The Effect of General Deterrence Variables on Oversight of Florida's Driver and Vehicle Information Database (DAVID)

A Dissertation submitted to
the Graduate School
Valdosta State University

in partial fulfillment of the requirements for the degree of

DOCTOR OF PUBLIC ADMINISTRATION

in Public Administration

in the Department of Political Science
of the College of Humanities & Social Sciences

March 2022

Gary B. Gordon

M.P.A., Troy University, 2016
B.A., Saint Leo University, 2013

This dissertation, "The Effect of General Deterrence Variables on Oversight of the Driver and Vehicle Information Database (DAVID)," by Gary B. Gordon is approved by:

Dissertation Committee Chair

DocuSigned by:
Carol Glen
ADEA3EBF2287460...

Carol M. Glen, Ph.D.
Professor, Political Science & Public Administration

Committee Members

DocuSigned by:
Minsun Song
81637642 9FBB442...

Minsun Song, Ph.D.
Assistant Professor, Political Science & Public Administration

DocuSigned by:
Albert Murillo
41F4ECB8D480415...

Albert G. Murillo, Ph.D.
Human Resource Research Manager
Hillsborough County Sheriff's Office

Associate Provost for Graduate Studies and Research

Becky K. da Cruz

Becky K. da Cruz, Ph.D., J.D.
Professor of Criminal Justice

Defense Date 03/23/2022

FAIR USE

DUPLICATION

I authorize the Head of Interlibrary Loan or the Head of Archives at the Odum Library at Valdosta State University to arrange for duplication of this dissertation for educational or scholarly purposes when so requested by a library user. The duplication shall be at the user's expense.

Signature 

I refuse permission for this dissertation to be duplicated in whole or in part.

Signature_____

ABSTRACT

The Driver and Vehicle Information Database, known as DAVID, is a database operated by the Florida Highway Safety and Motor Vehicles and is used by many law enforcement agencies as an important investigative tool due to the information contained within. One important function of the agencies that allow their employees access to DAVID is to ensure the information is secured and not misused in violation of federal and state law, under a provision known as the Driver Privacy and Protection Act codified in 18 U.S.C. § 2721 (1994). Literature on general deterrence suggests that methods can be taken from an oversight standpoint that would allow for better control and deter users from misusing the data contained within DAVID. This study hypothesized that, if provided, standard operating procedures, ethics training, acceptable use policies, and consistent disciplinary procedures would act to improve oversight and be effective general deterrents against such misuse. The study tested the hypotheses using (n = 86) DAVID points of contact from various police agencies in Florida by way of an online survey. The results indicated a statistically significant relationship between standard operating procedures and acceptable use policies on oversight and deterrence. The null hypothesis could not be rejected regarding ethics training and disciplinary procedures on oversight and deterrence. The results supported two of the four hypotheses, and they may serve as a pathway to develop better administrative policies and procedures to improve the oversight process and help deter users from misusing DAVID in violation of law.
Keywords: D.A.V.I.D., DPPA, FLHSMV, driver license, point of contact

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

AUP	Acceptable Use Policy
DAVID	Driver and Vehicle Information Database
DPPA	Driver Privacy and Protection Act (1994)
EI	Early Intervention
ELVIS	Electronic License and Vehicle Information System
EWS	Early Warning System
FCIC	Florida Crime Information Center
FLHSMV	Florida Highway Safety and Motor Vehicles
IRB	Institutional Review Board
LEEP	Law Enforcement Enterprise Portal
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NDEx	National Data Exchange
NGI	Next Generation Identification
OIG	Office of the Inspector General
POC	Point of Contact
SOP	Standard Operating Procedure(s)
UCR	Uniform Crime Report

ACKNOWLEDGEMENTS

I want to express my sincerest appreciation and thanks to my committee for their support and encouragement on this journey. Dr. Carol M. Glen, my committee chair, Dr. Minsun Song; and Dr. Albert G. Murillo. You all helped turned the idea of this project into fruition, and I could not have done it without you.

My completion of this project would not be possible without the amazing friends and fellow students in the DPA 2017 cohort. I want to pay special thanks to my classmates Dr. Jessica, who became my doctoral concierge, Dr. Chris, and soon-to-be Dr. Marlon. Of course, my closest and dearest, Dr. Tanya, who talked me off the ledge and kept on me when I wanted to walk away from this project. Our weekly Sunday night phone call status checks kept me focused on moving forward. Thank you! Now look at us!

I want to acknowledge my brothers, sisters, and supervisors of the Hillsborough County Sheriff's Office who covered for me when I had to miss work to work on this project, giving me time off, and always keeping the fire lit under me so I would finish. I'm no longer 10–6 working on becoming a doctor!

Finally, the love support of my family and friends who struggled through this with me. Mom, Dad (miss you), Chase, Canin, and big little sis, Wendy! My heartfelt thanks.

DEDICATION

I dedicate this to my Chase, Canin, Uncle Ron, my mom, Maureen, and my late father, Ephraim.

Chapter I

INTRODUCTION

Driver and Vehicle Information Database

The Department of Florida Highway Safety Motor Vehicles (FLHSMV) maintains and authorizes the use of the Driver and Vehicle Information Database (DAVID) to over 900 agencies around the country. DAVID is a secure, online database accessed through the internet that allows an authorized user to retrieve driver and motor vehicle information and driver license transactions and records, and it is also the reporting mechanism for Fatalities and Serious Bodily Injury (FLHSMV, 2021). DAVID provides important personal and confidential information that not only includes driver and vehicle information but also provides current and past photographs, addresses, social security numbers, emergency contact information, government documents, signature facsimiles, and a vast array of other sensitive data. The information contained within the database can be an instrumental tool for criminal investigations and other law enforcement related purposes.

To access the DAVID system, an agency must sign a Memorandum of Understanding (MOU) with FLHSMV that states the purpose for use, defines the meanings and terms contained within the MOU, expresses the legal authority to access the database, reiterates the necessity to safeguard the information in the database, and lists the required compliance and control measures needed to protect the database from misuse (Office of the Inspector General, 2018). However, the MOU only provides for what information is to be protected, not how the information is to be protected nor any

specific method to deter misuse. An individual who is authorized by the agency to access DAVID from a secure terminal is required to enter a username and password and to acknowledge a legal disclaimer and DAVID usage warning. Once inside the database, the user can search using a driver license number, name, vehicle tag, vehicle identification number, vessel hull number, business name, address, etc. The search can also be performed using a 'like' option, where close matches due to unknown, exact information will be returned in the search result. To proceed with the search, the user must select one of 34 purpose codes for the search, which may include criminal investigation, emergency notification, crash, verify identity, traffic-related inquiry, or response to calls for assistance (DAVID, 2021). After the information is entered, the user may then access any of the detailed information in the driver record.

Driver Privacy Protection Act

The Driver Privacy and Protection Act (DPPA) signed into law in 1994 under 18 U.S.C. § 2721 requires all state driver and motor vehicle information to be protected from misuse and limits access to the driver information to purposes such as legitimate government agency functions. Prior to DPPA, state driver records were open to public disclosure in 34 states. Per DPPA, if these states' legislators voted to retain open records, then they must give drivers the option to keep their information personal (Senat, 2001). DPPA, with some exceptions, sought to close this potentially dangerous public disclosure of personal information though open-government advocates feared that the legal reasoning behind DPPA would lead to a blockage of access to other government databases, which provide the cornerstone of investigative reporting (Senat, 2001). DPPA, under 18 U.S. Code § 2721, has five parts related to protecting driver privacy.

Section A of DPPA (1994) states that no employee, officer, or contractor shall knowingly disclose or make available to any person or entity any personal information or highly restricted personal information in connection with any motor vehicle record without the person's expressed consent. Highly restricted personal information is described in detail under 18 U.S. Code § 2725 and refers to any information that identifies an individual, including their photograph or image, social security number, or medical and disability information.

Section B of DPPA (1994) specifies that permissible uses of sensitive information obtained through a driver record shall only be disclosed or used in matters relating to motor vehicle safety, motor vehicle emissions, motor vehicle product recalls, alterations, advisories, performance monitoring, maintenance of motor vehicle records, or for any purpose relating to the Anti Car Theft Act of 1992, Automobile Information Disclosure Act, or the Clean Air Act. Further, Section B limits the permissible use of said information in 14 subsections, but primarily for government agencies carrying out legitimate business: for lawful use in connection with motor vehicle and driver safety, for insurance and investigation purposes, and during the normal course of business by agents and contractors to the extent that they are only verifying the accuracy of the information (DPPA, 1994).

Section C of DPPA (1994) addresses the resale of driver information by an authorized recipient, but such information must be kept and made available to the state motor vehicle department upon request for a period of five years and must detail the purpose and use of the information.

Section D of DPPA (1994) establishes the waiver procedure in which the state or any of its agents may disclose information when it does not fall into any of the exceptions addressed in the statute. This section also relays an individual's privacy rights under the law and defines the procedure for informing an individual when and by whom their information has been requested.

Section E of DPPA (1994) prohibits conditioning or burdening the issuance of a person's motor vehicle record to obtain their expressed consent, and it permits the state to charge an administrative fee for issuing a motor vehicle record.

