential threat.

Countering Extreme Violence in Sports Stadiums

Sports are a significant part of our culture. The sports we enjoy most often involve aggressive physical activity and can become an addiction for some people (Nyadera & Bincof, 2019). Electronic surveillance helps police handle security issues during sporting events. Surveillance cameras monitor the entire area and continually record activities on stage. This allows officers to document criminal activity without compromising ongoing events.

Some cameras record license plate numbers and note vehicle movements during outdoor events. These allow authorities to respond quickly to emergencies or crimes in progress without wasting time flagging down witnesses first. Law enforcement agencies need to identify suspects as they travel around the world. Criminals and others change all sorts of information about themselves, but their faces remain the same. The first operational facial recognition system (face trace) was developed by the Central Intelligence Agency (CIA) in the late eighties.

It combines image analysis technology with collateral information to create an electronic mug shot collection. Using simple collateral information about a suspect's height, age, sex, and photograph, the system allows users to identify an unknown person with a reasonable probability. The system matches information extracted from the

photographs with similar information extracted from a database of photos of existing suspects.

The technology was subsequently transferred to the Immigration and Naturalization Service (INS) for use by the Border Patrol. Facial recognition technology can be used in emergencies where a suspected criminal attack is imminent or underway by dramatically reducing the time first responders and investigators need to generate leads and identify suspects. This can improve response times or help prevent or mitigate harm from such attacks, saving lives.

FaceFirst is also a new technology. The ultimate sports and concert face recognition platform is perfect for arenas and stadiums. The patented facial recognition platform helps create safer and more personalized events using the face recognition technology available. FaceFirst is a biometric surveillance solution that proactively detects criminals, banned fans, stalkers, potential terrorists, VIPs, and other guests by providing stadium personnel with instantly actionable information when they need it. Using artificial intelligence and deep learning, FaceFirst offers surveillance, mobile access control, personal identity management, and more. The platform also helps provide a VIP experience to premium ticket holders.

Stadiums are places where people gather to watch sports competitions and are often spots for crime and violent behaviors and can even be prime targets for terror attacks. To keep attendees safe, security managers must take several precautions regarding the security of attendees and fans during games when organizing sporting events (Nyadera & Bincof, 2019).

Though physical identification of known suspects and or violent disruptors can be achieved manually, Nyadera and Bincof (2019) explained that during sporting events, the huge crowd of fans proved tedious and challenging for security personnel to patrol and mitigate against every threat; hence, the need for technology, especially facial recognition software. Unless the photograph is captured under very controlled conditions, the system may have difficulty identifying the individual or even detecting their face in the photograph. The system works best when environmental factors, such as camera angle, lighting, facial expression, and others, are controlled to the maximum extent possible.

Privacy Concerns

As technology advances, so do the techniques for collecting, using, and analyzing biometric data, resulting in heightened security and privacy concerns, especially for using a biometric facial recognition system in stadiums and sports arenas (Nijholt, 2020). Facial recognition technology uses a database of photos, such as mugshots and driver's license photos, to identify people in security photos and videos. It uses biometrics to map facial features and help verify identity through critical features of the face.

There have been several instances where stadiums use biometric data to track the movements of fans, leading to concerns about how this data is being used and the security of the collected data. With increased privacy concerns, Nijholt (2020) highlighted instances where stadiums are accused of selling this data to third parties, raising even more concerns. Thus, it is essential to ensure that biometric data is collected and used in a way that respects the privacy of those involved. Biometrics authentication is a growing field in which civil liberties groups have expressed significant concerns over privacy and

identity issues. Today, biometric laws and regulations are in process, and biometric industry standards are being tested.

The main reason for privacy concerns amongst citizens is the lack of federal regulations surrounding the use of facial recognition technology. Many are worried about how accurate the technology is and if there are biases and misinformation in these technologies. One issue, for example, is that the technology has been proven in multiple studies to be inaccurate at identifying people of color, especially black women (Forbes, 2019). Another major concern is the use of facial recognition for law enforcement purposes. Many police departments in the U.S., including New York City, Chicago, Detroit, and Orlando, have begun utilizing the technology.

According to a May 2018 report, the FBI has access to 412 million facial images for searches (Forbes, 2019). Not only is this a concern with the possibility of misidentifying someone and leading to wrongful convictions, but it can also damage our society by being abused by law enforcement for matters such as constant public surveillance. Biometrics is nothing new to professional sports teams and their home stadiums, arenas, and ballparks. The most common form of biometrics used at sports venues is facial recognition and fingerprint biometrics. Facial recognition technology has transformed—and enhanced—the consumer experience across numerous industries. This includes travel, hospitality, retail, and healthcare, to name a few.

Facial recognition is also making its way into the stadiums, arenas, and ballparks of professional sports franchises nationwide. The current system keeps fingerprints/ photos of criminals and non-criminals in separate databases. Non-criminals may have their prints stored by the FBI if they have applied for a job that requires fingerprints for a

background check. However, under the new system, if an employer asks a candidate to submit a photo with their fingerprints, this will be stored by the FBI, too. The difference is that all photos will be stored on the same database regardless of whether someone has been arrested for a crime. This means that even if you have never been arrested for a crime, if your employer requires you to submit a photo as part of your background check, your face image could be searched - and you could be implicated as a criminal suspect just by having that image in the non-criminal file. FBI shows that 4.3 million photos in the database by 2015 will be for non-criminal purposes (BBC News, 2014).

As sports venues embark on a widespread facial recognition rollout, states and cities from coast to coast and federal lawmakers in Washington D.C. are attempting to enact strict laws regulating this next-generation technology. Further complicating matters, facial recognition is also emerging as the next major target of bet-the-company biometric privacy class action litigation. Professional sports teams (and the venues they call home) should implement robust, flexible biometric privacy compliance programs to limit the potential for expansive liability while encouraging fan participation and consumer confidence. These programs must maintain ongoing compliance with today's rapidly expanding body of law to avoid being on the receiving end of a potentially devastating biometric privacy class action lawsuit. At the same time, other professional sports franchises have also started integrating facial recognition systems into their home venues' operations. While fingerprint scanners currently dominate the market, facial recognition is poised to become the most popular form of biometrics at sports venues due to the rapidly increasing demand for contactless biometric solutions.

The Sports Event Security Assessment Model

In May 2005, the Department of Homeland Security, in conjunction with the Mississippi Emergency Management Agency, awarded the University of Southern Mississippi a $568,000 research grant to create a research-based model for the security management of university sports venues. Several risk assessment methodologies were reviewed, and the DHS risk assessment criterion was customized for assessing sports venues. The Sports Event Security Assessment Model (SESAM) was developed through the collaboration of academic and security professionals in a six-hour brainstorming session. Academic professionals with experience in the sports event security area and training in DHS threat/risk assessment participated. Security professionals included former FBI, CIA, and Secret Service employees with an extensive background in risk assessment methods and vulnerability assessment experience in the security and sports security field. This collaborative group supported the development and field testing of the model. SESAM is an open standard that allows organizations to perform a consistent and repeatable risk assessment on their sports facility or event (Harati et al., 2019).

The SESAM framework is based on four key pillars: risk identification, risk assessment, risk management, and security planning. The first step in the SESAM process is identifying potential security risks associated with the event. An assessment of the likelihood and consequences of these risks follows this. Once the risks have been identified and assessed, event organizers can develop a security plan to mitigate and manage them. The SESAM framework provides a comprehensive and systematic approach to security risk management for sports events. It is designed to help event organizers identify, assess, and manage security risks associated with their events. Using

the SESAM framework, event organizers can ensure their event is safe and secure for all participants.

The model provides a way for organizations to carry out a risk assessment, which helps identify potential threats, inform the design and plan of the site security plan, measure performance against the designed security measures, and improve overall facility security. The government uses a Sports Event Security Assessment Model (SESAM) to capture, analyze, and communicate the lessons from large-scale sporting events.

The model includes 21 critical security elements and 14 core competencies necessary for sports event security readiness (Harati et al., 2019). The model considers the unique characteristics of each sporting event and venue and provides a structured approach for identifying, assessing, and managing security risks.

The SESAM is a security risk assessment model that enables an organization to assess its level of security preparedness through a series of analysis steps and understand its specific security concerns. The model allows the user to examine the characteristics of their sports events, which can then be used to make security improvements (He, 2021). The SESAM process involves three steps: identify the sports event, determine the risk involved in your sports event, and take action to prevent or minimize risk.

Contingency planning will aid sports businesses in recovery efforts and the continuation of operations during incidents. The process's first step involves identifying a Sports Event Security Assessment Team (SESAT), including all key personnel responsible for game day security. These may include the athletic facility manager, campus police chief, emergency management director, local sheriff, and campus physical

plant facility manager. Once the SESAT is established, meetings and interviews are scheduled to provide assessment objectives and define the assessed area based on a one-mile radius of the sports venue. Next, the characterization of assets and target identification is achieved through in-depth surveys and interviews at each sports facility.

Conclusion

Criminal activities at sporting stadiums interfere with sporting activities besides risking the lives of fans and athletes. This literature review sought to support the problem and justify the purpose of the study, hence the need for this qualitative descriptive research. An extensive review of the literature revealed that violence witnessed in football might result from drug abuse, excessive consumption of alcohol, or poverty. Violent behaviors, such as hooliganism, vandalism of properties, and physical altercation, result in panic and anxiety that impacts sports negatively. Although hooliganism and violence among football fans are common in Western countries, such as the events of 1985 in England when Liverpool and Juventus fans fought against each other, similar instances have been reported in other parts of the world, fighting between Al-Ahly and Al-Masry football clubs led to the death of 76 fans in Egypt in 2012.

Crime, violence, and hooliganism are costly to the sports world in terms of lives lost and destroyed properties. To minimize this loss, the literature review has identified different strategies adopted and implemented to deter crime and violence. Countries have invested in the police force and have mandated them to use all available means and strategies to control fans and prevent acts of violence in the stadiums. Uniformed and non-uniformed police officers are often deployed to the stadium during football games to deter fans from engaging in violence. In addition to physical human security using

guards, technology has been demonstrated as key in mitigating extreme violence. The findings of reviewed studies evidence that installing CCTVs around the stadium improved security by helping the management monitor and identify fans causing violence. Further, complementing the CCTVs with facial recognition software helped accurately identify and apprehend crime perpetrators.

Investing in technology has enhanced the security of stadiums in the United States. While investing in technology has enhanced the security of British stadiums, conducting risk assessments to identify vulnerabilities, risks, and threats has proved critical. Conducting match assessments regularly and periodically helps football authorities meet the security needs of the games flexibly based on the latest intelligence and confirmed reports. Common technologies used to assess and enhance stadium security include biometric security systems, CCTVs, metal detectors, and facial recognition. In Chapter 3, the researcher will provide an in-depth discussion of the methodology for the study.

CHAPTER 3: METHODOLOGY

The purpose of this qualitative descriptive research was to explore how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast. The problem that prompted this qualitative research is that despite the increase in violence and crime in sports stadiums and the use of biometric systems, it is not known how stadium security managers perceive and describe their experiences with biometric systems in mitigating crime and violence in and around sports stadiums on the east coast.

A purposive convenience sample of 20 sports security managers from stadiums on the East Coast of the U.S. was selected for semi-structured interviews. The semi-structured interview questions were developed based on the Technology Acceptance Model theory concepts. The researcher developed and conducted semi-structured interview questions to describe variation across study participants' perceptions. The method of data analysis was a thematic analysis of qualitative data using NVivo qualitative data analysis software (version 12) and following Braun and Clarke's (2006) six-step thematic analysis process.

Research Questions

This study explored how security managers of sporting arenas perceive using facial recognition software to mitigate crime and violent behaviors in sporting stadiums during sporting events. The study explored how these managers perceive and describe the success or failure of security protocols and measures when they use facial recognition

software to prevent crime and violent behaviors within the stadium environment. The following four research questions will guide the study.

RQ1: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the East Coast?

RQ2: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the East Coast?

RQ3: *Perceived Ease of Use (PEU)* Will learning to operate facial recognition technology in stadiums be challenging for security managers?

RQ4: *Perceived Usefulness (PU)* How will the technology at work improve my productivity?

The Rationale for a Qualitative Methodology

The researcher selected a qualitative research method to examine the perspectives of security managers who work in sporting arenas. Qualitative research enables a researcher to focus on a problem to gain in-depth knowledge based on a specific sample's perspective of this problem. Qualitative research focuses on understanding a social phenomenon, asking how and why, and relating a sample's direct and shared experiences (Aspers & Corte, 2019). A qualitative study is beneficial when the researcher does not know the variables and needs to explore the problem (Allan, 2020). Collecting data is sought to describe a phenomenon measuring not numerical data but viewpoints, opinions, and perceptions (Gronmo, 2019). Qualitative analysis allows social phenomena to be explained in their environment and explains how the study members interpret specific experiences (Gildersleeve & Guyotte, 2020).

Based on the description of qualitative methodology, it was appropriate to address the purpose of the study, which is to explore how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the east coast.

Alternative research methodologies that were explored included quantitative research and mixed-methods research methodologies. The quantitative methodology was not selected for the study because a quantitative method concentrates on outcomes using research questions and hypotheses to correlate two or more variables or to establish a cause-and-effect association. Quantitative research is used to determine facts concerning a social phenomenon, not understanding the phenomenon from the perspective of a sample (Hong et al., 2017). A quantitative researcher needs to measure collected quantifiable data using closed-ended questions or numerical statistics to support a stated hypothesis (Hong et al., 2017). As the current study's researcher aims to explore a sample's perceptions, collecting quantifiable data is inappropriate for the research.

A mixed methodology is also inappropriate for the current research as this method utilizes both qualitative and quantitative research methods (Gronmo, 2019). The researcher of the study only wishes to examine the social phenomenon from the perspective of a sample of sports arena security managers using qualitative data, thus disqualifying the appropriateness of mixed-methods research.

Rationale for Research Design

A qualitative descriptive research design was selected to guide the data collection. Qualitative descriptive research is a qualitative research design used to present a systematic and accurate description of the problem or phenomenon being investigated

(Dulock, 1993). Qualitative researchers use a descriptive research design to clearly describe a phenomenon of interest based on the frequency of occurrence, specific characteristics, and location. Dulock (1993) noted that qualitative descriptive design is used to discover new meanings associated with the phenomenon under discussion.