No language in DPPA permits usage, access, nor dissemination of any part of a driver record for anything other than a lawful purpose. As discussed later in an Associated Press report, seemingly innocuous behavior, such as idle curiosity and casual browsing of DAVID photos and addresses of a driver, is still a crime and violation of federal law. The five DPPA sections make no exceptions and require the information to be kept secure and confidential, even from those entrusted to access a driver database.

DAVID Point of Contact

FLHSMV, according to its policies, requires that each agency have a DAVID Point of Contact (POC) whose administrative function is to ensure DPPA compliance for their respective agency. The authority to audit, monitor, and conduct investigations over FLHSMV and its systems lies with the Inspector General's Office. Under FLHSMV's policy 11.07 dated 07/01/1983 and revised on 08/10/2016, the Inspector General has oversight authority under F.S.S. 11.45 and F.S.S. 20.055, and the limitations and employee relief for sustained adverse actions are all defined under related F.S.S. 112.3187 (FLHSMV, 2020). Under the policy, the Office of the Inspector General (OIG)

was created as part of the Inspector General Act of 1994. In addition, an OIG was established for every state agency "as a central point for coordination of responsibility for activities that promote accountability, integrity, and efficiency in government" (FLHSMV, 2020). Within F.S.S. 20.055, the OIG must provide direction for audits and investigations; keep the head of the agency informed of fraud, abuse, and deficiencies relating to programs; review corrective actions taken to improve program performance; advise in the development of measures, standards, and procedures; and ensure a balance between audits, investigations, and accountability activities.

To ensure these objectives are met, each agency that affords access to DAVID to its employees must have a POC who oversees DAVID activities within the department they serve. The OIG cannot individually audit, inspect, and investigate all 957 agencies. Thus, the POCs act as an extension of the OIG for the individual agencies. The establishment of the POC is codified in a MOU between the agency and FLHSMV. POCs have administrative functions, and they can review activities and status for their agency, ensuring all user information is updated and accurate (FLHSMV, 2020). One of the most important functions of a POC is granting DAVID access to users based on their role within their agency. FLHSMV also recommends having multiple POCs to perform these functions in the event of the primary POC's absence. According to the MOU between FLHSMV and the agencies, the POC must perform a quarterly quality control review, which includes but is not limited to checking for signs of misuse. Signs of misuse can include reason codes used to search for individuals such as running spouses, siblings, or celebrities; the date and time queries were run; repeated runs of the same person; or any unexplained access to the emergency contact information. The POC must also ensure

that any printed information from DAVID is destroyed by cross-cut shredding or incineration (Escambia County Corrections, 2017; FLHSMV, 2020).

However, the OIG's 2018 Audit Report contained documented issues concerning the POC list. According to the report, the external agency and FLHSMV are both required to sign a MOU, but a comparison of MOU information revealed the external POC list to be inaccurate, as it contains as many as 55 tax collector offices whose employees are considered internal, not independent POCs (Office of the Inspector General, 2018). Furthermore, four of the MOUs were terminated or expired, and 13 agencies had never signed a MOU to gain access to DAVID (FLHSMV, 2020). At the time of this research, the 2019 OIG Audit Report was not yet published. Its publication will, however, demonstrate if any of these deficiencies were corrected.

History of Abuse

Several media outlets have reported various violations that have occurred when driver information is accessed or used improperly. In a 2016 report in the Associated Press, a review by journalists showed law enforcement officers frequently misuse law enforcement databases to obtain information about romantic interests, business associates, journalists, and neighbors (Gurman, 2016). These systems can be exploited to give an individual officer critical information about people s/he may encounter on the job for non-law enforcement reasons, such as settling quarrels, resolving personal conflicts, and voyeuristic curiosity (Gurman, 2016). In other cases, the access of the information has resulted in criminal behavior. According to a 2016 CBS News report that mirrored the Associated Press report, these cases have included egregious violations, such as when an Ohio officer used the information he accessed through the system to stalk his

girlfriend; he ultimately pleaded guilty to stalking (Gurman, 2016). In two other cases, a Michigan officer used a database to look up the addresses of women he found to be attractive, and in Miami, Florida, two officers used a driver database to run unauthorized checks on a journalist who authored an unflattering story on them (Gurman, 2016). A similar report in Computerworld found that not only had officers run illegal and improper searches that had nothing to do with the lawful performance of their jobs, but between 2013 and 2015 some 325 employees with access to databases were fired, suspended, or resigned for misuses; more than 250 times, officers were reprimanded for misuse; and though 90 employees nationwide abused various databases, the imposed disciplinary measures in these cases remained unclear (Storm, 2016).

Over the past decade in Florida, several governmental agency employees have violated DPPA by accessing and using data contained within DAVID for purposes outside of a legitimate function. One case of notoriety occurred in 2011 after a Florida State Trooper arrested a Miami-Dade police officer for reckless driving and speeding while on duty. After the arrest, dozens of officers from numerous agencies around the state violated federal policy when they searched the trooper's personal information in DAVID without any lawful or legitimate purpose (Huriash, 2017; Mauney, 2014). These hundreds of searches on the trooper resulted in numerous fines for officers as well as agencies. In that case, DAVID's most accessed features were the trooper's photo array and home address. The trooper shortly afterward suffered harassment when a series of prank calls and suspicious deliveries were sent to her South Florida home, resulting in her subsequent move to the Florida panhandle (Huriash, 2017). In a similar case out of Jacksonville, Florida, in 2017, an activist, whose troubled history with law enforcement

stemmed from his video recording them in public, claimed that his driver information had been illegally searched in DAVID for no legitimate or lawful purpose. More concerningly, when WJXT – Jacksonville submitted a Freedom of Information Act request to investigate the activist's claims, they discovered hundreds of more violations, including some that involved officers snooping on several of WJXT's own news journalists (Gardner, 2017). In those subsequently uncovered violations, the journalists' photo arrays and addresses were the most accessed items.

In 2020, in Tampa, FL, WTSP - Tampa journalists uncovered dozens of DAVID misuses by government employees through a public records request. A Tampa Bay Area sheriff's office detective used DAVID to search an activist who had asked for the detective's internal affairs file; a dispatcher at a local department used DAVID to access addresses of coworkers to send Christmas cards; a municipal police department employee used DAVID to look up the driver information of a teenaged girl he was involved with romantically and her parents' information as well; and a police officer used DAVID to search information about young women he met while working on duty in an official capacity (Bourne & Powell, 2020). One Florida Fish & Wildlife Conservation Commission dispatcher used DAVID to get information to stalk his ex-girlfriend and her friends and then committed arson by setting fires to their properties (Bourne & Powell, 2020). Furthermore, the report revealed that since 2015 there have been over 900 DAVID misuse violations for which, other than a letter of counseling, only two officers were punished criminally.

Statement of the Problem

Over the past decade, dozens of cases have been reported around the country in which government employees have violated DPPA by improperly accessing and using driver information contained within state motor vehicles databases for non-legitimate purposes. In the State of Florida, such driver information is contained within DAVID, which is managed by FLHSMV. Controlled access to the information within DAVID is required by DPPA to which over 900 agencies have access. Each agency must assign a POC whose primary role is to audit and oversee the activities occurring in DAVID for FLHSMV and to ensure DPPA compliance. Despite DPPA's requirements and those set forth by FLHSMV, access violations of DAVID continue to occur each year, putting drivers at risk for illegal, improper, or unethical use of their personal information. Given these conditions, FLHSMV's protections of driver information to deter authorized users from misuse in DAVID are ineffective, and the tools available to the POCs to allow for proper auditing and monitoring of access may be insufficient. Corrective measures to curb illegal behavior by authorized users must be provided to the POCs and their respective agencies to help them deter misuse within DAVID.

Objectives of the Research

This research study is framed by general deterrence theory using a mixed methods approach to measure the strength and direction of a set of existing independent variables already in common use. The independent variables are given to the DAVID POCs via an online survey to predict the impact on their ability to adequately perform their job and to deter future misuse within the database. Thus, this research does not seek to create a new theoretical framework, but expands on the existing general deterrence theory to explain the predicted phenomenon. According to Jabareen (2009), extensively used qualitative

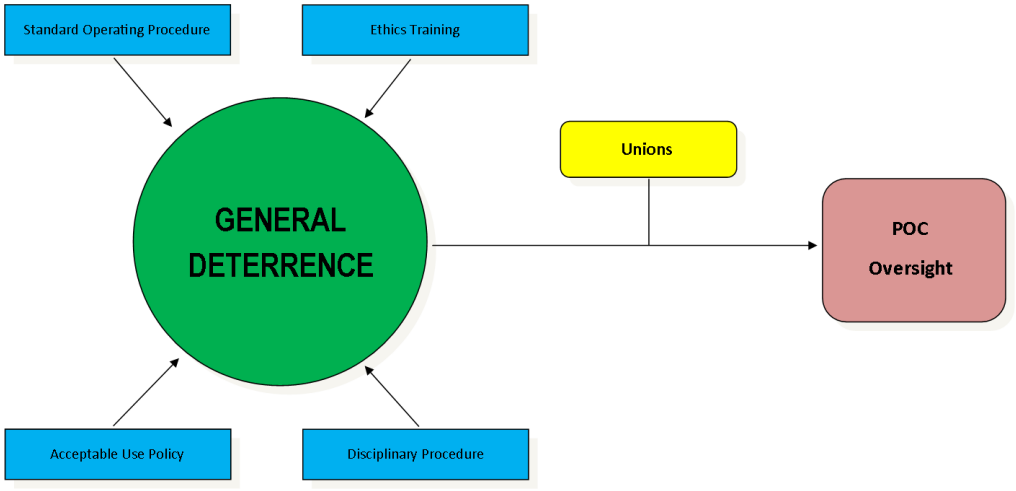
methods, such as the thematic analysis employed in this research, are good for providing a description but not for generating theorization. Similarly, Strauss and Corbin (2009) explained that a theory uses concepts and that these concepts are related by way of statements of relationships. However, in this study, the independent variables of a standard operating procedure (SOP), ethics training, acceptable use policy (AUP), and disciplinary procedures are posited to be unrelated concepts of general deterrence theory, and their impact on the continuous dependent variable of a POC's audit and deterrence are explained through multiple regression analysis.