Based on the preceding discussion, qualitative descriptive research was appropriate to provide a systematic and accurate description of biometric facial recognition software use in sports stadiums in the United States. Moreover, qualitative descriptive research helped the researcher describe in-depth security managers' perception and experience with facial recognition software and its effectiveness in mitigating crime and violence in and around sports stadiums on the east coast.

Koh and Owen (2000) argued that Researchers also use qualitative descriptive research designs to explore and study ongoing events (Koh & Owen, 2000). Crime and violent behavior are common occurrences during sporting events. Security threats and risks of sports fans being abused, mugged, or property being destroyed necessitate continuous monitoring for such behavior and identifying the perpetrators, stopping them before they put their plan into action. While physical security has been reported to improve security, technology has a wide application, and the outcome is almost instant. Thus, the continued use of technology to deter crime and violence in sports stadiums supports the appropriateness of qualitative descriptive research design. Researchers use qualitative descriptive research design when answering the 'what' and 'how' questions (Sandelowski, 2000). Qualitative descriptive research design aligns with the research questions that the research will use to describe what security strategies have been used to mitigate crime in sports stadiums and how technology (biometric facial recognition

software) has been used to deter violent behavior and crime in and around sports stadiums on the East Coast.

Other qualitative research designs, such as grounded theory, ethnographic design, or phenomenological design, were not appropriate for the current study as a multiple case study. Grounded theory was not applicable because this method generated data to develop an explanation of a theory that would not occur in the present study (Tie et al., 2019). An ethnographic design would not answer the posed research question as this type of study investigates the social-cultural experiences of a specific culture or society (Jones & Smith, 2017). Phenomenology examines the lived experiences of a small sample of participants, helping to learn from the experiences of others (Neubauer et al., 2019). Phenomenology is used to examine an understudied phenomenon that is not easily explained. While the intent of the current study could be one of phenomenology, the topic of crime and prevention and protection methods is not an understudied area of research.

Population and Sample Selection

The general population of interest for the study included sports arena security managers working on the East Coast of the U.S. The target population was security managers currently employed in a sports arena on the east coast, who have used biometrics facial recognition software currently or in the past as part of their security protocols and measures, and who have addressed prevention measures related to acts of crime and violence. The researcher used convenience sampling to recruit an appropriate sample size. The researcher recruited 20 security managers who participated in the semi-structured interviews.

The sample sizes for the interviews were established based on the need for data saturation from the collected data. Saturation is when the collected data does not yield new results (Saunders et al., 2018). Researchers suggested using at least 12 participants for interview purposes allowing a researcher to reach data saturation when collecting data (Vasileiou et al., 2018). The number of interview participants was 20.

Recruiting and Sampling Strategy

The plan for recruiting and selecting study participants purposively began with acquiring site authorization from the related sports arena CEO or another person in a position of authority. The researcher secured authorization to recruit security managers from at least twenty different sports arenas on the East Coast region of the U.S. through email. The researcher will share the semi-structured interview protocol in the solicitation if the CEO or person in a position of authority wants any question(s) revised or removed. The researcher will do so as long as it does not compromise the validity and alignment of the research. Retaining any interview questions that the researcher initially wants to revise or remove will only occur if explaining the importance of the focal question or questions convinces the researcher to change their mind.

The researcher accessed each CEO or person in authority's email address through the sports arena's relative website. Each response for access from the CEO or authoritative person was provided on business letterhead and included in the appendix of the dissertation research and the final dissertation. The person who signed off on the site authorization provided the researcher with either an email address or business phone number for the stadium's security manager for recruiting purposes.

The researcher began the recruiting process only after site authorization and IRB approval had been given. This process was conducted through email or phone calls, with the researcher communicating the purpose and significance of the current study within the request for volunteers. The researcher used convenience sampling to recruit the necessary number of participants. A convenience sample is considered a sampling method that relies on the availability or location of the researcher for participant selection (Frey, 2018). Convenience sampling is used for recruiting participants who are easily accessible and conveniently located to the researcher. The locale of the arenas where the potential participants are employed is convenient to the researcher because he also works in the industry and has direct contact with these venue leaders employed as security managers.

The researcher employed snowball sampling if convenience sampling does not provide the needed number of participants. Snowball sampling is used in recruitment and requires the researcher to ask those participants already participating in their study to identify other potential participants. Snowball sampling has two steps: first, to identify potential participants in the population, and second, to ask the first group to recruit others interested in participation (Levine, 2014). A second benefit to this type of sampling is the opportunity to discover characteristics of a population the researcher was unaware of (Levine, 2014). This sampling method allowed the researcher to ask the head of security at one sports stadium venue to refer to another authority from a second venue.

For those security managers who volunteered to participate in the study, each had to meet the following inclusion criteria: a) they must currently or in the past work in a sporting arena or stadium located on the east coast of the U.S., b) they must have used

biometrics facial recognition software currently or in the past as part of their security protocols and measures at a sports arena, c) they must have addressed prevention measures related to acts of crime and violence as part of their present or previous security protocols, d) they must be over the age of 18 years, and e) they must speak, read, and understand the English language.

The recruited security managers were asked to sign an Informed Consent form (Appendix D). All ethical assurances were relayed to the participants through the Informed Consent form. This form delivers all information with protection for each participant. The researcher emailed the participants an unsigned Informed Consent for their signature, explaining that the form's purpose is to assure the participant that the data collection methods are all ethical and that there will be no harm to anyone participating (Purvis et al., 2021). The form was signed electronically, and data collection began once signed and returned through email to the researcher.

Trustworthiness

Trustworthiness in qualitative research aims to guarantee the rigor of the study. The four elements of this rigor include credibility, transferability, dependability, and confirmability, which are used to establish trustworthiness in the data collection instrumentation and the data collected (Korstjens & Moser, 2018).

Credibility

The credibility of the data must be established to ensure that all data is captured as a reality of experience based on the participant's recall (Shenton, 2004). The credibility of the study focuses on the reliability of the data. Further, the credibility of research relies upon the confidence placed in the reliability of the data and the truthfulness of its relative

findings (Birt et al., 2016). The researcher's bias threatens a study's credibility, negatively influencing the research results. The researchers will minimize this threat by using bracketing to monitor personal bias (Birt et al., 2016). Bracketing involves noting personal bias in a field journal during all data collection and analysis steps. This reflexive process allows the researcher to return to documented variables of personal bias and ensure that these are not present within the resultant findings.

In establishing credibility, the researcher employed member checking. Member checking is an essential technique used to determine the representation of responses from the data and analysis (Birt et al., 2016). The participants will review the transcribed interview data to increase the correctness of the recorded and transcribed responses and address possible errors. If such mistakes were noted, participants were asked to clarify, and the researcher made changes or additions as needed.

Transferability

Transferability is defined as the extent to which a study's findings and data process can be replicated in another setting with similar results (Korstjens & Moser, 2018). Korstjens and Moser (2018) described transferability as part of the trustworthiness need for applicability whereby the thick descriptive is extracted based on how the researcher produced the results. This information is clearly understood so other researchers can reproduce the same research in the future. Transferability is created by supplying other researchers with proof that the study's findings could apply to other populations, situations, times, and contexts (Korstjens & Moser, 2018). Establishing transferability occurs by mitigating failure for replication and ensuring the process is not generic (Korstjens & Moser, 2018).

Transferability must also ensure that the sample is sufficient in size and composition. The method utilized to establish that the study is transferable and minimize any threat will consist of focusing on mitigation against the failure of replication and processes not being generic (Korstjens & Moser, 2018). This study used convenience and snowball sampling to recruit participants; the sample's composition was primarily motivated by their projected ability to provide valuable data. This motivation will also ensure that the answers to the research questions come from individuals with direct knowledge of security measures to prevent criminal acts in a sporting arena.

Dependability

Dependability as a component of trustworthiness consists of the durability of the finding over some time (Shenton, 2004). Dependability demonstrates stability and is threatened by a lack of transparency regarding the details of the findings. The researcher minimized this threat by creating an audit trail. An audit trail documents every decision and step to arrive at the final results (Shenton, 2004). Using an audit trail as a dependability strategy allows the researcher to defend certain decisions that may not be on the original plan. The researcher will also provide in-depth methodological descriptions to establish the dependability of the current study.

The researcher used Braun and Clarke's (2006) six-step process for thematic analysis to guide the presentation of the steps used to detail themes from the interviews and questionnaires. This detailed description will be made available to inform others about how the researcher established the results. This information can be helpful if other researchers plan to conduct the same study and intend to come up with the same findings. For insurance of dependability, the researcher will also include coding schema through

hand-coding documentation and presentation of the coding processes through NVivo. Thus, the method used to develop themes to address these research questions will be transparently presented and documented.

Confirmability

Confirmability is the objectivity of the qualitative study as evidenced by a procedure grounded on the standards expected in quality research (Chess, 2017). This element of trustworthiness is essential in establishing that enough care and integrity were practiced to maintain objectivity during the study (Guba & Lincoln, 1982). The researcher used strategies to develop the confirmability of this study, including creating a well-defined coding procedure and detailed methodological descriptions. Confirmability will be established using a well-defined and fully described method of coding processes (Shenton, 2004). For example, the threat of researcher bias was mitigated by the researcher keeping a reflexive journal, so it was noted if any bias was apparent. For this research, the coding procedure will follow the thematic data analysis method (Braun & Clarke, 2006). This data analysis procedure was selected because of the opportunity given to the researcher to be iterative and reflective of the emergent themes (Strauss & Corbin, 1990). A detailed description will be made available to inform others about how the researcher came to the results. The researcher will then provide a detailed explanation of the thematic analysis process.

Data Collection and Management

Once recruitment was completed, with the necessary number of participants agreeing to participate and signing the Informed Consent, the researcher began to collect data. The researcher used two different sources to collect the necessary data. The first

data source was a researcher-developed semi-structured interview with open-ended questions, and the second was a survey.

Semi-Structured Interviews

The researcher used semi-structured interviews to collect data from the participants. These questions were research-developed and followed the interview protocol in Appendix C. The interview questions were open-ended, and they allowed the participants to elaborate on any respective responses they chose. Participants were interviewed individually and asked questions about their involvement with biometric facial recognition software and its application for security measures against criminal acts.

The interviews took place on a Zoom conference call, which the researcher set up based on a specific time previously agreed upon by the researcher and participant. The researcher emailed the interview Zoom call link to the participant before the stated day and time. These interviews were audio-recorded and transcribed using the Zoom transcription application, then sent to the participant for member checking.

Survey

Each participant who was also interviewed completed the survey on SurveyMonkey's online platform. The questions for the interviews and the survey were the same (Appendix C). The data from the interviews and the survey were triangulated after analysis.

Demographic Survey

A demographic survey was distributed to all volunteers before participant selection. The survey (Appendix B) had the necessary qualifying questions for being selected to participate in the current study. Upon the volunteer’s request, the researcher

distributed the surveys via email, and the participants were given a time frame for returning the surveys completed to the researcher. All data collected, including the signed Informed Consent forms, the audio recording, and the transcribed recordings of interviews were de-identified and assigned an alphanumeric identifier (e.g., P1, P2, P3, FGP1, FGP2, FGP3, …). The researcher secured all data in a password-protected file on the researcher's computer, with only the researcher having access. The data will be secured for three years, and then the researcher permanently deletes all data from the computer's hard drive.

Expert Review and Field Study

Three to five field experts reviewed the semi-structured interview protocol for the qualitative descriptive study in security services, specifically focusing on crime prevention. These experts examined the interview and the survey questions to ensure appropriate protocol. First, the researcher requested assistance from several field experts to review the semi-structured interview and the survey protocols and questions. The researcher emailed them and asked them to offer constructive criticism of the dissertation committee-approved protocols, returning the feedback within one week.

The researcher requested that two participants sit for the interviews as part of a field study to test the content of the interview questions. These participant's data were not used, but the researcher had a chance to determine if the questions were concise and understandable. The researcher used the field expert to review and dissertation committee-approved semi-structured interview protocol using the same data collection and transcription method. Once transcribed, the researcher shared the transcripts with his

dissertation committee members. The researcher revised the semi-structured interview protocol per the committee's feedback regarding the content of the transcripts.

Data Analysis Procedures

The researcher analyzed the transcripts from the semi-structured interview responses guided by Braun and Clarke's six-step (2006) process for theme development and thematic analysis. The researcher used NVivo qualitative data analysis software to implement these phases. The specific steps for analyzing the transcripts from the interviews included first establishing a preliminary coding of the transcripts, with the researcher developing the initial codes using concepts from the theoretical framework of the theory of CPTED that informed the development of the instrumentation protocol.

In the next step, the researcher coded the transcripts iteratively, completing two iterations without developing new codes or revising previous ones. Third, the researcher iteratively assembled the codes into categories. Each category was formed from at least two codes until two iterations produced no new categories or revisions to previous categories. In the fourth step, the researcher iteratively assembled these into themes that directly addressed the posed research questions. The researcher used NVivo's coding functionality for these first four steps.

Step five entailed the extraction of illustrative direct quotations. For each theme, the researcher cut and pasted direct quotations that illustrated the theme into a separate Microsoft Word document. Direct quotations are illustrative when they add depth or richness to the general explanation of a given theme or subtheme. The researcher extracted at least two direct quotations for each theme for eventual inclusion in Chapter 4 of the dissertation.

The final step analyzed the direct quotations for subtheme development. This analysis entailed an interpretation of the direct quotations assigned to each theme. These direct quotations offered a substantive variation for thematic development, and from these, the researcher further extracted subthemes. Subthemes did not adhere solely to the categories used in step four as a developed theme. This final step conveys the analysis results, convincing both the validity and merit of the analysis beyond a simple description of the themes.

Ethical Considerations

Ethical considerations are based on factors associated with the confidentiality and security of human subjects, their civil liberties, and rights within the constitution of participation in the current study. The researcher ensured that all protections to safeguard the rights of the participants were in place and did not limit these protections. The researcher also notified participants in writing and verbal assurances regarding the framework for the data's use in the study. All procedures utilized for recruiting, data collection, data analysis, and data distribution followed the specified guidelines from the university's IRB requirements and the Belmont Report (National Commission for the Protection of Human Subjects of (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). Based on the fundamental principles of the Belmont Report, each participant was respected and treated autonomously, remained unharmed while maximizing participation benefits, and was treated fairly and equally. The Belmont Report is essentially a summary of the ethical principles noted by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, which was passed in 1979 (National Commission

for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). All results are published with the permission of each participant without disclosing the participant's full name or identity.

Before recruiting participants, site approval was obtained, with IRB approval attained before data collection. All participants signed an informed consent form before data collection. Informed consent protects the participants from any such unethical behaviors or harm. It follows the protocols set by the University and the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). All data records were made accessible.

The analyses abided by the participants' requests; moreover, respected their well-being, desires for anonymity, and rights when concluding the data and its usage (Kaiser, 2009). All personal identifying information and specifics about the people in the sample population were de-identified, with the researcher assigning each separate data an alpha-numeric identifier. Furthermore, all data, including demographic information and informed consent, were safeguarded electronically by saving them on the researcher's secured computer with a password-protected file and only for the researcher to have access. After three years, the researcher will permanently delete all data from this computer.

Summary

The qualitative multiple case study design for the current research provided a means to examine the perspectives of security managers who work with biometrics facial recognition software to prevent crime and violent attacks in the sports arena where they are employed. In choosing a qualitative methodology with a multiple case study research

design, the researcher collected the data necessary to answer the research questions. For the study, the researcher used convenience and snowball sampling. The researcher interviewed 20 participants using a semi-structured interview and survey. The data collected was analyzed using NVivo and guided by Braun and Clarke's (2006) six-step thematic analysis process. The findings contributed to scholarship and future professional practices in security management in mitigating crime and violent attacks in sporting arenas.

CHAPTER 4: FINDINGS

The purpose of this qualitative descriptive research is to explore how stadium security managers perceived and described their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast of the U.S. The following four research questions were used to guide this study:

RQ1: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the East Coast?

RQ2: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the East Coast?

RQ3: Perceived Ease of Use (PEU): Will security managers find it challenging to operate facial recognition technology in stadiums?

RQ4: Perceived Usefulness (PU) How will this technology at stadiums improve security managers productivity?

The purpose of this chapter is to present the themes that emerged as the major findings in this study after executing the data collection and data analysis procedures described in Chapter 3. The following section of this chapter is a description of the demographic characteristics of the study participants. This chapter then includes a description of the data analysis procedure applied to the semi-structured interview data, followed by a presentation of the study findings, organized by research question. This chapter concludes with a summary of the findings.

Demographics

The participants were a convenience and snowball sample of 20 security managers who met the following inclusion criteria: a) they worked in a sporting arena or stadium located on the East Coast of the U.S., b) they used biometrics facial recognition software as part of their security protocols and measures at a sports arena, c) they addressed prevention measures related to acts of crime and violence as part of their present or previous security protocols, d) they were over the age of 18 years, and e) they spoke, read, and understood the English language. Table 1 indicates additional, relevant demographic characteristics of the individual study participants.

Table 1

Participant Demographics

			✓ = Method used to collect security data within the organization				
	Job title	Years of experience with current venue	Consent forms	Photos accessed	from law	enforcement Facial image data	collection through
P1	Chief Security Officer	10-15		✓			
P2	Chief Security Officer	10-15		✓			

P3	Chief Security Officer	10-15		✓	
P4	Director of Security	10-15		✓	
P5	Chief Security Officer	10-15		✓	
P6	Chief Security Officer	5-10		✓	
P7	Security Manager	5-10		✓	
P8	Security Manager	5-10	✓		
P9	Chief Security Officer	1-5			✓
P10	Security Manager	5-10	✓		
P11	Director of Security	5-10			✓
P12	Director of Security	> 20			✓
P13	Director of Security	< 1		✓	
P14	Chief Security Officer	15-20			✓
P15	Director of Security	15-20			✓
P16	Director of Security	5-10		✓	
P17	Director of Security	15-20		✓	

P18	Chief Security Officer	1-5	✓
P19	Director of Security	5-10	✓
P20	Director of Security	1-5	✓

Data Analysis

The interview data was analyzed using the inductive thematic procedure recommended by Braun and Clarke (2006). The procedure consisted of the following steps: (a) familiarization with the data, (b) initial coding, (c) searching for themes, (d) reviewing the themes, (e) naming the themes, and (f) reporting the findings. The following sections indicate how each step was applied to the data.

Step 1: Familiarization with the Data

The 20 interview transcripts were read and reread to gain familiarity with the scope of their contents (Braun & Clarke, 2006). The purpose of this step was to gain a holistic familiarity with the data to enable the identification of patterns within and across the individual participants' responses. Handwritten notes were made regarding repeated words, phrases, and ideas to indicate potential points of analytical interest that might serve as a basis for generating codes in the following analysis step.

Step 2: Initial Coding

The data was disaggregated into the smallest segments of text that conveyed meaningful ideas, and those segments of text were assigned to initial codes, which were labeled with brief, descriptive phrases that summarized the meaning of the data assigned to them (Braun & Clarke, 2006). For example, P7 stated, "I think facial recognition is one

of the larger pieces of the [security strategy] puzzle. I don't know if it's the end all be all, but definitely a valuable tool." This data segment was assigned to an initial code labeled, 'facial recognition as an important part of an effective strategy.'

When different data segments had similar meanings, they were assigned to the same initial code. For example, P1 said, "A well-trained staff is a little bit more flexible than just relying on specifically a technology. However, due to facial recognition software, improvements in cameras, improvements in AI, I would think that facial recognition would be the quickest." P1's response had a similar meaning to P7's response, so it was assigned to the same code. Overall, 199 data segments across the 20 transcripts were assigned to 21 initial codes. Table 2 indicates the initial codes and how many data segments were assigned to each.

Table 2

Data Analysis Initial Codes

Initial code (alphabetized)	*n* of participants contributing (*N*=20)	*n* of data segments assigned to code (*N*=199)
Camera as weakest link in facial recognition	13	13
Clear policies and monitoring accuracy	5	5
Easy to operate	13	13
Facial recognition as an important part of an effective strategy	19	19
Facial recognition can block troublesome individuals	17	17

Initial code (alphabetized)	*n* of participants contributing (*N*=20)	*n* of data segments assigned to code (*N*=199)
Facial recognition has the potential for false ID	19	20
Facial recognition is not inherently racially biased	17	17
Facial recognition may be racially biased	3	3
Facial recognition reduces human error	2	2
Facial recognition streamlines the entry of ticket holders	1	1
Facial recognition technology will not improve productivity	1	1
Having public buy-in is effective	2	2
Human oversight of data is effective	4	4
Moderately easy	4	4
No health risks associated with facial recognition	20	20
No privacy concerns with facial recognition	4	4
Partnering with law enforcement is effective	2	2
Performance improvement possible	18	18
Privacy is a concern with facial recognition	16	16
Screening checkpoints are effective	1	1
Using multiple strategies is most effective	17	17

Step 3: Searching for Themes

The themes that emerged from the data were identified by grouping related codes to form a smaller number of broader categories (Braun & Clarke, 2006). For example, the code *facial recognition* as an important part of an effective strategy was grouped with six other codes identified as related because they all indicated the participants' perceptions of effective security strategies. As another example, a second preliminary theme was formed by grouping four initial codes identified as related because they all indicated perceived limitations of facial recognition technology. Table 3 shows how the 21 initial codes were clustered to form five preliminary themes.

Table 3

Data Analysis Grouping of Initial Codes into Preliminary Themes

Preliminary theme Initial code grouped to form preliminary theme	*n* of participants contributing (*N*=20)	*n* of data segments assigned (*N*=199)
Preliminary Theme 1: Perceptions of effective security strategies	20	79
Discrepant data - Facial recognition may be racially biased		
Facial recognition as an important part of an effective strategy		
Facial recognition can block troublesome individuals		
Facial recognition is not inherently racially biased		

Preliminary theme Initial code grouped to form preliminary theme	*n* of participants contributing (*N*=20)	*n* of data segments assigned (*N*=199)
Facial recognition reduces human error		
Facial recognition streamlines the entry of ticket holders		
No health risks associated with facial recognition		
Preliminary Theme 2: Perceived limitations of facial recognition technology	20	53
Camera as weakest link in facial recognition		
Discrepant data - No privacy concerns with facial recognition		
Facial recognition has potential for false ID		
Privacy is a concern with facial recognition		
Preliminary Theme 3: Perception of Facial Recognition Efficacy	20	31
Clear policies and monitoring accuracy		
Having public buy-in is effective		
Human oversight of data is effective		
Partnering with law enforcement is effective		
Screening checkpoints are effective		
Using multiple strategies is most effective		

Preliminary theme Initial code grouped to form preliminary theme	*n* of participants contributing (*N*=20)	*n* of data segments assigned (*N*=199)
Preliminary Theme 4: Perception of facial recognition technology ease of use	17	17
Easy to operate		
Moderately easy		
Preliminary Theme 5: Perception of facial recognition technology performance improvement	19	19
Discrepant data - Facial recognition technology will not improve productivity		
Performance improvement possible		

Step 4: Reviewing the Themes

The themes were reviewed to ensure they had internal and external homogeneity (Braun & Clarke, 2006). External heterogeneity meant that the themes were sufficiently distinct from one another to justify their presentation as separate themes. All five of the preliminary themes passed this test. Internal homogeneity meant that each theme represented a sufficiently cohesive concept to justify its presentation as a single theme rather than being more appropriately broken into two or more smaller themes. All five preliminary themes also passed this test, so they were retained.

Step 5: Naming the Themes

The preliminary themes were named to indicate their significance in relation to the study objectives (Braun & Clarke, 2006). The data assigned to each theme was carefully reviewed to assess its importance. When the significance of the data was identified, the theme was compared to the research questions to determine which research question was most relevant to address. Each theme was then named to indicate its significance as an answer to a research question. Table 4 shows the finalized names given to the preliminary themes.

Table 4

Finalized Names Given to Preliminary Themes

Preliminary theme		Finalized theme
Perceptions of effective security strategies	→	Theme 1: Facial recognition was perceived as an important part of an effective strategy
Perception of facial recognition efficacy	→	Theme 2: Facial recognition was perceived as most effective when used with human oversight and multiple, overlapping security strategies
Perceived limitations of facial recognition technology	→	Theme 3: Facial recognition was perceived as raising some concerns about false identification, camera functionality, and privacy
Perception of facial recognition technology ease of use	→	Theme 4: Facial recognition technology was perceived as easy or moderately easy to learn to use

Perception of facial recognition technology performance improvement	→	Theme 5: Facial recognition technology was perceived as improving performance under the right conditions

Presentation of the Findings

This presentation is organized by research question. Under the heading for each research question, the findings are presented under the themes that emerged during data analysis to address the question. Table 5 is a preliminary overview of how the themes are presented to address the research questions.

Table 5

Themes Presented to Address Research Questions

Research question		Theme(s) presented to address question
RQ1: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the East Coast?	→	**Theme 1:** Facial recognition was perceived as an important part of an effective strategy
RQ2: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing	→ →	**Theme 2:** Facial recognition was perceived as most effective when used with human oversight and multiple, overlapping security strategies.

crime and deterring violence at sports stadiums on the East Coast?		**Theme 3:** Facial recognition was perceived as raising some concerns about false identification, camera functionality, and privacy.
RQ3: Perceived Ease of Use (PEU): Will security managers find it challenging to operate facial recognition technology in stadiums?	→	**Theme 4:** Facial recognition technology was perceived as easy or moderately easy to learn to use
RQ4: Perceived Usefulness (PU) How will this technology at stadiums improve security managers productivity?	→	**Theme 5:** Facial recognition technology was perceived as improving performance under the right conditions

RQ1 was: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the East Coast? The theme that emerged during data analysis to address this question was:

Theme 1: Facial Recognition Was Perceived as an Important Part of an Effective Security Strategy. All 20 participants contributed data to this theme. The participants indicated that facial recognition technology (FR) was an important part of an effective security strategy. Other components of an effective security strategy were described as including a well-trained staff, AI video analytics, digital ticketing, surveying

and monitoring surrounding buildings, and installing license-plate and -tag readers at loading docks. One reason the participants reported that they perceived FR as part of an effective security strategy was that it could be used to identify potentially dangerous individuals to ensure the safety of performers, staff, and guests. Most participants said they did not perceive FR as racially biased, although a small minority of participants provided discrepant data. All participants indicated that FR and other strategies and technologies were part of an effective security strategy. P1 described a well-trained staff working in conjunction with FR as an effective strategy: "A well-trained staff is a little bit more flexible than just relying on a specific technology. However, due to facial recognition software improvements in cameras, I would think that facial recognition would be the quickest." P6 corroborated P1's response: "Technologies like facial recognition can be highly effective strategies, but they aren't effective without a well-trained staff.

They don't have the flexibility and the adaptability that a well-trained staff has. You need the technology and the personnel working together." P4 cited digital ticketing as another effective strategy that can work in conjunction with FR:

> Just about all professional sports venues are now requiring digital ticketing, which means the fan has to create an account to hold the ticket. So, it's a verified account, so the venues know who the people are, and who's coming, and presenting tickets.

P9 said of FR and its need to be part of an overall security package rather than a standalone solution, "With better cameras, better AI, the speed at which they are able to identify, and the accuracy, facial recognition would be the fastest security tool, but it

requires human oversight to mitigate privacy concerns." P7 described FR as an important part of an effective security strategy, saying of FR, "I don't think it's the end-all-be-all, but I do believe that its role is going to be growing larger and larger. I think it's definitely one of the larger pieces of the puzzle." P11 implied that FR was not an ideal tool but that, at the time of the study, it was the best technology available for stadium security: "They're working on all kinds of different ways to do it [effective stadium security] without the invasiveness of facial rec, but right now I don't think there's anything that's better." P13 cited FR as one element of an effective security strategy. Still, he noted that it was subject to bias, and he added that other technologies could compensate to some degree for this defect of FR:

> AI video analytics can be helpful as well, keeping you safe by identifying behavior, trespassing, fighting, and running, collapsing as well. So, objects like guns and bags. So, instead of focusing on the identity of a person, that's focusing on behaviors or objects, that kind of takes away some of the bias that exists in some of the software that is related to facial recognition.