Research Questions

This quantitative research study proposes an analysis of predictive general deterrence variables at the system administrator level that measures the strength of the variable and the ability of the administrator to manage and deter misuse within a government database. The relationship between the variables and the deterrence is moderated by the presence of police unions, see Figure 1.

Figure 1

Independent Variables with Union Moderator Flowchart



The results of the research can assist practitioners and agency leadership to draft policies that will better equip the DAVID POCs and agencies to prevent authorized users from abusing DAVID. This study addresses four research questions:

- Question 1: How effective is the implementation of a clear and concise DAVID-specific standard operating procedure (SOP) in allowing the POC to effectively manage and deter access violations?
- Question 2: How effective is the requirement of ethics training on database access and usage by the users in allowing the POC to detect and prevent an access violation?
- Question 3: How effective is the implementation of a DAVID-specific acceptable use policy (AUP) enforced by a POC in allowing the POC to effectively manage and prevent access violations?

- Question 4: How effective is a consistent, standardized disciplinary procedure regarding DAVID usage violations in allowing a POC to proactively detect and prevent an access violation?

Summary

Authorized users' violation of DPPA through abuses and misuses of DAVID is a problem that has existed for quite some time. Policies and procedures have been put into place to help manage DAVID and to minimize the number of abuses; however, even with these measures, abuses continue. POCs help to oversee and manage the system, as they are charged with granting and monitoring user access as well as conducting audits. As discussed in this introductory section, there is an apparent failure in policy in terms of the ability to manage DAVID and curb abuse as reported in internal OIG audits and by investigative reports by the media. To address this pervasive issue, the research examines the aforementioned independent variables, and it is organized as follows:

Chapter 2 examines the review of literature that expounds on the foundation of general deterrence theory and the impact of the Fourth Amendment of the United States Constitution regarding searches and seizures. The review of literature extends to the independent variables of standard operating procedures, ethics training, acceptable use policies, and disciplinary procedures and enforcement and examines how each of these variables directly relates to general deterrence theory.

Chapter 3 will discuss the methodology used in this research. The methodology is based on a DAVID Point of Contact Survey administered online through Qualtrics™ which was used to collect the data for this study. Only municipal police agencies in Florida were able to participate in this study. All 254 municipal agencies were contacted

by phone to obtain the names and email addresses of the POCs, who were then asked to participate in the study. Chapter 3 will also discuss the metrics used to create the survey questions, what they intend to measure, and how the survey was distributed among the sample of participants.

Chapter 4 examines the results of the DAVID Point of Contact Survey using both descriptive and predictive statistics, multiple regression analysis, binary logistic regression, Pearson's *R*, Durbin–Watson statistic, and variance inflation factors. It is hypothesized that each of the independent variables will show a strong correlation between the ability of the POCs to manage and deter abuse within DAVID.

Chapter 5 interprets and discusses the results of the DAVID Point of Contact Survey and how the results can shape future FLHSMV and DAVID POCs policy recommendations and practices. The recommendations proposed in this study are not new general deterrence policy concepts but instead shown to be underutilized or ignored in the MOUs, which have allowed the abuses within DAVID to occur.

Chapter II

REVIEW OF LITERATURE

General Deterrence Theory

In the 1764 essay *On Crimes and Punishment*, Cesare Beccaria introduced the concept of general deterrence theory, which posited that, absent deterrence, individuals will make decisions based on what provides pleasure and avoids pain, even if those desires lead to criminal behavior (Tomlinson, 2016). As Beccaria was not in favor of harsh punishments, he believed that punishment should prevent individuals from committing harm to fellow citizens and to deter others from doing the same (Pizzi, 2012). Three key concepts of general deterrence theory are that any punishment undertaken must be swift such that it is carried out soon after the crime is committed; that it is proportionate, meaning crimes mild in nature garner punishments mild in nature; and that it deters, meaning the point of the punishment is not to further hurt the offender but to prevent future offenses (Vick, 2016). More commonly, general deterrence theory's three concepts are based on severity, certainty, and celerity of the sanctions (Connolly et al., 2017). The U.S. Department of Justice (2016) indicates that the certainty of being caught is the most powerful deterrent of crime. These broad overviews of general deterrence theory align well within the corrections system of the United States in terms of incarceration and sentencing of offenders who commit violent crimes, but they become more nuanced in the public and private sectors, where offenses are often civil or administrative in nature, as is the case with DAVID access violations.

In law enforcement, behavior by officers is influenced by policies, and those policies are contained within a paramilitary construct (Bishopp et al., 2016). The paramilitary nature of police agencies requires these agencies to oversee the officer's daily activity, investigate and sanction any misconduct, and create new policies for rules of conduct as needed (Bishopp et al., 2016). However, in an article examining police misconduct from a legal perspective, Sekhon (2019) makes the argument that municipal policing is misperceived by the courts and law scholars because not only are officers "street sovereigns," whose power derives from the law, but they are not contained by it either. Sekhon (2019) goes on to suggest that the police can derogate from the law as necessity dictates, and it is they who dictate that necessity. Recall the DPPA discussed earlier, which allows for access to the data by law enforcement for a lawful purpose. Applying Sekhon's argument, the information contained within DAVID can be accessed by an officer as lawfully needed if the officer states that the reason for the access is lawful since that determination rests with him/her. However, general deterrence theory counters this assertion because, with proper training and the threat of sanctions, illicit behavior can be controlled as well as provide for a disincentive for others to engage in such illicit behavior (Connolly et al., 2017).

General deterrence theory has been used to address police misconduct as well as to provide a blueprint for the development of administrative policy addressing employee behavior. In a study by Pogarsky and Piquero (2004), for example, several hundred police officers from a mid-sized southwestern United States department were studied to determine how much formal and informal threat of sanctions influenced an officer's decision to commit misconduct and what role impulsivity and experience of prior

punishments played in their decision making. The Pogarsky and Piquero (2004) study examined four factors of general deterrence theory on police misconduct: extant theory provided further understanding of whether a single theory might be able to explain an array of socially sanctioned and criminal behaviors; general deterrence theory filled a gap in the literature concerning the deterrence process for police versus that for other individuals; perceptual deterrence research to explain individual processes underlying crime; and an exploration of the causes of police misconduct. Klockars et al. (2005), conducting survey research on police misconduct for the U.S. Department of Justice, found that clearly understood policies and rules have a greater impact on deterrence than simply hiring the "'right'" people (p. ii). In addition, Klockars et al. (2005) made an important observation that an officer learns to evaluate the seriousness of various types of misconduct by observing how their department detects and disciplines behavior. Klockars et al.'s research showed, as would be the case for DAVID, that the role of the POC in detecting a violation is equally as important as the sanction that stems from the report of the violation by the POC and is given by the agency itself. Similarly, early warning systems (EWS) and early intervention (EI) techniques used by agencies have had a significant impact on general deterrence and police misconduct. Worden et al. (2014) describe EI systems as a key tool for managing the risk of misconduct, and these systems have become an accreditation requirement, often used in consent decrees, and are treated as a best practice in police administration. EI systems involve the collection of computerized data based on employee performance, where analysis by management allows the agency to identify officers who have recurring performance problems, such as high numbers of uses of force, citizen complaints, etc. (Walker, 2006). The Commission

on the Accreditation of Law Enforcement Agencies (CALEA) (2021), for example, requires the implementation of early intervention systems for agencies to retain accreditation delineated in chapter 35 which covers performance evaluation. Moreover, EI systems help deter and prevent police misconduct and abuse by monitoring indicators of police action that may signify police misconduct, and, in so doing, they allow administrators to intervene quickly with counseling and retraining (Worden et al., 2014). In additional research regarding general deterrence and policing, Hughes (2001) examined both the general methods of controlling police behavior and the impact of civil liability as a regulation mechanism. Hughes suggested that there are two methods of controlling police behavior that are administrative and/or legal. Administrative methods of control occur through officer selection, training, departmental policies, rules, and procedures (Hughes, 2001). Legal methods of control, Hughes argued, include criminal sanctions in which the officer can be prosecuted or subject to liability based upon tort law. While the arguments presented here suggest a consensus among contemporary scholars as to the legal and overarching purpose of general deterrence theory, their concurrence countered Andenaes' (1970) prevailing stance that referenced earlier works by Kant (1795) and Bittner and Platt (1965) to argue that punishment should be applied to only the person who commits an offense and not to hold that person to account for what others may do in the future. Andenaes' (1970) position referred to the Kantian Principle first proposed by German philosopher Immanuel Kant, which states that an individual's goodwill is based on their adherence and duty to moral law. Andenaes went on to argue that the application of Kant's Categorical Imperative should mean that an individual who commits an offense should be punished according to their crimes only

and not upheld as an example to others. However, it should be noted that even Andenaes did not take an absolute, affirmative position for or against the Kantian Principle as it applies to law but raised the question as to the ethical application of general deterrence when applied to the individual and such deterrence is reasonable.