P16 recalled the "high-rise" threat that occurred in Las Vegas when an active shooter fired down on a crowd with automatic weapons from a high-rise balcony. P16 said of how his organization worked to mitigate the potential for similar threats, "We've done surveys around all the buildings that surround us and those are monitored so that if someone enters onto a rooftop, then we get a motion detection and the screen flashes red." When security personnel received the alert, they could examine the visual to assess whether the person on the roof appeared to be a threat, contact the building owner to alert them, find out whether the person was authorized to be there, and, if necessary, contact

911. P19 said, “I think having license-plate-tag and driver-license readers at your loading dock are helpful.” P19 added of his overall security philosophy, “I think security is not ‘one thing works.’ I think it’s layers, it’s just a lot of layers, I think, of redundant systems, and that’s how you have a successful program.” Thus, all participants described FR as effective, but none of them believed that it was effective or appropriate to rely solely on that technology. Instead, they believed in implementing security strategies composed of multiple collaborating elements, including well-trained personnel and, in some cases, other technologies, such as AI video analytics, license-plate readers, and digital ticketing.

FR was considered part of an effective security strategy because it could be used to block troublesome individuals from entering venues, according to 17 participants. P2 indicated that one of the best uses of FR was “The ability to rapidly identify someone that is on a Bolo list or watchlist, would be the first one [use of the technology] that pops into your head.” P4 expressed why FR was useful and, indeed, almost necessary if individuals who were trespassed from a venue were to be effectively excluded:

> Facial recognition technology can be deployed by venue security to assist in the identification of persons who have been previously banned from the venue. Security staff at the gates traditionally are focused on screening fans, thousands of fans per event. And identifying one fan out of 40,000-50,000 fans for the human is challenging, if not nearly impossible.

P9 further corroborated the finding that FR was useful in keeping troublesome or banned individuals out of a venue, saying that the technology could be used to identify “Someone that’s been put on a like a No Trespass list, someone that’s caused incidents, disruptions before.” P12 described how an artist’s security team used FR to protect the

performer from stalkers by attaching circuit boards to the stadium's FR system, and he went on to note that Homeland Security could use a similar system to alert stadium officials to the presence of individuals on a terror watchlist:

> When Taylor Swift was here . . . [she] had over 500 restraining orders against people that were basically stalking her. What her security team did is they put these interactive gameboards inside each of the gates at the stadium that actually had facial recognition software in it, and we were able to pick up one of the people that were on her restraining order list, trying to get into the stadium. I think that's on artist protection, but I think also from a terrorism and Homeland Security perspective, if you had any known people, maybe someone that's on the terrorist watchlist or something like that, trying to get into the stadium, that would definitely be something that we'd want to know about and be able to follow up and investigate.

When P19 received an alert about an individual who was stalking or threatening a professional athlete who practiced in his venue, if the alert included a photograph, "If that person enters the building, you automatically get an alert in your command center, and they start tracking that person wherever the intel and the data is able to track that person, wherever they are in the building." Like P19, P15 noted that in addition to excluding troublesome individuals, FR could be utilized to dispatch additional security personnel if a banned individual succeeded in entering the venue: "If facial rec picks up someone that's caused disruptions before, we'd give staff a heads-up to where they would want to allocate resources in the stadium." P20 indicated that FR was at its most beneficial when

it was tied to a law enforcement database, corroborating P12's comment about the potential usefulness of linking FR at stadiums into Homeland Security's terror watchlist:

> I keep using the NBA as an example. We get alerts on individuals that do stuff across the country. The NHL has something similar to that. . .We get a hit on somebody as they're being screened, going through a security screen, and that could be a quick alert, and we can address it appropriately based upon that individual, whatever they did, and why they were even put in that type of [law enforcement] database.

The participants, therefore, indicated that FR was useful for identifying individuals who were banned from venues, had threatened performers, or were otherwise potentially dangerous to exclude them or monitor them to ensure the safety of performers, staff, and guests.

An additional reason 17 participants described FR as an element of an effective security strategy was that they did not perceive the technology as racially biased. However, some participants indicated that bias could enter into facial recognition analysis through human error. P1, for example, said, "The technology is agnostic. The humans that are using it and how they choose to implement it is where the bias comes in." P3 agreed with P1, saying, "Whoever's programming what to look for is where the bias comes in." P7 said of FR, "I don't believe it is racially biased." P8 also did not believe the technology was racially biased, but that, like any technology, it was sometimes prone to error, and that follow-up investigation was needed to confirm its results before action was taken:

> It's one of the tools you have to use some confirming investigation to follow up on a facial recognition hit. It shouldn't be like, "Hey, go arrest that person," or "Hey, go throw that person out because you got a hit on facial recognition." You have got to do some more investigation.

P10 also did not believe the technology was inherently biased: "It's an evolving technology where it has misidentified people. I think that it's something that as the technology progresses, I think, will most likely be addressed." P11 denied any racial bias in the technology: "I don't see how anybody could ever make that argument [of racial bias]. A black face is no more prone to set off rec than white faces." P17 answered the question of whether FR was racially biased by stating, "No." Most participants perceived FR as not racially biased, although some believed that human error could cause the technology to manifest racial bias in its results.

However, three participants provided discrepant data indicating that they perceived FR as racially biased. P4 reported that experience in testing some older versions of the technology had provided him with evidence of racial and gender bias: "My personal experience with doing some demonstrations in beta testing, this was all pre-2020, [was] that the accuracy of facial recognition technology varied greatly depending on gender and racial groups." P20 suggested that different features characteristic of different ethnicities might affect the technology and its ability to identify faces: "I'm back and forth with that one just because some ethnic groups have stronger facial features than others." Unlike other participants who indicated that human error was the element that might introduce bias into facial recognition, P16 suggested that the absence of human oversight might allow bias in the analysis to go uncorrected: "The

technology has been improved to the point where false positives have been reduced, diminished. But anytime you take the human element out of it, there's always a chance that you may get a false positive." Thus, three participants provided discrepant data indicating that they perceived a danger of racial bias in FR.

RQ2 was: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the East Coast? Two themes emerged during data analysis to address this question, as follows: (Theme 2) facial recognition was perceived as most effective when used with human oversight and multiple, overlapping security strategies, and (Theme 3) facial recognition was perceived as raising some concerns about false identification, camera functionality, and privacy. The following sections are presentations of these themes.

Theme 2: Facial Recognition Was Perceived as Most Effective When Used with Human Oversight and Multiple Overlapping Security Strategies. All 20 participants contributed data to this theme. As discussed under Theme 1, all participants perceived FR as part of an effective security strategy. In data associated with the present theme, the participants indicated the other strategies they considered effective in conjunction with FR technology for preventing crime and deterring violence. Overall, consistent with their responses under Theme 1, the participants indicated that they perceived FR as most effective when utilized as part of a suite of prevention and deterrence strategies. Other recommended strategies included having visible, strategically placed, uniformed security personnel; having undercover security personnel; having proactively monitored camera surveillance; partnering with law enforcement; having

security checkpoints with walkthrough metal detectors or magnetometer wands; enforcement of fan conduct policies; and human oversight of FR systems.

P1 cited "Signage" as an effective security strategy, and P3 mentioned "Visible security officers." P4 noted, "I think they needed a consistent layer of approaches, where no single protective measure is going to be a hundred percent," and added, "strategies that can be effective in managing stadium violence include alcohol management." P5 recommended, "Visible staff and proper staff training to recognize early indications of fan aggression in the stands." Like P3 and P5, P20 observed that visible personnel were an effective deterrent: "Technology helps, but just having that presence, whether it's the law-enforcement presence, the canine presence, but just having that presence at different locations, especially at access points and exit points, so people can understand that you're prepared." P8 suggested "Text-for-assistance programs and proactive monitoring of cameras," and P10 advised "strategic placement of security officers and law enforcement officers." P13 agreed with other participants about the importance of strategically placing uniformed security officers, and he added the recommendation that undercover officers should be incorporated, as well:

> I think the concept of omnipresence, of having uniformed personnel identified discourages that type of behavior. I think you have to couple that with undercover personnel monitoring that as well. I think camera surveillance systems need to have a whole arsenal of different approaches to minimize those types of incidents.

P13 and P14 mentioned camera surveillance: "The CCTV cameras let us know if there's an issue outside the ballpark, how traffic's flowing, how pedestrian traffic's flowing if there are any threats or problems in the immediate area if we need to request

emergency services." P15 cited fan conduct policies as essential: "Most importantly is just the consistent commitment to enforcing the fan conduct policies." P16 described how a threat of violence was mitigated:

> We had a truck hijacked, and it was recovered within five blocks of the ballpark, and inside the truck were three pipe bombs. So, that shut down ingress and egress on one of our major roadways, and that impacted the ballpark and our operation for about two hours until the bomb squad was able to mitigate the threat. But we had communication set up, and we were able to use available technology at the end of the game to notify fans to avoid that street.

P17 said that in addition to FR, effective measures included "Walkthrough metal detectors, our police units that we have in here, and our trained security teams." P19 reported, "Crowd management outside queuing the lines and letting people know what prohibited items were before they hit the door so we could keep the lines moving. Once you get to the door, there's staff running the magnetometers, searching bags." P19 added that armed security officers were under contract to assist any individuals attempting to bring weapons into the stadium, where weapons were prohibited. Law enforcement officers were also present.

When FR was utilized, the participants indicated that human oversight was necessary for an effective security strategy. P16 stated that security managers should ensure "Human oversight on all the data captured. And then, privacy with regards to how that data is protected so that we can't have a nefarious group or individual hack into the system." P18 recommended "Random and independent inspections" of all FR systems that collected personal data about individuals entering venues. P19 recommended

ensuring that all users of FR were trained to provide proper oversight of an up-to-date system: “Making sure all of the users, the operational users, and the end users, are aware of the capabilities of the system and what can and cannot be accomplished. Just continually retraining, updating, upgrading that technology.” P20 recommended human oversight to ensure the cybersecurity of guests’ personal data: “Right now, cybersecurity is very big, and I think anytime you’re collecting any type of data, you got to have those steps and processes. Anytime you think there’s any type of breach, you got to have a contingency plan.” The following theme addresses perceived limitations of FR that participants regarded human oversight as necessary to mitigate.

Theme 3: Facial Recognition Was Perceived as Raising Concerns About False Identification, Camera Functionality, and Privacy. All 20 participants contributed data to this theme. The participants indicated that FR technology had limitations that required human oversight and further investigation after the technology made a positive identification. One of the dangers was false positives. However, most participants believed that human oversight could prevent any resulting harm and that false positives with FR were rarer than false identifications with the unaided human eye. Another danger was privacy concerns. Most participants identified the cameras as the weakest link regarding the FR system components.

All of the participants indicated that FR had the potential to make false identifications. P2 stated, “When you look at false identification, in and of itself, yes. There’s the opportunity for false identification.” P6 also admitted the possibility of FR making a false identification. Still, he added that the probability of FR making a false ID may be lower than the likelihood of the unaided human eye doing so: “When you

compare it to the alternatives, the human security officer who sees something that looks a little out of the ordinary, then I would say, statistically, it [the probability of false identification] would probably be lower." P7 indicated that human oversight could effectively mitigate any tendency for FR to make false positives: "I do believe there will be false positives, but again, I think that can be mitigated through your follow-up investigation." P14 also referenced the importance of mitigating technological error through human oversight: "It doesn't just go from the technology saying that my face popped. It gets screened by humans." P10 also admitted the possibility of false positives. Still, he doubted that false positives through FR were more likely than false positives through unaided human eyesight: "I don't know that that [FR] increases the incidents of false alarms." P11 noted that different venues set different percentage values to determine a match for positive identification and that setting a higher value reduced the incidence of false positives:

> I think we need a 90 to 95 [percent]-plus match to engage someone, because typically when you are 90, 95 plus, there's no mistake. Once you dip below 90, then you run the risk of somebody looking like somebody else.

P12 also referenced percentage-match setpoints for a positive identification. He described that setting as a way to mitigate racial bias in FR: "Different ethnicities tend to look alike based on styles, hair color, haircuts, hairstyles. Individual arenas are going to have to set what their marker is. For me, I wouldn't go below 95%," match for a positive ID. P20 said a false positive could occur because "An individual could gain weight, an individual could lose weight, an individual could be sick, and a lot of their facial features may change." Thus, all participants recognized that false positives were possible with FR.

However, most participants believed that human oversight could prevent any harm that might result and that false positives with FR were rarer than false identifications with the unaided human eye.

Sixteen participants indicated that privacy was a concern with FR technology. P1 said, “You need to make sure it’s [FR is] not being utilized for racial stuff, like racial profiling. It should only be used for screening for your predetermined watchlist.” P3 agreed that invasion of privacy might be a concern for some guests: “If you’re in a public forum, and you have people who aren’t wanted for crimes, people want to protect their privacy, I guess it [FR] could be a certain level of lack of privacy for the consumer.” P5 agreed, saying, “There’s always the danger that people’s rights are going to be violated through things like racial profiling with facial rec. It should only be used to identify specific individuals who have already been troublesome from a determined watchlist.” P4 noted that some jurisdictions prohibited FR because of privacy concerns: “There definitely are potential privacy concerns. States and local jurisdictions also have, some of them, have regulations already in place that either restrict or prohibit the use of facial recognition technology.” P8 indicated that guests should only be subject to FR scanning if they consented to be: “If the stadium is utilizing facial recognition software, then the people that are entering should be made aware, and they could either choose to enter knowing that facial recognition is in use, or they could take their business elsewhere.” P9 agreed, saying that guests in stadiums needed to know what data was being collected and how it was being used: “One of the biggest areas that needs to be addressed is what it’s [the data is] being used for, or how it’s being utilized and how it’s not being utilized.” P13 also agreed: “Everyone entering the facility should be made aware that facial rec is

in use. If they choose to enter, they do so with the knowledge that this technology is in use. Otherwise, they have the option to leave." P18 recommended signage to inform potential guests: "If there's facial recognition in use, there should be signs outside the facility that say facial recognition is being used so the people who don't want to be captured on it don't go in." Thus, most participants indicated that some guests might have valid concerns about having their privacy violated through being identified by FR in a public forum, particularly if the technology was being used for an illegitimate purpose, such as racial profiling, as P1 and P5 noted.

Thirteen participants identified the cameras as the weakest component of the FR systems in their stadiums. P1 stated, "The cameras themselves, I would say, are the weakest link." P3 said cameras were a concern because they could become "misadjusted and not focused in the right area or become outdated." P4 identified cameras as the weakest link in FR systems because "Most existing security cameras are not mounted in the proper location or at the proper height for collecting effective images for facial recognition. So, any deployment of the technology will require dedicated cameras specific to the facial recognition program." P9 said cameras were a concern because they were "Operating under such different lighting conditions." P12 stated that cameras sometimes went offline:

> If you have a system issue, let's just say your cameras go down, which is a very common error. Anyplace that has cameras, cameras go down from time to time. If your cameras go down and you're relying on facial rec, then you're lost.

P19 noted that a single camera going offline could become a significant problem: "You're in the middle of an event, and a camera goes down, or it starts glitching while

you're tracking someone. Could be a problem." P20 cited a range of issues that could reduce the efficacy of cameras for FR:

> With facial recognition, especially when you're using certain cameras, some of the equipment issues can be the brand of camera, the quality of the camera, whether that camera's positioned correctly, whether that camera, believe it or not, is clean or dirty. It depends. And what if that camera's in the place where, just say for a sports entertainment venue where in an intro you might have some haze from an introduction or something, which may throw it off a little bit?

Most participants, therefore, cited cameras as a component of delicate FR systems that could quickly go offline or suffer minor functional impediments that impaired their efficacy at critical times and were easily misplaced, smudged, or obscured.

RQ3: Perceived Ease of Use (PEU). Will learning to operate facial recognition technology in stadiums be challenging for security managers? The theme that emerged during data analysis to address this question was:

Theme 4: Facial Recognition Technology Was Perceived as Easy or Moderately Easy to Learn. All of the participants contributed data to this theme. P1 said FR was easy to use and was "very similar to, you know, a standard CRT system." P2 described the technology as moderately easy to use: "Upon implementation, a five or a six [on a scale of 1 to 10] is generally where I would put most what you call easy technology." P5 also rated FR's perceived ease of use as a 5 on a scale of 1 to 10, but he added, "I would say as it's implemented, that 5 goes on down to like a 2." P7 said of the perceived ease of use, "I'd go with easy." P10 stated, "Once you've been trained on the use of the program, and you become proficient at it, I think it's pretty easy to utilize."

P14 described FR as “Easy technology,” but rated its perceived ease of use as moderate: “a 5 or a 6 because you still have the learning curve of learning the system and learning the shortcuts and ins and outs of the system.” P19 said, “The ones that I’ve seen demonstrated, I’d put them on a scale of like a 2.” P4 indicated moderate ease or difficulty in learning the technology, but the difficulty was associated more with developing appropriate policies than learning the technology: “I indicated neither easy nor difficult. And really it, for end users operating the technology, just requires training and policies and that sort of thing.”

P11 described the technology as easy to use once the value of a percentage match for a positive identification was determined: “I would say it’s fairly easy once you set the parameters for its use, which is always the biggest thing.” P12 addressed the same topic as P11, recommending that new users of the technology set the parameter for identification at a high percentage value and then lower it through trial and error until an optimum value was found: “You want to get it to where you’re not stopping the wrong person two or three times a night. So that’s the most difficult part. But even then, I’d say you go higher and then work your way down.” P20 said that FR was easy to use after undergoing the appropriate training: “Overall, once you go through adequate training and get you some face—no pun intended—some face time in with what you’re doing, you get your reps in, I think it comes to be pretty user-friendly.” The participants, therefore, indicated that FR technology was easy to learn to use and at least moderately easy to implement. Some training might be required, but the software is easy to learn once a user has undergone appropriate training.

RQ4 was: Perceived Usefulness (PU) How will this technology at stadiums improve security manager's productivity? The theme that emerged during data analysis to address this question was:

Theme 5: Facial Recognition Technology Was Perceived as Improving Performance Under the Right Conditions. All of the participants contributed data to this theme. The participants indicated that FR improved performance under certain conditions. Those conditions included keeping individuals from watch lists out of venues, coordinating with law enforcement, and monitoring the venue.

Nineteen participants indicated that FR assisted them in performing at least some security functions. P2 stated, "As far as helping to perform security functions, absolutely [FR helps] cause it's giving the extra time." P6 also referred to extra time, saying that if conditions were right, FR could provide security staff with additional time to respond to emerging incidents and a more comprehensive monitoring range: "If implemented right, with the positioning of cameras and staffing on the monitoring side, it gives security extra time and distance." P7 stated, "If there was an actual threat or someone that had a propensity toward violence and we needed to know about it, I would say it [FR] would [enhance performance]." P9 said, "100%, as far as maintaining security functions and monitoring the venue." P11 cited improved collaboration with law enforcement: "It does allow us to align a little bit better with law enforcement." P12 referred to an enhanced capacity for excluding troublesome individuals from the stadium, as discussed under Theme 1: "It is better for the patrons because now we can keep a certain type of troublemaker out." P15 also described FR as enhancing security performance concerning specific individuals identified as potentially dangerous: "When we have a person who is

on a predetermined watch list, it [FR] enables us to identify them and then exclude them or monitor them more effectively." P17 said whether FR enhanced security performance, "Absolutely," and P18 responded to the same question by stating, "Yes." Thus, the participants described FR as enhancing their security performance, particularly concerning specific threats, such as identifying individuals on watchlists and giving staff time to respond to emerging incidents.

Summary

Four research questions were developed to guide this study. RQ1 was: What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the east coast as measured by how frequently violent situations are prevented? The theme that emerged during data analysis to address this question was that facial recognition was perceived as an important part of an effective security strategy. All 20 participants contributed data to this theme. The participants indicated that facial recognition technology (FR) was an important part of an effective security strategy. Other components of an effective security strategy were described as including a well-trained staff, AI video analytics, digital ticketing, surveying and monitoring surrounding buildings, and installing license-plate and -tag readers at loading docks. One reason participants reported that they perceived FR as part of an effective security strategy was that it could be used to identify potentially dangerous individuals to ensure the safety of performers, staff, and guests. Most participants indicated they did not perceive FR as racially biased, although a small minority of participants provided discrepant data.

RQ2 was: How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the East Coast? Two themes emerged during data analysis to address this question. The first RQ2 theme was: facial recognition was perceived as most effective when used with human oversight and multiple overlapping security strategies. All 20 participants contributed data to this theme. As discussed under Theme 1, all participants perceived FR as part of an effective security strategy. In data associated with the present theme, the participants indicated other strategies they considered effective in conjunction with FR technology for preventing crime and deterring violence. Overall, consistent with their responses under Theme 1, the participants indicated that they perceived FR as most effective when utilized as part of a suite of prevention and deterrence strategies. Other recommended strategies included having visible, strategically placed, uniformed security personnel; having undercover security personnel; having proactively monitored camera surveillance; partnering with law enforcement; having security checkpoints with walkthrough metal detectors or magnetometer wands; enforcement of fan conduct policies; and human oversight of FR systems.

The second RQ2 theme was that facial recognition was perceived as raising concerns about false identification, camera functionality, and privacy. All 20 participants contributed data to this theme. The participants indicated that FR technology had limitations that required human oversight of the technology and further investigation after the technology made a positive identification. One of the dangers was false positives. However, most participants believed that human oversight could prevent any resulting

harm and that false positives with FR were rarer than false identifications with the unaided human eye. Another danger was privacy concerns. Most participants identified the cameras as the weakest link regarding the FR system components.

RQ3 was: Perceived Ease of Use (PEU). Will learning to operate facial recognition technology in stadiums be challenging for security managers? The theme that emerged during data analysis to address this question was: facial recognition technology was perceived as easy or moderately easy to learn and use. All participants indicated that FR technology was easy or moderately easy to use. Some training might be required, but the software is easy to learn once a user has undergone appropriate training.

RQ4 was: Perceived Usefulness (PU). How will this technology at stadiums improve security managers' productivity? The theme that emerged during data analysis to address this question was that facial recognition technology was perceived as improving performance under the right conditions. All of the participants contributed data to this theme. The participants indicated that FR improved performance under certain conditions. Those conditions included keeping individuals from watch lists out of venues, coordinating with law enforcement, and monitoring the venue. Chapter 5 provides discussion, interpretations, and recommendations based on these findings.

CHAPTER 5: DISCUSSION

The problem addressed in this study was that despite the increase in violence and crime in sports stadiums and the use of biometric systems, it was not known how stadium security managers perceive and describe their experiences with biometric systems in mitigating crime and violence in and around sports stadiums on the east coast. Biometrics was nothing new to professional sports teams and their home stadiums, arenas, and ballparks. In this regard, this study determined how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast of the U.S. This study employed qualitative descriptive research design. The data sources were semi-structured interviews and survey that helped the researcher collect data critical to reporting security managers' perceptions and experience with facial recognition software to prevent crime and violence in sports events. Braun and Clarke's (2006) thematic analysis steps were used to analyze the collected data.

By triangulating data sources mentioned in the previous chapter, the shared experiences of 20 participants were categorized into the following four themes: (1) Facial recognition was perceived as an essential part of an effective strategy, (2) Facial recognition was perceived as most effective when used with human oversight and multiple, overlapping security strategies, (3) Facial recognition was perceived as raising some concerns about false identification, camera functionality, and privacy, (4) Facial recognition technology was perceived as easy or moderately easy to learn to use, and (5) Facial recognition technology was perceived as improving performance under the right conditions. The first section of this chapter will present an interpretation of the results as

discussed under the themes above. The second section discusses the findings concerning the theoretical and conceptual frameworks presented in Chapter 2 and the previous research reviewed. How the findings from this study support and extend prior research is also discussed. This chapter concludes with a discussion on limitations, followed by implications for future research and future practice, and ends with a conclusion.

Interpretation of Results

This section provides a discussion of the results of this study as they relate to and answer the research questions. The interview findings revealed managers' perceived experiences with biometric systems in mitigating crime and violence in and around sports stadiums on the east coast.

Research Question One

What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence at sports stadiums on the East Coast?

Participants consistently reported that facial recognition was perceived as an important part of an effective security strategy. Participants perceived that facial recognition technology (F.R.) was a significant component of an effective security strategy at sports stadiums. According to the participants, facial recognition technology can be used to identify dangerous criminals who would be trying to access the stadium to cause harm to the spectators in the stadium. The findings imply that using facial recognition technology can help enhance the security of stadium fans and athletes by deterring crime and other violent behaviors. It helps detect criminals and their plans early, contributing to the potential crime prevention to protect fans and athletes.

Findings indicated that participants perceived other components of an effective security strategy to be a well-trained staff, A.I. video analytics, digital ticketing, surveying and monitoring surrounding buildings, and installing license-plate and -tag readers at loading docks. The participants reported that an effective security system could be attained through hiring systems experts and training and developing staff for updates on new trends in technology regarding facial recognition systems. The use of A.I. video analytics and digital ticketing ensures that no person gets into the sports stadium unchecked and unrecognized as a precaution to prevent any future crime in the sports stadium that may be caused by criminals who may have been brought into the stadium undetected.

One primary reason participants reported they perceived facial recognition as an effective security strategy was its ability to identify potentially dangerous individuals to ensure the safety of performers, staff, and guests. Further, the majority of the participants perceived facial recognition as unbiased. In contrast, a few participants provided discrepant data by indicating that F.R. may be biased sometimes based on who operates and controls the system. Overall, the findings imply that facial recognition can be an effective security strategy in combating criminal activities at the sports stadium. This security system strategy can prevent crime and deter violence at sports stadiums on the East Coast.

Research Question Two

How do sports stadium security managers perceive the effectiveness of technology such as biometric facial recognition software in preventing crime and deterring violence at sports stadiums on the East Coast?

Although facial recognition was perceived as the most effective security strategy to prevent crime and deter violence at sports stadiums on the East Coast, this strategy can be more effective when used with human oversight and multiple overlapping security strategies. In theme 1 of the first research question, participants perceived F.R. as part of an effective security strategy at sports stadiums. However, the findings indicated that other strategies considered effective in combination with F.R. technology for preventing crime and deterring violence could make F.R. more effective in preventing crime at sports stadiums. As a result, the participants perceived F.R. as most effective when it was utilized as part of a suite of prevention and deterrence strategies, including human insights. The findings demonstrate that human insights and intervention may help F.R. more effectively prevent crime and deter violence.

According to the participants, other strategies that can be used alongside the F.R. include having visible, strategically placed, uniformed security personnel and undercover security personnel. The findings indicate that other strategies to be used to help F.R. in detecting crime at sports stadiums included having proactively monitored camera surveillance; partnering with law enforcement; having security checkpoints with walkthrough metal detectors or magnetometer wands; enforcement of fan conduct policies; and human oversight of F.R. systems at the sports stadiums.

While facial recognition was perceived to be effective in preventing crime and deterring violence at sports stadiums, it was also perceived to raise some concerns about false identification, camera functionality, and privacy. The findings suggest that F.R. may have privacy and functionality issues when used to detect crime and deter violence at sports stadiums. Such limitations are associated with F.R. technology that requires human

oversight of the technology and further investigation after the technology is identified. False positives were one of the limitations of this strategy, as most participants believed that human oversight could prevent any resulting harm and that false positives with F.R. were rarer than false identifications with the unaided human eye. Participants also identified privacy concerns as a limitation of using facial recognition technology in preventing crime and deterring violence at sports stadiums on the East Coast, as cameras violated the privacy of the individuals being scanned through F.R. systems because not all persons getting into the stadiums can be criminals.