Fourth Amendment and Government Databases

Government and law enforcement agencies use numerous systems and databases to conduct official business and to provide for the safety and security. These databases allow the government to operate efficiently in carrying out its various functions, and these systems provide government actors with a great deal of access to personal and confidential information about citizens, especially those in the criminal justice system. These systems include but are not limited to the National Crime Information Center (NCIC), the National Data Exchange (N-DEx), the Law Enforcement Enterprise Portal (LEEP), Uniform Crime Reporting (UCR), Next Generation Identification (NGI), the Florida Crime Information Center (FCIC), Electronic License and Vehicle Information System (ELVIS), as well as a host of other systems at the federal and state level that store information relating to DNA, fingerprints, employment, banking, etc. According to the Federal Bureau of Investigation (n.d.), its NCIC is described as a "lifeline" of law enforcement that allows criminal justice professionals to apprehend fugitives, locate missing people, recover stolen property, identify terrorists, and perform their duties more safely.

Each of these databases is governed in some way by the Fourth Amendment of the United States Constitution, which places limits on unreasonable searches and seizures, and each database has limitations on access due to the purpose for which it is

used. As further explained by Sekhon (2017) regarding how the Supreme Court views the Fourth Amendment and law enforcement, each case the court examine refers to purpose and is weighed against the motivation of individual officers. Sekhon suggested that, in looking at police practices, the Supreme Court analyzes purpose through purpose-objective, subjective, and programmatic frameworks, and in so doing, it fails to ensure law enforcement behaves transparently and honestly (Sekhon, 2017). Fan (2012) offered a solution, perhaps where the high court fails, by developing a more sophisticated system of data-driven surveillance to help discern and red-flag patterns of problematic behavior. Creating data-driven surveillance systems to look for patterns of problematic police behavior would incentivize proper behavior by making any deviation more easily detected and quicker to address (Fan, 2012). The issues that both Fan (2012) and Sekhon (2017) identify are concerned with purpose, for example, how to detect when the alleged purpose of a police action is one of abuse.

Access to the information contained within a government database comes under great scrutiny because of the sensitivity of the information contained within it. While much of the access is assumed to be within the scope of lawful duties, databases can be used for controversial access, such as "fishing activities" where officers search for warrants, often for minor offenses, to create evidence to conduct searches or make arrests (Logan, 2019). This knowledge would allow the officer to justify a stop of a person based solely upon information contained within the database and not individually, an officer-created probable cause. Also, another problem, Logan (2019) argues, is not only the ease of access and interoperability of the databases and potential for biased policing, but the databases contain sensitive information that may not be criminal yet can be

embarrassing to the individual. Combined with items, such as arrest warrants, prior criminal interaction, fingerprints, DNA, biometric information, and information of a highly sensitive nature, the databases do not always provide an investigative benefit but act as a law enforcement panopticon. This panopticon becomes further intrusive by the data contained within a driver license database like DAVID, where personal identifiers, such as photographs, social security numbers, addresses, signature facsimiles, etc. are made readily available and easily searchable. To address this concern, four types of database access should be subjected to regulation. Suspect-driven access should rely upon proportionate justification of the Fourth Amendment intrusion; profile-driven access should rely upon transparency, vetting, and universality restrictions; event-driven access should be limited to the time and place of an event; and program-driven access should be limited by legislation that is evenly applied (Slobogin, 2017). Much of the literature shows that while the information contained within police databases is confidential and can aid in criminal investigations, there appears to be a lack of a consistent and cohesive policy that carefully monitors, protects, and limits how the information is accessed and used, or, as Fan (2012) propounds, there is not an independent third party to act as a fiduciary over the database to ensure compliance.

Standard Operating Procedures

Police agencies often develop written procedures to guide police officers' actions and behaviors (Fan, 2012; Logan, 2019; Sekhon, 2019; Slobogin, 2017). The implementation of clearly worded standard operating procedures (SOPs) that directly address the use and access of databases such as DAVID by the agency in which a POC oversees may help in that regard and provide for general deterrence against violations.

Much of the literature in the development and issuance of SOPs is dated or prevalent in other fields, such as pharmacy, but still very applicable to the problem being addressed in this research. For example, Schniepp (2015) provides the elements of how SOPs are to be constructed and applied, noting that they should be clear and concise, while simultaneously explaining that SOPs should be easily deciphered by employees: employees should be able to identify what task they should perform and when they should perform it, and how to document incidents so that the same results can be achieved each time. Gough and Hamrell (2010) surmised in their research on developing SOPs that procedures must not only be clear and understandable to those carrying them out but also those written procedures must have the same result every time. Ashworth (2007) asserted that SOPs have three essential elements, assurance, quality, and consistency. Worker adherence to SOPs requires management intervention, and the SOPs must be of high quality, standardized, and accurate because, without these features, workers are less likely to follow them, and their required use will be negative (de Treville et al., 2005).

SOPs are also used as a form of general deterrence against behaviors such as misconduct and employee fraud. Written in a manual, SOPs serve as a guideline for employees to not only carry out their routine jobs in the workplace, but to facilitate conduct and assist in dealing with issues such as bribery, conflicts of interest, and data security (Nawawi & Ahmad Saiful Azlin, 2018). For this reason, Nawawi and Ahmad Saiful Azlin (2018), in their research on employee fraud and misconduct, go on to suggest that SOPs are an integral tool in preventing or mitigating losses, and they help to minimize mistakes and deter poor judgment. Similarly, Weeden (2013), whose work

focused on creating a strong framework for SOPs, indicated that they reduce costs, and within the context of liability risks and directives, they are an excellent source for achieving compliance. Kallaman's (2006) research on risk management added that SOPs allow organizations to reduce risk by focusing on operational activities, administrative duties, and technical processes. Kallaman (2006) showed that SOPs abate risk by ensuring compliance, reducing work, improving quality, fostering understanding, increasing credibility, and providing legal defense. These factors are key in this research because they contextualize the necessity and importance of SOPs. Furthermore, the points raised by Nawawi and Ahmad Saiful Azlin (2018), Weeden (2013), and Kallaman (2006) were supported by two sample DAVID audits conducted by the Martin County (FL) Clerk of the Circuit Court (Timmann, 2019) and the Agency for Health Care Administration (2013). Both audits identified the need for policies and procedures to address the use of the DAVID to ensure compliance and both properly defined the responsibilities of users of the database. However, the age of the literature suggests a significant gap in articles on the development and implementation of SOPs and policies, which may contribute to the problem being addressed in this research.

Ethics Training

Ethics is a branch of philosophy that governs a person's choice between right and wrong and may provide an avenue for resolving the issues of database access, use, and abuse described by Sekhon (2019), Logan (2019), Slobogin (2017), and Fan (2012). Ethics training also provides for a moral compass and general deterrence against DAVID access violations. The Office of the Inspector General's 2018 audit revealed misuses in DAVID despite the existence of the DPPA, Florida state law, and the rules and

regulations put in place by the FLHSMV. However, not all misuse occurring in DAVID stemmed from criminal intent. Many of the violations came from curiosity or benign browsing of the data and photographs contained within DAVID. Ethics training, which all law enforcement officers receive in some form, should impress upon them the need to refrain from accessing DAVID for anything not specifically related to their job function. One pitfall to ethics training in law enforcement as discussed by Bayley (2012), is that it has become reactive pedagogy that has not advanced beyond simple scenario-based ideology. Etter and Griffin's (2011) research on ethics training in police departments discovered that officers see ethics training as "fluff" and would rather do training that directly applies to their job. Etter and Griffin's (2011) study revealed a possible disconnect. Even though training in both ethics and firearms relate to an officer's job, some officers may not see training in the ethical use of DAVID as necessary because it is an abstract concept, whereas the use of firearms and defensive tactics are more tangible. Indeed, two studies, one by de Schrijver and Maesschalck (2015) and the other by Marion (1998), mirrored this issue and revealed that police recruits often view ethics training as an unnecessary course that could be better spent on more interesting coursework, such as firearms and self-defense. Morgan et al. (2000) also found ethics training to be sorely lacking and argued that it should be placed at a higher level in the police training curriculum.

In each of the aforementioned studies, ethics training was rarely sought by officers and rarely offered by agencies; thus, most officers do not receive ethics training beyond the minimal training offered in the academy. To further complicate this point, most officers, prior to entering the field, believe they are already ethical (de Schrijver &

Maesschalck, 2015). Furthermore, many studies on police integrity and ethics revealed perceived seriousness of behavior to be a strong predictor of a fellow officer's likelihood of reporting another officer's violation; consequently, officers are more likely to report serious crimes but less likely to report what they feel are less serious crimes (Hickman et al., 2016). The Hickman et al. (2016) study, using a sample of (n = 499) officers from Philadelphia, revealed that serious violations committed by fellow officers are strong indicators of reporting. However, in the case of DAVID abuse, as shown by the literature, officers viewed ethics training as overall unnecessary and thus might see many of the violations as minor indiscretions, not serious enough to warrant reporting fellow officers. Despite the personal views of officers, ethical use violations of DAVID, as shown in this research, continue to be a persistent problem and rely on POC administrators to audit and report violations.

Ethics training is a key factor in the general deterrence of misconduct. For example, Kaptein (2015) posited the role of ethics training to influence the behavior of employees by promoting ethical behavior and impeding unethical behavior. Moreover, Kaptein (2015) proposed seven functions of ethics training: to offer clarity to employees regarding ethical and unethical behavior, to demonstrate role model behavior, to provide resources to employees that promote ethical behavior, to foster a commitment to ethical behavior among employees, to enhance transparency surrounding ethical behavior, to create an openness in the discussion of ethical issues, and to reinforce ethical behavior. Ethics training also hinges upon rewards for ethical behavior and punishments for unethical behavior (Kaptein, 2015). Stucke (2014) appeared to support Kaptein's position on ethics and deterrence by identifying six similar functions of ethics training.

Stucke (2014) also found, through analysis of empirical studies on ethics and deterrence, that organizations promoting an ethical organizational culture were far more successful. In an earlier work by Harrington (1996) explored the impact of the codes of ethics on corporate computer abuse and explained codes of ethics as the basis for formal sanctions that can create fear of punishment for breaking the code of ethics. Furthermore, if the employee signed an acknowledgment of the codes of ethics, then they become acutely aware of the potential unpleasant actions that can be taken against them (Harrington, 1996). The correlation between deterrence and breaking the law enforcement code of ethics is detailed by Flink (1995), who looked to the Utah Supreme Court's decision in the 1986 case of Wayne L. Jones v. Toole County. The paramount nature of integrity allows for a peace officer's certification to be revoked or suspended for conduct that would diminish, erode, or jeopardize public trust regarding law enforcement; such behavior will not be tolerated by the judiciary and must be rooted out by law enforcement before it subjects them to liability (Flink, 1995) The direct relation between ethics training and general deterrence is consistent among different disciplines, from private business (Kaptein, 2015), corporate law (Stucke, 2014), information technology (Harrington, 1996), and judicial review (Flink, 1995). Thus, it is the position of this research that the same principles on ethics and deterrence hold true for law enforcement.

Acceptable Use Policy

The implementation of an acceptable use policy (AUP), sometimes referred to as a Fair Use Policy or Computer Use Policy, harkens back to a distinctive point raised by Slobogin (2017), who suggested the four types of database access that should be governed by regulation. An AUP is a type of policy that establishes an agreement and

understanding between the employee and employer and defines the expectation by a network/service owner, creator, or administrator, which in this case is the FLHSMV who manages DAVID, that restricts the way the network or service can be used by the end-users (Thomas, et al., 2015). AUPs play an increased role in information security by curtailing employees' access to material deemed inappropriate for work, and employees' violations of these agreements have been the basis for termination (Foltz et al., 2008). Foltz et al. (2008) explained that usage policies were developed to address both legal and security issues and employee rights. Holmes (2003) argued that an effective AUP should monitor the use of assets, establish no expectation of privacy, prohibit improper employee use, establish proper employee use, protect sensitive information, define methods for disciplinary action, and require employees' acknowledgment of the AUP. An organization must do more than merely generate an AUP; they must ensure that employees read and understand the AUP. AUPs are commonly seen in educational settings, where students are granted internet access and the granting institution has the students agree that they will only use the internet as consistent with learning objectives. Oftentimes, these agreements exclude the use of social media, access to adult content, etc. In the case of DAVID, an AUP can set the boundaries for what the FLHSMV expects of users and restrict the way confidential and personal data can be used.

AUPs stem from the concept of general deterrence theory, which presumes that employees make risk and reward decisions based on expected gratification by taking advantage of opportunities and avoiding the severity of potential punishment for malfeasance (Ugrin & Pearson, 2008). In the private sector, research conducted as early as 2002 revealed that an AUP without the impact of enforcement was ineffective because,

even if the punishment were spelled out in the AUP, once employees believed that they would not be enforced, some would violate the rules (Ugrin & Pearson, 2008). This finding is important because, in the case of DAVID, the POCs' ability and consistency to apply the rules stipulated in the DPPA and by the FLHSMV may have a tremendous impact on the likelihood of a DAVID use violation. Holmes (2003) showed another direct connection between AUPs and general deterrence by arguing that both are specifically designed to deter misuse by giving proper legal notice on expected usage, explaining potential disciplinary actions, and requiring acknowledgment. However, Holmes (2003) made it abundantly clear that AUPs lose their impact and effectiveness of deterrence if the users do not read them. Along the same line, Doherty et al. (2011) generally agree with the sentiments of Ugrin and Pearson (2008) and Holmes (2003), but they also raise an important factor in that AUPs focus too much on defining unacceptable behaviors and not enough on promoting desirable ones. Therefore, it is equally important to use AUPs as a method of general deterrence through negative reinforcement and punishment as it is to use positive reinforcement and reward.

Flowers and Rakes (2000) conducted general deterrence and AUP research in the public sector by evaluating the effectiveness of K–12 schools' AUPs in deterring misuse of internet access by students. The result of the research showed a mixed response of improperly structured AUPs, many of which were outdated, and several schools indicated that their legal department had constructed their AUP, while other schools' information technology directors had created theirs (Flowers & Rakes, 2000). The schools also offered varying responses for who was responsible for monitoring students' internet use (Flowers & Rakes, 2000). Still, the greatest concern uncovered by Flowers and Rakes'

(2000) work was that only 10% of schools at the time had an active AUP. More recently, Ruhnka and Loopesko (2013) researched how employees' violation of AUPs creates legal and civil liability risk exposure for their organization and how employees are legally protected against punishment if the AUP is inadequate or nonexistent, especially when the employee is operating within the scope of their employment. Ruhnka and Loopesko's (2013) research strikes at the very heart of the problem being addressed in this research regarding DAVID misuse which creates legal and civil liability risk exposure if an employee violates a DAVID AUP.

Disciplinary Procedures and Enforcement

In various fields, abundant literature shows the correlation and effectiveness between disciplinary procedures and general deterrence. Deterrence is the best behavioral response to the threat of discipline and sanctions; however, it assumes that the threat of discipline and punishment is objective (Nixon & Barnes, 2019). Helfers et al. (2020), following the public outcry due to law enforcement misconduct, echoed the need for an objective and fair disciplinary procedure, stating that many departments have experienced public scrutiny over their disciplinary procedures, which must be implemented fairly and objectively, otherwise increased punishments might produce adverse reactions. This concept of discipline to promote deterrence is not a new idea; in fact, it has been written about for centuries. However, references to general and specific deterrence have changed over time. As Chalfin and McCrary (2017) explain, general deterrence refers to the threat of discipline and punishment, whereas specific deterrence refers to the experience of discipline and punishment. The position of this research

focuses on general deterrence due to the threat of sanctions stated in the memorandums of understanding that agencies must agree to and sign to access DAVID.

In a comprehensive study on risk perception and general deterrence, Apel (2013) explored the threat of sanctions' impact on criminal behavior. Apel's (2013) research revealed that the average citizen has a good working knowledge of criminal statutes but does a relatively poor job of estimating the impact of the possible sanctions. However, and more importantly, direct, and vicarious experiences with punishment are significant deterrents to future risks (Apel, 2013). Apel (2013) measured situational risks in which peripheral factors, such as substance abuse, peer presence, and arousal, significantly impact the choices people make in choosing to commit violations. This research study's Introduction chapter discussed a type of situational risk that occurred when DAVID users violated access by using the database to stalk individuals or to browse photos of people the officer found attractive. In that case, officers made a calculated risk to abuse DAVID access to satisfy their arousal while weighing their perception of what could happen to them if they were caught. Peripheral factors discussed by Apel along with the DAVID abuse examples provided earlier in the Introduction chapter indicate that, absent a consistent disciplinary procedure, general deterrence is reduced, and poor decision making is more likely to occur.

For law enforcement, discipline and general deterrence are keys in building and keeping public trust, as misconduct erodes perceptions of police legitimacy. Police misconduct is quite complex and broadly defined, ranging from criminal behaviors that violate the law, departmental policy, and ethical codes of conduct (Donner et al., 2016). Criminological theories such as Pogarsky and Piquero's (2004) deterrence may help

explain why people commit crimes and why police misbehave (Donner et al., 2016). For example, in a comprehensive study on the fairness of disciplinary procedures and deterring misconduct, Ivkovic et al. (2016) put forward the notion that in the concept of simple deterrence, the harsher the penalty, the less likely officers are to become involved in the code of silence and misconduct. In the same study, Ivkovic et al. (2016), presented the concept of disciplinary indifference, which says that if agencies rarely discipline for misconduct, officers should be less deterred by the threat of sanctions because discipline would be seen as the exception and not the rule. Likewise, in the simple justice model, officers reporting violations and misconduct was linked to their perceptions of disciplinary fairness, in which they possessed the desired discipline to be carried out appropriately and justly (Ivkovic et al., 2016). The relationship between disciplinary fairness and deterrence relates to Helfers et al.'s (2020) and Nixon and Barnes' (2019) studies on objective and fair discipline.