Research Question Three

Perceived Ease of Use (PEU): will learning to operate facial recognition technology in stadiums be challenging for security managers?

Technology can be challenging for users when introduced in their workplace. In this regard, security managers may need adequate training to learn how to use facial recognition systems. The findings indicated that participants perceived facial recognition technology as easy or moderately easy to learn how to use. Participants felt that they found it easy to learn how to use the technology as perceived ease of use made it less challenging to use in the sports stadiums. Participants highlighted that some training might be required for security managers, and after undergoing appropriate training, the facial recognition technology software was easy to learn and use.

Research Question Four

Perceived Usefulness (P.U.) How will this technology at stadiums improve security managers' productivity?

The findings revealed that with the right conditions in place at sports stadiums, facial recognition technology improves performance in preventing crime and acts of violence at sports stadiums on the East Coast. Participants perceived that when implemented under the right conditions, facial recognition technology can help improve the performance of security managers in preventing crime and acts of violence at sports stadiums on the East Coast. The conditions revealed by the participants included keeping individuals from watch lists out of venues, coordinating with law enforcement, and monitoring the venue to ensure limited security breaches by the criminals to the sports stadium.

Connection to the Theoretical and Conceptual Frameworks of this Study

The findings from this study align with the technology acceptance model, which can best describe the significance of technology in promoting stadium security (Davis, 2023). The technology acceptance model stresses that for technology to be accepted and used by a potential user, both the developer and user must share the belief that the developed technology is valuable and easy to use (Davis, 2023). As described by Davis et al. (2023), perceived usefulness and ease of use can significantly impact the implementation of technology, as in this case, at a sports stadium on the East Coast. The perceived usefulness of the technology acceptance model can be the extent to which individuals or organizations believe that using a given technology would improve their productivity and job performance (Davis, 2023). Further, perceived ease of use can be the extent to which a person believes using a particular technology would be effortless. Users are likely to accept and use technology systems that are accessible, less complex, and require minimal effort to install and use.

Throughout the findings of this study, facial recognition technology has been perceived to be important in enhancing security at the sports stadium. It helps detect criminals and their plans early, contributing to the potential prevention of crime and deterring violence to protect fans and athletes. This significance aligns with the perceived usefulness component of the technology acceptance model (Davis, 2023), which can make security managers of the selected sports stadiums on the East Coast accept and allow the installation and use of biometric facial recognition systems to enhance stadium security based on the systems' perceived usefulness. Perceived usefulness can prompt security managers at sports stadiums to consider accepting technology for enhanced performance in preventing crime and deterring violence in sports stadiums. According to the findings, facial recognition was perceived as most effective when used with human oversight and multiple overlapping security strategies. The current study findings also align with the technology acceptance model component of perceived ease of use (Davis, 2023).

As per the findings, facial recognition technology was perceived as easy or moderately uncomplicated to learn and use. According to Norfolk and O'Regan (2020), the system's privacy, compatibility with other security systems, and convenience influenced biometric systems' perceived usefulness and ease of use at sports stadiums.

Facial recognition technology was perceived as improving performance under the right conditions, indicating its perceived usefulness as indicated in the technology acceptance model component of perceived usefulness by Davis et al. (2023); individuals or organizations can perceive or believe that using a given technology would improve their productivity and job performance. Liu et al. (2021) revealed that while perceived

ease of use had no significant impact on individuals' decision to use face recognition software, perceived usefulness associated with accuracy and perceived enhanced security influenced the positive use of facial recognition systems.

The current study findings strongly connect with the technology acceptance model components of perceived ease of use and perceived usefulness of technology in sports stadiums by security managers. In sports stadiums and sporting activities, Yang and Cole (2020) revealed that smart stadiums employ a wide range of technologies to enhance the security and protection of fans and security personnel as well as enhance performance due to the ease of technology use and its usefulness in enhancing security performance in deterring violence at sports stadiums. As much as this study indicated some limitations of facial recognition technology, such as privacy concerns posing a security threat, technological and digital developments are critical in enhancing security at sports stadiums (Miraz & Ali, 2020). The findings have contributed to the technology acceptance model by revealing that perceived ease of use can be enhanced by promoting training and development of security managers who would accept the adoption of technology in sports stadiums.

Relationship between Results and Prior Research

The findings of this study indicate that participants perceive facial recognition technology (F.R.) as a significant component of an effective security strategy at sports stadiums. The use of facial recognition technology can help enhance the security of stadium fans and athletes by deterring crime and other violent behaviors. This aligns with the study by Flicker (2019), which found that the use of biometric technology at stadium entrances in arenas such as Madison Square Garden increased the safety of spectators and

athletes. The use of facial recognition technology enhanced the security of stadium fans and athletes by deterring crime and other violent behaviors (Dauvergne, 2022). Participants reported that facial recognition technology (F.R.) was a significant component of an effective security strategy at sports stadiums. The findings concur with previous research, which indicated that security managers could employ facial recognition technology when a suspected criminal act is about to occur or is already in progress, especially at sports stadiums with a huge gathering of spectators watching the games (Tóth, 2021). This can speed up response times, prevent or lessen the damage caused by such attacks, and ultimately save lives at sports stadiums.

The findings have contributed to previous research by revealing that an effective security system at sports stadiums can be achieved through hiring facial recognition technology systems experts and training and development staff for updates on new trends in technology regarding facial recognition systems. However, previous research indicated that installing sufficient CCTVs around the stadium improves security by helping the management monitor and identify fans causing violence and reminding fans that their behavior is monitored (Hutchins & Andrejevcic, 2021) rather than using CCTV as the sole security feature in stadiums. On the other hand, current findings align with Yusoff et al. (2020), who found that complementing the CCTVs with facial recognition software helped accurately identify and apprehend crime perpetrators.

The findings indicate that other strategies to help F.R. detect crime at sports stadiums included partnering with law enforcement and having security checkpoints with walkthrough metal detectors or magnetometer wands. This is similar to previous research, which revealed that the essence of having command and control centers in the

stadium is to allow security personnel to easily monitor facial recognition technology footage on both sides of the stadium (Hutchins & Andrejevcic, 2021). Kowalska (2019) stated that the security control in the stadium housed the public address systems, fully integrated closed-circuit television system for surveillance, alarm systems, turnstile monitoring capabilities, and control systems for stadium entrances. The stadium management can also upgrade their on-site security system with a mobile command center fitted with CCTV and connected to the control room, allowing accessible communication between security personnel manning the stadium (Hutchins & Andrejevcic, 2021).

Privacy concerns were identified as a limitation of using facial recognition technology in preventing crime and deterring violence at sports stadiums on the East Coast, as cameras violated the privacy of the individuals being scanned through F.R. systems. The findings suggest that privacy and functionality issues were evident when using F.R. to detect crime and deter violence at sports stadiums. The findings align with previous literature by Nijholt (2020), who indicated that as technology advances, so do the techniques for collecting, using, and analyzing biometric data, resulting in heightened security and privacy concerns, especially for the use of biometric facial recognition system in stadiums and sports arena (Nijholt, 2020).

Where stadiums use biometric data to track the movements of fans, there have been concerns about how this data is being used and the security of the collected data. With increased privacy concerns, Nijholt (2020) highlighted instances where stadiums are accused of selling this data to third parties, raising even more concerns. The findings of privacy concerns would help sports stadium management to ensure that biometric data

is collected and used to respect the privacy of those involved, including having biometric laws and regulations in process and biometric industry standards being tested. Research outcomes also revealed that security managers might need training on facial recognition technology software for ease of learning and use. Sports stadiums are a major spot for deploying and developing facial recognition technology. They are used to envision and model a spectator experience governed by the operation of automated surveillance and sensor-based monitoring systems, which promise greater security and enhanced consumption opportunities, prompting enhanced training among security managers for ease of use of the technology (Nyadera & Bincof, 2019).

The study outcomes showed that participants perceived facial recognition technology can help improve the performance of security managers in preventing crime and acts of violence at sports stadiums when implemented under the right conditions. The findings are consistent with past research by Rakhmanova et al. (2022), who revealed that individuals would adopt and use certain technology if they perceived it to improve their performance and productivity. Research data outcomes have contributed to the previous literature by establishing that implementing facial recognition technology in sports arenas improves security managers' performance in preventing crime and deterring violence in sports stadiums.

Limitations

This study had limitations. First, the individuals interviewed only represented a small group of security managers in charge of a security sports stadium on the East Coast. Therefore, external validity may be limited, making it difficult to generalize findings outside the context of the sports stadiums on the East Coast. Thus, the scope of

participants should be enlarged to accommodate different perspectives related to facial recognition technology.

This study was limited to sports stadiums and security managers in this area. This implies that the findings may not be transferable to settings and populations other than security managers and sports stadiums. Transferability also must include assurance that the sample is sufficient in size and composition (Korstjens & Moser, 2018).

Implications for Future Research

Several sports areas continue to warrant investigation from technological security perspectives. Future researchers may consider investigating multiple sports stadiums in larger, more diverse states other than the East Coast to enhance the transferability of findings. This may provide a deeper understanding of how to implement facial recognition with fidelity and effectively to meet the diverse needs of sports stadium security measures.

Future research examines training and development to enhance the use of facial recognition technology among not only the security managers in sports arenas but also in areas other than the sports settings, as this study was limited to sports stadiums and security managers in this area. This implies that the findings may not be transferred to other states and populations other than security managers and sports stadiums.

Since privacy concerns pose a security threat at sports stadiums, and technological and digital developments are critical in enhancing security at sports stadiums, further research should be conducted to determine effective strategies to protect data collected using facial recognition technology to ensure that the data privacy of individuals is respected.

Implications for Future Practice

The findings regarding the perceptions and attitudes of security managers about using facial recognition at sports stadiums may assist the security personnel in offering the greatest level of security and distributing government funding and resources, such as facial recognition software, to safeguard sports stadiums during various gaming activities. Facial recognition technology may assist law enforcement officials in creating policies and allocating resources for adopting facial recognition technology.

Law enforcement officers can use the research findings to understand the use of technology in tracing and detecting terrorism activities to protect the people in sports stadiums (Hutchins & Andrejevcic, 2021). The research results may help security managers implement policies in adopting and using facial recognition to safeguard sports stadiums. In enhancing stadium security, the security managers could also use the research findings to guide the security operations around the sports stadiums. Police enforcement may better prevent and investigate crimes, criminal acts, and improve stadium safety using facial recognition software technology (Tóth, 2021).

Conclusion

This study sought to determine how stadium security managers perceive and describe their experiences with biometric security systems, especially facial recognition software, to mitigate crime and violent behaviors in sports stadiums on the East Coast of the U.S. The results from this qualitative study demonstrate that facial recognition technology is a significant and effective strategy for enhancing security systems at sports stadiums by security managers. Understanding security managers' perceptions and

attitudes may help implement facial recognition strategies in safeguarding sports stadiums.

Given the widespread issues regarding violence at sporting events and stadiums, the research findings may help to understand whether extreme violence may decrease through enhanced crowd control techniques mixed with the latest in surveillance and security technologies. Although security managers can perceive facial recognition as raising privacy concerns about false identification and functionality, it was perceived as easy to learn and improves performance under the right conditions, highlighting its perceived usefulness. The findings have aided in filling the gap in research by answering research questions indicating the perspectives of security managers regarding the usefulness of facial recognition technology in enhancing security at sports stadiums on the East Coast. Further research can be conducted to determine how effective training of security managers in technology contributes to the improved performance of facial recognition technology.

This study included interviews with 20 security managers from major sports arenas and venues on the East Coast. The survey responses and interviews demonstrate that facial recognition technology is a significant and effective strategy for enhancing security systems at sports stadiums by security managers. Understanding security managers' perceptions and attitudes may help implement facial recognition strategies in safeguarding sports stadiums. Crime and violence can never be eliminated; we can take additional steps to counter it.

APPENDIX A: INTRODUCTION LETTER TO PARTICIPANTS

Good morning:

My name is Darnell R. Downes, I am a doctoral candidate at St John's University's Lesley H. and William L. Collins College of Professional Studies: Criminal Justice, Legal Studies and Homeland Security Division. I am also a Police Sergeant within the New York City Police Department. I am requesting your assistance and participation in a research project (online survey) as part of my doctoral dissertation. I am conducting a study on traditional sports stadium security and facial recognition biometrics to prevent crime and violence in sports arenas.

I am hopeful that the results of this research, informed by security executives and managers such as yourselves, will help facial recognition technology in stadium security, in preventing violence and crime. The amount of time, effort, and resources involved in your participation will be minimal. The survey consists of 13 questions that require your answer and open space for dialogue if you wish to elaborate on any element of the survey. It is anticipated that the survey will take no longer than 15 minutes to complete. The survey is anonymous, you will not be asked to furnish any biographical data that can identify you, and I will not be provided with your personally identifiable information or email address. All data collected for this dissertation will be used only for the purposes of the research phase of the dissertation, which may culminate in publications and or presentations. The data collected from this survey will be collected anonymously and analyzed in the aggregate.

It is not being conducted or sponsored by any government agency. Your participation is purely voluntary; however, it would be greatly appreciated and considered a valuable contribution to this research project. It is my sincere hope that the information gained from this research will help homeland security agencies and security professionals achieve their mission in protecting sports arenas/venues, from crime and violent acts. Hopefully, it will help improve morale and quality of life for employees of these arenas.

I would like to thank you in advance for considering this request and hope you agree to participate in this research project. If there is anything about the study or your participation that is unclear or that you do not understand if you have questions or wish to report a research-related problem, you may contact me at 516-743-8241, Darnell.Downes19@my.stjohns.edu, or my faculty director, Dr. Bernard Jones, at 718-390-4176, jonesb1@stjohns.edu. For questions about your rights as a research participant, you may contact the University's Institutional Review Board, St John's University, Dr. James O'Keefe, IRB Coordinator, okeefej@stjohns.edu, 718-390-4432.