Fan's (2012) argument, discussed above, that a third party should use data-driven surveillance to uncover police misconduct, raised questions for this research. Even if abuse or improper access is found, how can it be addressed? Government agencies may codify the use of disciplinary procedures and enforcement, both of which serve as general deterrence against violations of policy. As indicated in an AUP, enforcement is a crucial part of ensuring compliance. DAVID POCs are charged with using the DPPA to ensure compliance in DAVID by anyone who was granted access. However, it is crucial to note that not all government employees who have access to DAVID have the same rights and dismissal procedures. Some employees work at-will, meaning their employer can terminate their employment for any legal reason at any time without incurring civil

liability (Gely et al., 2016; Tomlinson & Bockanic, 2009). Likewise, these employees can leave their jobs at any time for any or no reason at all. Conversely, many law enforcement officers are employed under a collective bargaining agreement, which indicates that, for employees to be punished or terminated, they must have violated a specific policy, committed gross misconduct, performed below acceptable standards, or committed a violation of law, and even then, the disciplinary process must occur in a specific manner. The presence of unions, arbitration, and collective bargaining all play significant roles in the severity and frequency of discipline. In a 2021 study involving 624 police arbitration cases from 2006 to 2020, due to union negotiations, 52% of the cases saw reduced discipline, while in 46% of the cases where the officer was terminated, the agency was required to rehire them (Rushin, 2021). In the same research study, officers' suspension time was reduced by 49% when their punishment was more severe (Rushin, 2021). Therefore, research into the impact of disciplinary procedures and deterrence must consider the mediating role of unions in any statistical equation.

In a report by Thomas et al. (2015), they described the proper procedures for administering discipline to employees who violate social networking and indicated that discipline must lay out the exact procedure for violating policy as well as the appeals process afforded to the employee. A supporting example of a consistent disciplinary procedure appeared in a study by Harris et al. (2015), where they examined the use of police matrices and their effectiveness in curbing misconduct. Absent aggravating or mitigating circumstances, categorizing offenses into tiers with a proportional range of sanctions is one way to achieve consistency. However, Harris et al. (2015) uncovered the point that many police agencies nationwide have or are planning to implement some type

of formal disciplinary matrix, but the use of matrices is more common when a collective bargaining contract is in place. Where collective bargaining is not present, an issue arises in the administering of discipline using progressive measures inconsistently, a lack of or too much consideration of the weight of prior offenses, and the discordant application of cardinal and ordinal proportionality (Harris et al., 2015). Tomlinson and Bockanic (2009) supported Harris et al.'s (2015) position when they stated that if an employee receives an adverse punishment, such as termination, employers must ensure they have uniform written policies that are consistently applied and well-publicized to all of their employees. Tomlinson and Bockanic (2009) went on to claim that disciplinary procedure and policies must state when an automatic termination can occur as a result of an offense; if an offense is subject to progressive discipline, the employer should indicate that any list of offenses and punishments are not all-inclusive, and that the employer has the right to administer discipline where appropriate. The common theme among these articles was that the employer must be clear, consistent, and treat all employees fairly and equally regarding disciplinary procedures and policy. For the POCs, a consistent and well-publicized disciplinary process for violations in DAVID by their respective agency should deter misuse before it is discovered in an audit, and it should protect the integrity of the database from future abuse.

Presently, there is not substantial scholarly literature on abuses that occur specifically within the DAVID system nor any other driver and motor vehicle database nationwide. Notably, as shown in this literature review, there are general processes and systems in place within law enforcement to help curb improper and illegal behavior, but none that address the handling of data. This research seeks to bridge the gap in scholarly

information by expanding on the extant literature on general deterrence and correlating it to DAVID. Upon successful completion of the research, the newly learned information can be applied to DAVID, but also universally applied to any number of law enforcement databases in which the careful handling and management of sensitive information are paramount. Ultimately, the research can be used as a basis to create policies where none exist, or to show the necessity of training and educating law enforcement on best practices in protecting sensitive information from abuse.

Chapter III

METHODOLOGY

Introduction

This chapter of the research focused on the methods used to gather the data to test the stated hypotheses. The format for this chapter detailed the hypotheses, provided a thorough description of the survey instrument, provided a description of the survey participants and study measures, and then laid out the procedure used in administering the survey. The researcher also provided an overview of the statistical analyses to be used.

Hypotheses

The hypotheses of this study are as follows:

Hypothesis 1

The implementation of a clear and concise DAVID-specific SOP provides the POC proper oversight of DAVID.

- H_1: When the implementation of a DAVID-specific SOP is applied, there will be an increased ability by the POC to effectively oversee and deter potential access violations.
- H_0: The implementation of a DAVID-specific SOP has no statistical impact on the ability of the POC to effectively oversee and deter potential access violations.

Hypothesis 2

The requirement of ethics training on database access and usage by DAVID users provides the POC proper oversight of DAVID.

- H_2: The requirement of ethics training on database access and usage will show an increased ability by the POC to effectively oversee and prevent access violations.
- H_0: The requirement of ethics training on database access and usage has no statistical impact on the ability of the POC to effectively oversee and deter access violations.

Hypothesis 3

The implementation of a DAVID-specific acceptable use policy provides the POC proper oversight of DAVID.

- H_3: When the implementation of an acceptable use policy specific to DAVID is applied, there will be an increase in the ability of a POC to effectively oversee and deter access violations.
- H_0: The implementation of an acceptable use policy has no statistical impact on the ability of the POC to effectively oversee and deter access violations.

Hypothesis 4

The application of a consistent, standardized disciplinary system with regard to DAVID usage violations provides the POC proper oversight of DAVID.

- H_4: The application of a consistent, standardized disciplinary procedure regarding DAVID will show an increase in the ability of the POC to effectively oversee and deter access violations.

- H_0: The application of a consistent, standardized disciplinary procedure has no statistical impact on the ability of the POC to effectively oversee and deter access violations.

Survey Instrument

To answer the research questions, address the hypotheses, and conduct a valid and reliable collection of data, the principal method of data collection was done through the use of a cross-sectional survey. The survey used in this research was entitled *Point of Contact DAVID Oversight Survey*, and it was administered online through Qualtrics™ and accessed through Valdosta State University (see Appendix A). The researcher chose an online method of survey, sometimes referred to as a web survey, because it is the most effective method in distributing a survey where there is an established e-mail list of the target population (Remler & Ryzin, 2015). This cross-sectional survey collected data from a population of interest at one point in time (Chambliss & Schutt, 2013), and the population of interest were DAVID POCs operating in a Florida municipal police agency. The POC participants answered survey questions anonymously online, and the identity of the participants could not be readily ascertained directly or through any identifiers linked to the participants. Therefore, the Valdosta State University Institutional Review Board determined this study was exempted from oversight under Exemption Category 2 (see Appendix B).

The survey consisted of up to 27 questions; however, this survey was not designed to require any POC to answer all 27 questions, as some questions would not apply to every agency's situation. When that occurred, a binary answer selection of "no" auto-skipped the respondent to the next logical question in the survey. Questions D1, D2,

D3, D4, U1a, and U1b were demographic questions. Questions Q1a through Q4d addressed the research questions and hypotheses. Specifically, questions Q1a, Q2a, Q3a, and Q4a were binary and if answered "no," auto-skipped passed the "b" and "c" questions and took the respondent to the "d" question in the block. For example, answering "no" to question Q1a, which inquired whether the agency had an SOP regarding DAVID, skipped the respondent to Q1d, which asked a logical follow-up question to Q1a. Likewise, a "no" answer to Q2a, which inquired whether the agency required ethics training, skipped the respondent to question Q2d, which asked a logical follow-up question to Q2a. If the respondent answered in the affirmative on the "a" question, they were taken through "b" and "c" and never shown the "d" question. Questions Q1a through Q4d presented those questions to be answered on a 5-point Likert Scale of one (1) to five (5) so that each answer could be weighted. The respondents were presented the choices of "strongly agree," "agree," "neither agree nor disagree," "disagree," and "strongly disagree," all of which were weighted on a scale from one (1) to five (5) as shown in Table 1.

Table 1

Likert Scale Values and Description

Likert Value	Description
5	Strongly agree – the statement is very consistent with respondent's opinion
4	Agree – the statement is mostly consistent with the respondent's opinion
3	Neither agree nor disagree – the respondent does not possess a negative or positive opinion
2	Disagree – the statement is mostly inconsistent with the respondent's opinion
1	Strongly disagree – the statement is very inconsistent with the respondent's opinion

Questions Q5a and Q5b asked the respondent to identify the greatest effective and least effective variable that assists them in their oversight duties when comparing all four variables simultaneously. The answers to these two questions helped the researcher to quickly identify personal favorability and least favorability of the variables among the POCs. Questions Q6a and Q6b collected data on known and suspected numbers of DAVID access violations in the POC's own agency. These two questions were designed to provide a historic picture of the number of violations that occurred over the past five years and to provide context for the issue raised in the research questions. Question Q7 was experimental and created to help POCs quickly audit DAVID activity. The result of Q7 appeared as part of the recommendation summary after the research was completed. Question Q8 identified the POC's overall view of their ability to properly provide DAVID oversight, which directly addressed the purpose of the research.

Per the IRB Research Statement, which appears as the first page of the survey in Appendix A, participants voluntarily took the survey and were allowed to stop responding or skip any questions they chose not to answer. Thus, not every question would equate to the total number of participants. In cases where the participants' choice to not answer a question in the survey resulted in missing values, those answers were excluded in the final tabulation of the variable. The projected time to complete the survey for each participating POC was approximately 10–12 minutes; however, Qualtrics™ reported that the actual average time of completion was 8.2 minutes.

Study Participants and Data Collection

There are presently (n = 957) agencies and organizations nationwide that have lawful access to DAVID (Office of the Inspector General, 2018). However, this research

had two parameters and was narrowly tailored in determining how it was to be distributed. First, it was targeted specifically to municipal law enforcement agencies, and second, it was intended only for the POCs within those municipal law enforcement agencies who have DAVID oversight within the State of Florida. The agencies and organizations that did not meet those parameters or whose jurisdiction fell outside the authority of a municipal law enforcement agency in the State of Florida were excluded. In addition, agencies such as airport police, school district police, or any police agency that did not have municipal law enforcement powers granted to it were also excluded for three reasons. First, the focus of this research centered only on the POC oversight of municipal law enforcement agencies, and of the 957 agencies that presently have DAVID access, most are not law enforcement, or they are agencies whose jurisdiction falls outside the scope of this research, such as the Federal Bureau of Investigation, the court system, and offices such as tax collectors. Second, Florida county sheriff's offices (n = 66), though having law enforcement powers, were excluded due to the potential collinearity of data. Some small agencies, for instance, rely upon the county sheriff's office to run checks in DAVID and the sheriff has controlling jurisdiction over the municipal agencies. In that case, certain questions in the survey could have caused confusion or led to ambiguous answers by the POC, as it may have been difficult to separate whether their answers described the municipal police department or the sheriff's office. Third, the unit of analysis remained consistent among the POCs' answers, ensuring they each described the same type of agency, oversight responsibility, and personnel over whom they audit.

To obtain the contact information of survey participants, the researcher used the Florida Department of Law Enforcement Criminal Justice Agency Links webpage, which provided the alphabetical list of all Florida local law enforcement agencies (n = 275) (FDLE, n.d.). There were 36 agencies on the list that were pre-excluded, as they did not meet the criteria for this study, which only examined municipal police agencies. From the list, 13 agencies were identified as school board police departments, seven agencies were identified as airport police, three agencies were identified as port authority/county police, and two agencies were identified as tribal police, which have federal authority. An additional 10 agencies were discovered to be disbanded, and one agency had merged with the county sheriff's office.

For the remaining (n = 239) municipal law enforcement agencies, the researcher attempted to conduct a census survey in which each agency was contacted by telephone between June 4, 2021, and July 23, 2021, to request the name and email address of the DAVID POC. If the POC or authorized representative of the agency provided the email address, a formal request to participate in the survey was sent via email, which contained an anonymous access hyperlink to the Qualtrics™ database (see Appendix C). The anonymous link did not allow the survey to capture, store, or in any other way allow the researcher to readily identify the participant. Of the 239 agencies that were contacted, 143 agency POCs either agreed to participate in the survey, or the name and email address of the POC was provided by the agency administration to the researcher to forward the anonymous link. The survey link remained active through Qualtrics™ from June 4, 2021, to August 31, 2021, and the total number of actual survey participants was (n = 86) for a survey response rate of 60.1%. A web survey is an efficient method of

distribution to a population that is accustomed to receiving and responding to email communication; however, unsolicited emails can result in a low response rate in addition to weariness associated with bulk emails containing embedded links (Remler & Ryzin, 2015). For this reason, though the researcher had access to the POC emails to send a mass distribution to them, an introductory phone call was first made to the agency requesting participation and likely resulted in the higher response rate. Nonetheless, because the result of the actual participation was less than a full set from the target population, the survey description was modified from a census survey to a purposive, stratified sample survey of POCs. A purposive, stratified sample is defined as a method of sampling where the sampled participants are selected separately from the population strata and identified in advance, and whose participants are particularly knowledgeable about the item under investigation (Chambliss & Schutt, 2013).

Study Measures

Agency Demographics

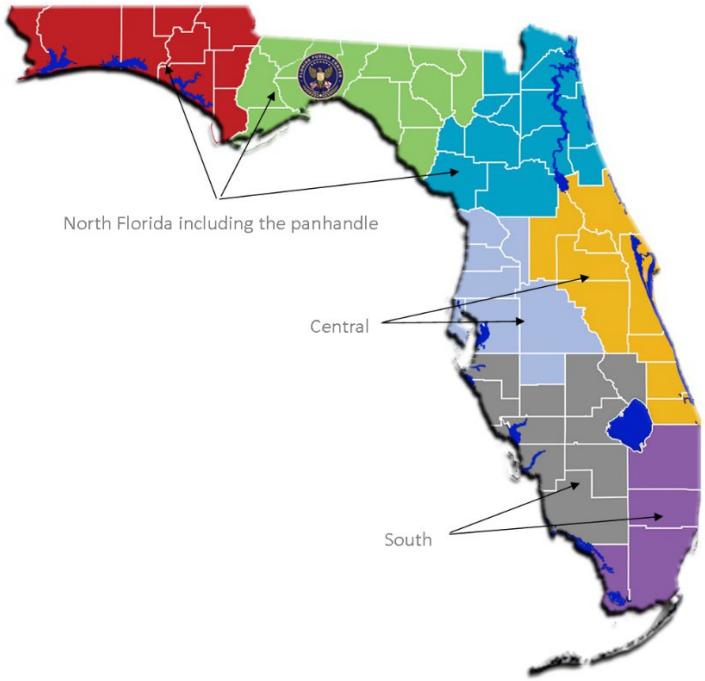
The survey instrument established demographic criteria of both the agencies and the POCs, ensuring a representative sample. Two agency demographics were measured utilizing categorical data of size and location. Agency size was measured using the parameters of 20 or fewer officers, 21-50 officers, 51-100 officers, 101-200 officers, and 201 or more officers. These size categories were created using data provided by *Police1* (Lexipol, 2021). Notably, agencies in north Florida more often serviced rural areas, and their number of officers tended to be smaller, while agencies in south Florida serviced urban areas and tended to have larger numbers of officers. The five size categories

assisted the researcher in distributing the survey to a representative sample of agencies of varying sizes.

The agency location was categorized using the parameters of North Florida including the panhandle, Central Florida, and South Florida. The determination of the geographic locations was created using the Florida Department of Law Enforcement Network of Fusion Centers map as shown in Figure 2 (FDLE, 2021). Note, the Fusion Centers Map served only as a guide to assign agencies geographically for the survey and not by any legal connection to a fusion center. Municipal agencies that are located in the jurisdictions of Northwest Florida Fusion Center (NWFFC), including the panhandle, North Florida Fusion eXchange (NFFX), and the Northeast Florida Fusion Center (NEFFC) were assigned to North Florida. Agencies located in the jurisdictions of the Tampa Bay Regional Intelligence Center (TBRIC) and the Central Florida Intelligence eXchange (CFIX) were assigned to Central Florida. Agencies located in the jurisdictions of Southwest Florida Fusion Center (RSIX) and Southeast Florida Fusion Center (SEFFC) were assigned to South Florida. The three location categories assisted the researcher in distributing the survey to a representative sample of agencies throughout the state.

Figure 2

FDLE Network of Fusion Center Map



Note: From the Florida Department of Law Enforcement, (FDLE, 2021).

POC Demographics

Two POC demographic categories and two subcategories were measured. The POC was measured utilizing the categorical data of years of experience and method of granting access to DAVID. POC years of experience were measured using the parameter of less than 1 year, 1–2 years, 3–4 years, and 5 or more years. POC granting access was measured using the parameters of any sworn officer, only sworn officers demonstrating a specific need, only supervisors or higher, or only select personnel. The subcategories of the presence of collective bargaining and POC oversight limitation by collective bargaining were presented as yes or no binary choices. As indicated in the literature

review, collective bargaining and unions play a role in police administration. This research sought to reveal whether collective bargaining plays a moderating role in the oversight of DAVID.

Study Procedure

To date, there are no known published, comprehensive studies specific to DAVID or its oversight. Thus, this case study was developed to predict the impact on POC oversight in DAVID from the general deterrence variables of SOPs, ethics training, acceptable use policies, and disciplinary procedures. The survey instrument was established by requesting POCs from various Florida municipal law enforcement agencies to complete an online survey giving their opinions on how much of an impact the four hypothetical variables have on their oversight ability. The procedure used a cross-sectional design model, multiple regression analysis, and descriptive statistics in IBM's SPSS software program version 26. Because the sample size of the participants who completed the survey was smaller than anticipated, additional tests of normality were performed, as was testing for multicollinearity to ensure that the independent variables were in fact independent and predictive. The additional statistical tests and results are explained in further detail in Chapter 4, *Data Analysis*.