Respectfully,

Darnell R. Downes

Doctoral Student

St John's University

TITLE OF STUDY

AN ANALYSIS OF TRADITIONAL SPORTS STADIUM SECURITY AND FACIAL RECOGNITION BIOMETRICS TOWARDS THE PREVENTION OF CRIME AND VIOLENCE IN SPORTS ARENAS

PRINCIPAL INVESTIGATOR

Darnell R. Downes

Doctoral Student

St John's University

8000 Utopia Parkway

Queens NY 11439

(516) 743- 8241

Darnell.Downes19@my.stjohns.edu

PURPOSE OF STUDY

You are being asked to take part in a research study. Before you decide to participate in this study, it is important that you understand why the research is being done and what it will involve. Please read the following information carefully. Please ask the researcher if there is anything that is not clear or if you need more information. The purpose of this study is to explore how sports stadium security managers perceive and describe their experiences with biometric security systems, specifically facial recognition software, to mitigate crime and violent behaviors in sports stadiums located on the east coast of the United States.

STUDY PROCEDURES

The amount of time required of each participant will be no longer than 60 minutes for the interview and 15 minutes to complete the survey. The researcher will establish an agreed-upon day and time with the participants for the interviews. Interviews will be audio-recorded, transcribed through the Webex transcription application, and emailed to each participant for member checking.

RISKS

There are no risks to this participation. You may decline to answer any or all questions and you may terminate your involvement at any time if you choose.

BENEFITS

There will be no direct benefit to you for your participation in this study. However, we hope that the information obtained from this study may increase security protocols in and around sports arenas using facial recognition technology or with standard protocols.

CONFIDENTIALITY

Your responses to this survey will be anonymous. Please do not write any identifying information on your survey or for the purposes of this research study, your comments will not be anonymous. Every effort will be made by the researcher to preserve your confidentiality including the following:

- Assigning code names/numbers for participants that will be used on all research notes and documents.
- Notes, interview transcriptions, and any other identifying participant information will be enclosed and locked on the researcher's laptop, in the personal possession of the researcher.

Participant data will be kept confidential except in cases where the researcher is legally obligated to report specific incidents. These incidents include, but may not be limited to, incidents of abuse and suicide risk.

CONTACT INFORMATION

If you have questions at any time about this study, or you experience adverse effects as a result of participating in this study, you may contact the researcher whose contact information is provided on the first page. If you have questions regarding your rights as a research participant, or if problems arise that you do not feel you can discuss with the Primary Investigator, please contact the Institutional Review Board at (865) 354-3000, ext. 4822.

VOLUNTARY PARTICIPATION

Your participation in this study is voluntary. It is up to you to decide whether or not to take part in this study. If you decide to take part in this study, you will be asked to sign a consent form. After you sign this consent form, you are still free to withdraw at any time and without giving a reason. Withdrawing from this study will not affect the relationship you have, if any, with the researcher. If you withdraw from the study before data collection is completed, your data will be returned to you or destroyed.

CONSENT

I have read and understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study.

Participant's signature _____Date _____

Investigator's signature _____Date _____

APPENDIX B: SURVEY INSTRUMENT / INTERVIEW TOOL

Name (please print):

_____

Interviewer: _____ Date: _____

Years of experience with your organization, please select one:

1 to 5 years of experience

5 to 10 years of experience

10 to 20 years of experience

Job title, please select one:

Chief Security Officer

Director of Security

Security Manager

Directions: The following questions will try to explore the understanding of the importance of the use of facial recognition technology in security risk management from your experience. These questions will help try to gain an understanding of the facial recognition technology, maintenance, and compliance from your experience. Finally, these questions will try to explore your knowledge of how organizational security posture is affected due to timely or non-timely data collection on security controls.

APPENDIX C: INTERVIEW QUESTIONS (SURVEY MONKEY)

Process Required Ease of Use for Facial Recognition Technology

Pre-Screening Question:

Are you a Director of Security, Chief Security Officer, or Security Manager in a sports arena/sports venue?

1. Describe what methods are required to collect security data within your organization.

2. How can facial recognition technology protect your stadium?

3. Do you think other security measures can perform a better job than facial recognition?

4. Describe a “Secure” arena.

5. Do you think facial recognition is racially biased?

6. Does facial recognition increase the risk of false alerts on individuals?

7. Are there any health risks using facial recognition technology equipment?

8. How will the use of facial recognition affect privacy concerns in your stadium?

9. What are some equipment issues faced during the use of facial recognition in the stadium?

10. What security methods can improve the effectiveness of the data collection process for compliance and improve organizational security posture?

11. Would using the facial recognition technology at your stadium improve performance in doing your job?

12. How easy is it to operate facial recognition technology?

13. On a scale from 1-10, how likely is it that using the technology would improve your work performance?

14. How easy is it to operate facial recognition technology?

- Very Easy
- Easy
- Neither Easy nor Difficult
- Difficult
- Very difficult
- Why?

15. What strategies do sports stadium security managers describe as effective in preventing crime and acts of violence in their stadiums?

16. Would you like to be included in a brief follow-up interview?

APPENDIX D: THANK YOU LETTER TO PARTICIPANTS

Dear _____,

I would like to thank you for your time for an interview and for sharing your experiences with me regarding facial recognition technology. Attached, please find the transcript of your interview. Please review the transcript for accuracy, and while reviewing, if you think some vital information is required, please do not hesitate to contact me. The transcript is captured as is and may have some grammatical errors, and you can ignore these. Once reviewed, please return if there are updates to the transcript as a soft copy within an email. All electronic records will be encrypted, and no personally identifiable information is retained. Once again, I would like to thank you and appreciate your time given for this research by sharing your experiences with me. If you have any questions or concerns, please feel free to contact me anytime by email.

Very Respectfully,

Darnell R. Downes

Doctoral Candidate

St John's University

REFERENCES

Allan, G. (2020). Qualitative research. In G. Allan, & C. Skinner (Eds.), *Handbook for research students in the social sciences* (pp. 177-189). Routledge.

Ashwin, P. (2022). *Mitigating lone actor terrorist threats to events in the United States: The application of risk-informed counterterrorism strategies for event organizers A narrative literature review.* (Doctoral Thesis, University of Leicester). https://doi.org/10.13140/RG.2.2.10142.20808/1

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research? *Qualitative Sociology, 42*(2), 139-160. https://doi.org/10.1007/s11133-019-9413-7.

Atkinson, C., & Murray, K. (2021). Leaving 'home?' Belonging, break-up and becoming in the police family. *The British Journal of Criminology*, *61*(2), 345-363. https://doi.org/10.1093/bjc/azaa066

BBC News. (2014). Privacy fears over FBI facial recognition database. *BBC News.* https://www.bbc.com/news/technology-27037009

Bicchieri, C., & Dimant, E. (2019). Nudging with care: The risks and benefits of social information. *Public Choice, 191*(3-4), 443–464. https://doi.org/10.1007/s11127-019-00684-6

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *2*6(13), 1802-1811. https://doi.org/10.1177/1049732316654870

Block, K., & Kaplan, J. (2023). An analysis of National Hockey League playoff games and city-level crime counts. *Crime & Delinquency, 69*(11), 2194-2217. https://doi.org/10.1177/00111287221118879

Brandt, S. (2023). Editor's Introduction to the Special Issue: Misogyny: Psychoanalytic and interdisciplinary perspectives. I*nternational Journal of Applied Psychoanalytic Studies, 20*(3), 398-402. https://doi.org/10.1002/aps.1835

Braun, V., & Clarke, V. (2006). Qualitative research in psychology. Routledge.

Brosnan, S. (2019). The impact of sports participation on crime in England between 2012 and 2015. *Sport in Society, 23*(6), 1080–1090. https://doi.org/10.1080/17430437.2019.1631805

Campbell, T. (2023). 'The enemy within': Football hooliganism and the miners' strike. *Sport in History, 43*(1), 81-102. https://doi.org/10.1080/17460263.2022.2091654

Chess, P. S. (2017). Chapter 3: Validity and reliability in qualitative research. GCU doctoral research: Advanced qualitative research methods. Pamukkale University *Journal of Social Sciences Institute.* https://www.researchgate.net/publication/362418590_Validity_and_Reliability_in_Qualitative_Research

Choudhary, T., Virmani, C., & Juneja, D. (2019). Convergence of blockchain and IOT: An edge over technologies. In E. Hassanien, R. Bhatnagar, N. Eldeen M. Khalifa, M. H. N. Taha (Eds.), *Toward social internet of things (SIOT): Enabling technologies, architectures, and applications*, (pp. 299–316). Springer. https://doi.org/10.1007/978-3-030-24513-9_17

Circo, G., McGarrell, E. F., Rogers, J. W., Krupa, J. M., & De Biasi, A. (2022). Assessing causal effects under treatment heterogeneity: An evaluation of a CCTV program in Detroit. *Journal of Experimental Criminology.* https://doi.org/10.1007/s11292-022-09519-9

Cleland, J. (2019). Sports fandom in the risk society: Analyzing perceptions and experiences of risk, security, and terrorism at elite sports events. *Sociology of Sport Journal*, *36*(2), 144–151. https://doi.org/10.1123/ssj.2018-0039

Cleland, J., & Cashmore, E. (2018). Nothing will be the same again after the Stade de France Attack: Reflections of association football fans on Terrorism, security, and surveillance. *Journal of Sport and Social Issues*, *42*(6), 454–469. https://doi.org/10.1177/0193723518797028

Copus, R., & Laqueur, H. (2019). Entertainment as crime prevention: Evidence from Chicago sports games. *Journal of Sports Economics*, *20*(3), 344–370. https://doi.org/10.1177/1527002518762551

Cox, R., Russell, D., & Vamplew, W. (2020). Encyclopedia of British football.

CyberLink. (2022). New CyberLink report finds over 131 million Americans use facial recognition daily and nearly half of them to access three applications or more each day. https://www.CyberLink.com/eng/press_room/view_4899.html

Dauvergne, P. (2022). The globalization of facial recognition technology. In P. Dauvergne (Ed.), *Identified, tracked, and profiled* (pp. 76-87). Edward Elgar Publishing. https://doi.org/10.4337/9781803925899.00015

Davis, F. D., Granić, A., & Marangunić, N. (2023). The technology acceptance model 30 years of TAM. *The Technology Acceptance Model*. Springer.

Deflem, M., & Chicoine, S. (2018). Policing terrorism. In M. Deflem (Ed.), *The handbook of social control*, 235-248. John Wiley & Sons Ltd.

Diaz, C., Haines, A., Richardson, O., Brooks, W., Ward, K., Albert, K., Amos, T., Baker, A. J., Beck, A., & Clemens, Z. (2019). *A threat assessment and security analysis*

of the three sports facilities of Indiana University-Purdue University, Indianapolis NCAA Softball Fields, Carroll Stadium, and the IU Natatorium. https://scholarworks.iupui.edu/items/1b2578f0-bbcd-47bc-841d-da26ac6c26a5

Dulock, H. L. (1993). Research design: Descriptive research. *Journal of Pediatric Oncology Nursing, 10*(4), 154-157. https://doi.org/10.1177/104345429301000406

Eck, J. E., & Clarke, R. V. (2019). Situational crime prevention: Theory, practice, and evidence. In J. D. McLeod, E. J. Lawler, & M. Schwalbe (Eds.), *Handbook of sociology and social research*, (pp. 355–376). https://doi.org/10.1007/978-3-030-20779-3_18

Ekmekci, P. E., Done, K., Arda, B., & Ekmekci, A. B. (2018). Beyond a game: Peer education to separate football and violence. *International Online Journal of Education and Teaching (IOJET), 5*(1), 180-188. http://iojet.org/index.php/IOJET/article/view/231/224

Eller, E., & Frey, D. (2019). Psychological perspectives on perceived safety: Social factors of feeling safe. *Risk Engineering*, 43–60. https://doi.org/10.1007/978-3-030-11456-5_4

Engelberg, T., & Moston, S. (2020). Crime and misconduct in Sport. Sport in Society, 23(6), 975–980. https://doi.org/10.1080/17430437.2020.1766814

Faraji, R., Hemmatinezhad, M., & Taylor, T. (2018). Critical factors affecting stadium security. *Journal of Applied Security Research, 13*(4), 473–488. https://doi.org/10.1080/19361610.2018.1498264

Flicker, K. (2019). The prison of convenience: The need for national regulation of biometric technology in sports venues. *Fordham Intellectual Property, Media and*

Entertainment Law Journal, 30, 985-1043. https://ir.lawnet.fordham.edu/iplj/vol30/iss3/7

Forbes, Y. (2019). *'The revolution will not be televised': Reimagining the role of black women in the freedom struggle.* Charlotte Teachers Institute. https://charlotteteachers.org/wp-content/uploads/2021/01/YForbes_CTI-CU_11-16-20.pdf

Frey, B. B. (2018). Convenience sampling. *The SAGE encyclopedia of educational research, measurement, and evaluation*. https://doi.org/10.4135/9781506326139.n155

Gardocka, T., & Jagiełło, D. (2022). Crimes related to mass events-criminal-legal and evidentiary issues. *Mykolas Romeris University Research Management System (CRIS).* https://cris.mruni.eu/cris/handle/007/18557

Gildersleeve, R. E., & Guyotte, K. W. (2020). Readymade methodology. *Qualitative Inquiry, 26*(8-9), 1122-1130. https://doi.org/10.1177/1077800419881661

Grant, C., & Oslanoo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." *Administrative Issues Journal, 4*(2), 12–26. https://dc.swosu.edu/aij/vol4/iss2/4

Gronmo, S. (2019). Social research methods. Sage Publishing.

Guba, E. G., & Lincoln, Y. S. (1982). Epistemological and methodological bases of naturalistic inquiry. *Educational Technology Research and Development, 30*(4), 233-252. https://doi.org/10.1007%2FBF02765185

Hall, S. (2012). Effective security management of university sports venues. *Sport Journal, 9*(4), 1-10. https://www.cabdirect.org/cabdirect/abstract/20073141280

Harati, S. H., Ashraf Ganjouei, F., Amirtash, A., & Nikaeen, Z. (2019). Investigating the physical security dimensions affecting volleyball stadium security. *Journal of System Management, 5*(1), 191-210. https://doi.org/20.1001.1.23222301.2019.5.1.9.0

He, Q., Xin, X., & Yang, Q. (2021). Security analysis and improvement of a quantum multi-signature protocol. *Quantum Information Processing*, *20*, 1-21. https://doi.org/10.1007/s11128-020-02962-5

Herrera, E. (2018). Masculinity, violence, and deindividuation in Argentine soccer chants: The sonic potentials of participatory sounding-in-synchrony. *Ethnomusicology, 62*(3), 470–499. https://doi.org/10.5406/ethnomusicology.62.3.0470

Hong, Q. N., Pluye, P., Bujold, M., & Wassef, M. (2017). Convergent and sequential synthesis designs: implications for conducting and reporting systematic reviews of qualitative and quantitative evidence. *Systematic Reviews, 6*(61), 1-14. https://doi.org/10.1186/s13643-017-0454-2

Hutchins, B., & Andrejevcic, M. (2021). Olympian surveillance: Sports stadiums and the normalization of biometric monitoring. *International Journal of Communication,* 15-20. https://ijoc.org/index.php/ijoc/article/view/16377

Jakar, G. S., & Gordon, K. O. (2022). Dead spaces: Sports venues and police stop in a major league, upper midwestern city in the United States. Journal of Sport Management, 36(4), 355–368. https://doi.org/10.1123/jsm.2021-0080

Jansen, A. M., Giebels, E., van Rompay, T. J., & Junger, M. (2018). The influence of the presentation of camera surveillance on cheating and pro-social behavior. *Frontiers in Psychology, 9*. https://doi.org/10.3389/fpsyg.2018.01937

Janofsky, A. (2019). *Stadiums weed out disruptive fans with facial recognition.* https://www.wsj.com/articles/stadium-weeds-out-disruptive-fans-with-facial-recognition-11567589403

Jones, J., & Smith, J. (2017). Ethnography: Challenges and opportunities. *BMJ Journal: Evidence-Based Nursing, 20*(4), 1-8. https://doi.org/10.1136/eb-2017-102786

Kaiser, K. (2009). Protecting respondent confidentiality in qualitative research. *Qualitative Health Research, 1*9(11), 1632-1641. https://doi.org/10.1177/1049732309350879

Koh, E. T., Owen, W. L., Koh, E. T., & Owen, W. L. (2000). Descriptive research and qualitative research. In E. T. Koh, W. L. Owen (Eds.), *Introduction to nutrition and health research*, (pp. 219-248). https://doi.org/10.1007/978-1-4615-1401-5_12

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice, 2*4(1), 9-18. https://doi.org/ 10.1080/13814788.2017.1375091

Kossakowski, R. (2020). 'You have to scream your head off!' mechanical solidarity and rules of gathering: Structural dimensions of fandom culture. *Hooligans, Ultras, Activists*, 17–57. https://doi.org/10.1007/978-3-030-56607-4_2

Kowalska, J. E. (2019). Prevention of Hooligan Behavior at football stadiums. *Journal of Education, Health, and Sport, 9*(11), 206–216. https://doi.org/10.12775/jehs.2019.09.11.018

Kurland, J. (2019). Arena-based events and crime: An analysis of hourly robbery data. *Applied Economics, 51*(36), 3947–3957. https://doi.org/10.1080/00036846.2019.1587590

Lange, E., & Young, S. (2019). Gender-based violence as difficult knowledge: Pedagogies for rebalancing the masculine and the feminine. *International Journal of Lifelong Education, 38*(3), 301–326. https://doi.org/10.1080/02601370.2019.1597932

Leitner, M. C., & Richlan, F. (2021). Analysis system for emotional behavior in football (ASEB-F): Matches of FC Red Bull Salzburg without supporters during the COVID-19 pandemic. *Humanities and Social Sciences Communications, 8*(1). https://doi.org/10.1057/s41599-020-00699-1

Levine, D. (2014). *Even you can learn statistics and analytics: An easy-to-understand guide to statistics and analytics.* Pearson FT Press.

Liu, T., Yang, B., Geng, Y., & Du, S. (2021). Research on face recognition and privacy in China—based on social cognition and cultural psychology. *Frontiers in Psychology, 12*. https://doi.org/10.3389/fpsyg.2021.809736

Loyens, K., Claringbould, I., Rossem, L. H., & van Eekeren, F. (2021). The social construction of integrity: A qualitative case study in Dutch football. *Sport in Society, 25*(9), 1714–1733. https://doi.org/10.1080/17430437.2021.1877661

Ludvigsen, J. A. L. (2022). Football and risk: Trends and perspectives. Routledge. https://doi.org/10.4324/9781003303480

Lynch, J. (2020). Face off: Law enforcement use of face recognition technology. *Electronic Frontier Foundation (EFF).* https://dx.doi.org/10.2139/ssrn.3909038

MacKenzie, A. (2023). A feminist postdigital analysis of misogyny, patriarchy, and violence against women and girls online. In P., MacKenzie, A., & Knox, J. (Eds.), *Constructing postdigital research: Method and emancipation* (pp. 275-294). Springer Nature.

Mailizar, M., Burg, D., & Maulina, S. (2021). Examining university students' behavioral intention to use e-learning during the COVID-19 pandemic: An extended tam model. *Education and Information Technologies, 26*(6), 7057–7077. https://doi.org/10.1007/s10639-021-10557-5

Mares, D., & Blackburn, E. (2019). Major league baseball and crime: Opportunity, spatial patterns, and team rivalry at St. Louis Cardinal Games. *Journal of Sports Economics, 20*(7), 875–902. https://doi.org/10.1177/1527002518822702

Marganski, A. J. (2019). Making a murderer: The importance of gender and violence against women in mass murder events. *Sociology Compass, 13*(9), e12730. https://doi.org/10.1111/soc4.12730

McChesney, K., & Aldridge, J. (2019). Weaving an interpretivist stance throughout mixed methods research. *International Journal of Research & Method in Education, 42*(3), 225-238. https://doi.org/10.1080/1743727X.2019.1590811

McGovern, C. (2023). Fenway and Crime: Opportunity, Geographic Differences, and Team Rivalry at Boston Red Sox Games. *Empirical Economic Bulletin, An*

Undergraduate Journal, *16*(1), 2. https://digitalcommons.bryant.edu/cgi/viewcontent.cgi?article=1211&=&context=eeb&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fstart%253D10%2526q%253Dcrime%252Bsports%252Bstadiums%2526hl%253Den%2526as_sdt%253D0%252C48%2526as_ylo%253D2022#search=%22crime%20sports%20stadiums%22

Menaker, B. E., & Sheptak, D. R. (2020). The impact of game day on crime on a university police department: Application of the civilizing process to sport-related law enforcement. *Journal of Policy Research in Tourism, Leisure and Events, 12*(2), 172–184. https://doi.org/10.1080/19407963.2018.1556675

Miraz, M. H., & Ali, M. (2020). Integration of blockchain and IoT: an enhanced security perspective. *Annals of Emerging Technologies in Computing (AETiC),4*(4), 52-63. https://doi.org/10.48550/arXiv.2011.09121

Morgan, H., Parker, A., Meek, R., & Cryer, J. (2019). Participation in sport as a mechanism to transform the lives of young people within the criminal justice system: An academic exploration of a theory of change. *Sport, Education, and Society, 25*(8), 917–930. https://doi.org/10.1080/13573322.2019.1674274

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report. U.S.* Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education, 8*, 90–97. https://doi.org/10.1007/s40037-019-0509-2

Newson, M. (2017). Football, fan violence, and identity fusion. *International Review for the Sociology of Sport, 54*(4), 431–444. https://doi.org/10.1177/1012690217731293

Nijholt, W. (2020). Stadium security. *Intersec: The Journal of International Security, 30*(3), 32–34. https://www.intersecmag.co.uk/wp-content/uploads/2020/03/032-034_Stadium-security_March20_Final_2_JDW.pdf

Norfolk, L., & O'Regan, M. (2020). Biometric Technologies at music festivals: An extended technology acceptance model. *Journal of Convention & Event Tourism, 22*(1), 36–60. https://doi.org/10.1080/15470148.2020.1811184

Nyadera, I. N., & Bincof, M. O. (2019). Human security, terrorism, and counterterrorism: Boko Haram and the Taliban. *International Journal on World Peace, 36*(1), 7-32. https://www.jstor.org/stable/26883662

Olszewski-Strzyżowski, D. J. (2018). European societies' access to sport – the European Union actions. *Geosport for Society, 9*(2), 71–81. http://geosport.uoradea.ro/2018_2/2018_2_GSS_Olszewski_18.09.03.040.pdf

Piepiora, P., Sikorski, W., & Supiński, J. (2019). Security measures used in Poland during football matches. *Journal of Education, Health, and Sport, 9*(10), 172–188. https://apcz.umk.pl/JEHS/article/view/27609

Pistone, I., Eriksson, E., Beckman, U., Mattson, C., & Sager, M. (2019). A scoping review of interventions for preventing and countering violent extremism: Current

status and implications for future research. *Journal for Deradicalization, 19*, 1-84. https://journals.sfu.ca/jd/index.php/jd/article/view/213

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention. *Criminology & Public Policy, 18(*1), 135–159. https://doi.org/10.1111/1745-9133.12419

Purvis, R. S., Ayers, B. L., Bogulski, C. A., Kaminicki, K. F., Haggard-Dugg, L. K., Riklon, L. A., Iban, A., Mejbon-Samuel, R., Lakmis, R., Riklon, S., Thompson, J. W., & McElfish, P. A. (2021). Multicomponent informed consent with Marshallese participants. *Journal of Empirical Research on Human Research Ethics, 16*(3), 144-153. https://doi.org/10.1177/15562646211005651

Pyun, H., & Hall, J. C. (2019). Does the presence of professional football cause crime in a city? evidence from Pontiac, Michigan. *Applied Economics*, *51*(36), 3958–3970. https://doi.org/10.1080/00036846.2019.1588942

Rakhmanova, E. N., Tihanyi, M., & Szabolcs, M. (2022). The legal and organizational basis of ensuring the safety of sports activities in Hungary. *Bulletin of St. Petersburg University. Law, 13*(3), 759-770. https://doi.org/10.21638/spbu14.2022.311

Ristea, A., Al Boni, M., Resch, B., Gerber, M. S., & Leitner, M. (2020). Spatial crime distribution and prediction for sporting events using social media. *International Journal of Geographical Information Science*, *34*(9), 1708–1739. https://doi.org/10.1080/13658816.2020.1719495

Robin, L., Peterson, B. E., & Lawrence, D. S. (2020). How do close-circuit television cameras impact crimes and clearances? an evaluation of the Milwaukee Police

Department's Public Surveillance System. *Police Practice and Research, 22*(2), 1171–1190. https://doi.org/10.1080/15614263.2020.1772783

Rossmo, D. K., & Summers, L. (2019). Offender decision-making and displacement. *Justice Quarterly, 38*(3), 375–405. https://doi.org/10.1080/07418825.2019.1666904

Sandelowski, M. (2000). Whatever happened to qualitative description? *Research in Nursing & Health, 23*(4), 334-340. https://doi.org/10.1002/1098-240X(200008)23:4<334::AID-NUR9>3.0.CO;2-G

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*, 63-75.

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications.

Su, Y., & Li, M. (2021). Applying technology acceptance model in online entrepreneurship education for new entrepreneurs. *Frontiers in Psychology, 12.* https://doi.org/10.3389/fpsyg.2021.713239

Sylas, E. I. (2006). *Terrorism: A global scourge.* AuthorHouse

Thabet, H. (2022). Football in Egypt: Between joy and politics. A.E Ayuk (Ed.), *Football (Soccer) in Africa*. (pp. 147-163). Palgrave Macmillan https://doi.org/10.1007/978-3-030-94866-5_7

Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine, 27*(9), 1-10. https://doi.org/10.1177/2050312118822927

Tiell, B., & Cebula, K. (2020). *Governance in sport: Analysis and application.* Human Kinetics Publishers.

Tóth, A. N. (2021). Technological innovations in the field of sports policing. *Часопис Національного Університету Острозька Академія, 1*(23), 21-24. https://lj.oa.edu.ua/articles/2021/n1/21tnaosp.pdf

Van Ham, T., Blokland, A., Ferwerda, H., Doreleijers, T., & Adang, O. (2019). Determinants of persistence in collective violence offending. *Deviant Behavior, 42*(1), 37–53. https://doi.org/10.1080/01639625.2019.1649954

Vandeviver, C., Bernasco, W., & Van Daele, S. (2019). Do sports stadiums generate crime on days without matches? A natural experiment on the delayed exploitation of criminal opportunities. *Security Journal, 32*(1), 1–19. https://doi.org/10.1057/s41284-018-0142-5

Van Valkenburgh, S. P. (2021). Digesting the red pill: Masculinity and neoliberalism in the manosphere. *Men and Masculinities, 24*(1), 84-103. https://doi.org/10.1177/1097184X18816118

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterizing and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology, 18*, 1-18. https://doi.org/10.1186/s12874-018-0594-7

Welsh, B. C., Piza, E. L., Thomas, A. L., & Farrington, D. P. (2019). Private security and closed-circuit television (CCTV) surveillance: A systematic review of function and performance. *Journal of Contemporary Criminal Justice, 36*(1), 56–69. https://doi.org/10.1177/1043986219890192

Yang, C., & Cole, C. L. (2020). Smart stadium as a laboratory of Innovation: Technology, sport, and datafied normalization of the fans. *Communication & Sport, 10*(2), 374–389. https://doi.org/10.1177/2167479520943579

Yin, R. (2015). Case study research: Design and methods (2nd ed.). Sage Publishing.

Yusoff, N. H., Tahir, Z., & Hamzah, S. (2020). Security systems to preventing misbehavior among football fans in Malaysia: How effective it is? *Journal of Physics: Conference Series, 1529*(2), 022009. https://doi.org/10.1088/1742-6596/1529/2/022009

Vita

Name	Darnell R. Downes
Baccalaureate Degree	Bachelor of Arts, Touro University, Brooklyn, NY Major: Psychology
Date Graduated	January, 2009
Other Degrees and Certificates	Master of Arts, Seton Hall University, South Orange, NJ. Major: Human Resources & Training Development
Date Graduated	July, 2016