Summary

The results of this quantitative study tested the four research hypotheses, that SOPs, ethics training, acceptable use policies, and disciplinary procedures impact the ability of the POCs to oversee DAVID and are a predictive measure to deter future misuse within the database. Proper oversight of access to the sensitive data contained within DAVID is critical to agencies that utilize the system due to the potential for civil

and criminal penalties as well as the loss of trust by the community. With more agencies accessing DAVID, including the development of the more robust driver database, ELVIS, discussed further in Chapter 5, it is important for law enforcement administrators to create and implement effective policies proactively and to understand how these policies and procedures prevent misuse and reduce their liability.

Chapter IV

RESULTS

Introduction

This chapter of the research focused on the presentation of data and the results of the study and was guided by the research hypotheses to address the research questions. Descriptive statistics of demographic characteristics of participants as well as study data were initially presented, after which assumptions of a multiple linear regression analysis were tested. After ensuring that all assumptions were met, the results of the regression analyses were presented, and conclusions were drawn. This chapter ends with a summary of the key findings of the analysis conducted for this study.

Descriptive Statistics

A total of 86 participants responded to the survey questionnaire. However, the data were cleaned for missing values. After cleaning for missing values, only 78 participants were included in the analyses. Table 2 presents the frequencies and percentages of demographic characteristics of participants and agencies. About 30.8% of participants have 20 or fewer sworn officers (n = 24), while 25.6% of participants have 21 to 50 sworn officers (n = 20). For the approximate geographic location, 38 participants were located in Central Florida (48.7%), 24 participants were located in South Florida (30.8%), and 15 participants were located in North Florida (19.2%). For their length of time as a DAVID point of contact in the agency, 49 participants responded with 5 or more years (62.8%), while 16 participants responded with 3 to 4 years (20.5%). Participants were also asked for the level of sworn officers granted. The majority of the

participants responded that only sworn officers demonstrating a specific need for DAVID were granted access (n = 61, 78.2%).

Table 2

Frequencies and Percentages of Demographic Characteristics of Participants and Agencies

		Frequency	Percent
Approximate number of sworn officers in agency	20 or fewer sworn officers	24	30.8
	21-50 sworn officers	20	25.6
	51-100 sworn officers	13	16.7
	101-200 sworn officers	8	10.3
	201 or more	13	16.7
	Total	78	100.0
Approximate geographic location of agency	North Florida including the panhandle	15	19.2
	Central Florida	38	48.7
	South Florida	24	30.8
	Total	77	98.7
Missing	System	1	1.3
Total		78	100.0
Length of time as the DAVID point of contact of agency	Less than 1 year	5	6.4
	1–2 years	8	10.3
	3–4 years	16	20.5
	5 or more years	49	62.8
	Total	78	100.0
Level of sworn officers granted access to DAVID	Only sworn officers demonstrating a specific need for DAVID	61	78.2
	Only supervisors and higher	6	7.7
	Only select personnel based on assignment (i.e., detectives, dispatchers)	2	2.6
	N/A	9	11.5
	Total	78	100.0

Participants were also asked to respond to two items on collective bargaining agreement or union. The majority of participants responded that there were officers in their agency under a collective bargaining agreement or union (n = 53, 67.9%). However, all of the participants under the collective bargaining agreement also determined that the collective bargaining agreement or union did not, in any way, limit their DAVID oversight responsibilities (n = 53, 67.9%).

Table 3

Frequencies and Percentages of Variables on Collective Bargaining Agreement or Union

		Frequency	Percent
Are the officers in your agency under a collective bargaining agreement or union?	No	24	30.8
	Yes	53	67.9
	Total	77	98.7
Missing	System	1	1.3
Total		78	100.0
Does the collective bargaining agreement or union in any way limit your DAVID oversight responsibilities?	No	53	67.9
	Yes	1	1.3
	Total	54	69.2
Missing	System	24	30.8
Total		78	100.0

The study variables included the responses of participants on items regarding quality and ability to effectively manage DAVID access based on SOP, ethics training, AUP, and disciplinary procedure, all of which are considered as predictor variables in the regression analyses as well as held the effectiveness to perform oversight duties as the dependent variable. The descriptive statistics of the study variables are presented in Table 4. Based on the descriptive statistics, the highest mean score was observed for

AUP quality (*M* = 1.66, *SD* = .85), while the lowest mean score was observed for SOP ability (*M* = 1.47, *SD* = .72) and ethics training ability (*M* = 1.47, *SD* = .65). The effectiveness to perform oversight duties had a mean of 1.85 (*SD* = .76) with a range of scores from 1 to 3.

Table 4

Descriptive Statistics of Study Variables

	N	Minimum	Maximum	Mean	SD
SOP Quality	76	1.00	4.00	1.64	0.80
SOP Ability	76	1.00	4.00	1.47	0.72
Ethics Training Quality	47	1.00	3.00	1.49	0.62
Ethics Training Ability	47	1.00	3.00	1.47	0.65
AUP Quality	65	1.00	4.00	1.66	0.85
AUP Ability	65	1.00	4.00	1.63	0.76
Disciplinary Procedure Quality	75	1.00	4.00	1.63	0.88
Disciplinary Procedure Ability	75	1.00	3.00	1.52	0.70
Effectiveness of Oversight	78	1.00	3.00	1.85	0.76

To properly analyze data in linear regression, the data was checked to verify that it could be analyzed in this manner in IBM's SPSS. Six assumptions determined appropriateness: 1) the variables are to be measured at a continuous level, 2) there is a linear relationship, 3) there are no significant outliers, 4) there is an independence of observations, 5) the data shows homoscedasticity, and 6) residual errors have been checked (Laerd Statistics, 2018). Specifically, in each hypothesis, the Durbin–Watson statistic ensured that the independence of observations was not violated. Moreover, Durbin–Watson checks for autocorrelation and has a statistical range of 0 to 4, with 2

being no autocorrelation. In Durbin–Watson, 0 to < 2 is positive serial autocorrelation, and > 2 to 4 is negative serial autocorrelation, with 1.5 to 2.5 being considered the optimal range (Statistics How To, 2022). For each hypothesis section, the Durbin–Watson result will be identified.

Prior to conducting the regression analyses, assumptions of regression analysis were tested. The first assumption is the normality of residuals. The Q–Q plot, or quantile–quantile plot, was used to determine whether there was normality of residuals for the variable effectiveness of oversight. Q–Q plots are a type of scatterplot that plot two sets of quantiles against one another, and if they come from the same distribution, a straight line should be formed from the points (Ford, 2015). A Q–Q plot, in other words, is a visual check of normal distribution. The result, presented in Figure 3, showed that the data points are within the normality line, thus indicating that the assumption for normality of residuals was not violated.

To check for outliers for the variable being plotted, a boxplot was also used, as shown in Figure 4. A boxplot is another way of displaying the data distribution based on a five-number summary: the minimum, first quartile, median, third quartile, and maximum (Galarnyk, 2018). The boxplot operationalizes an outlier as any value above or below three standard deviations from the mean. If such a condition exists, in SPSS, the outlier would appear as a dot at the top or the bottom of the boxplot. Figure 4 shows the results of the boxplot of the dependent variable effectiveness of oversight. The plot showed that there were no outliers in the dependent variable. Thus, the assumption of outliers was also met. Other assumptions were tested as the regression analysis results discuss.

Figure 3

Normal Q–Q Plot of Effectiveness of Oversight

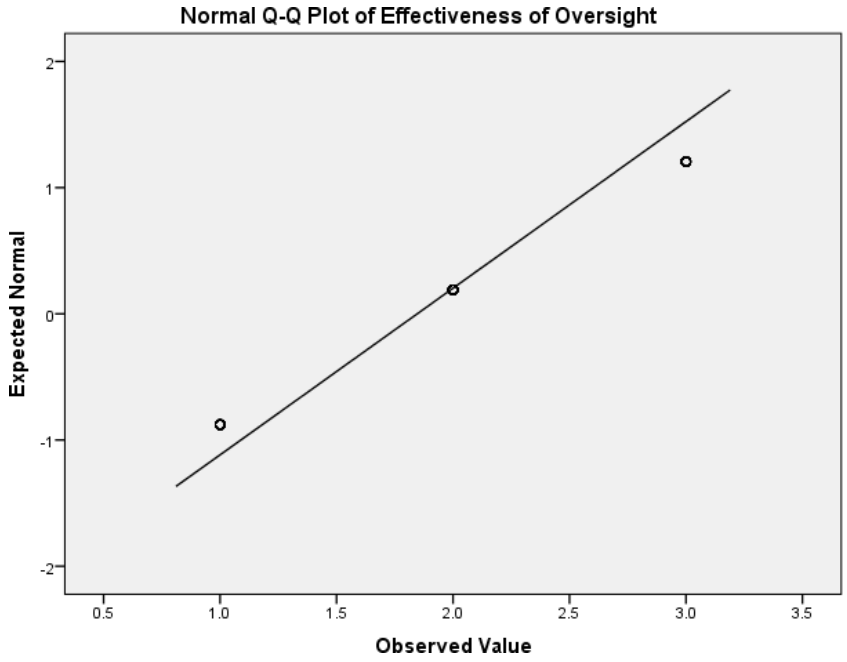
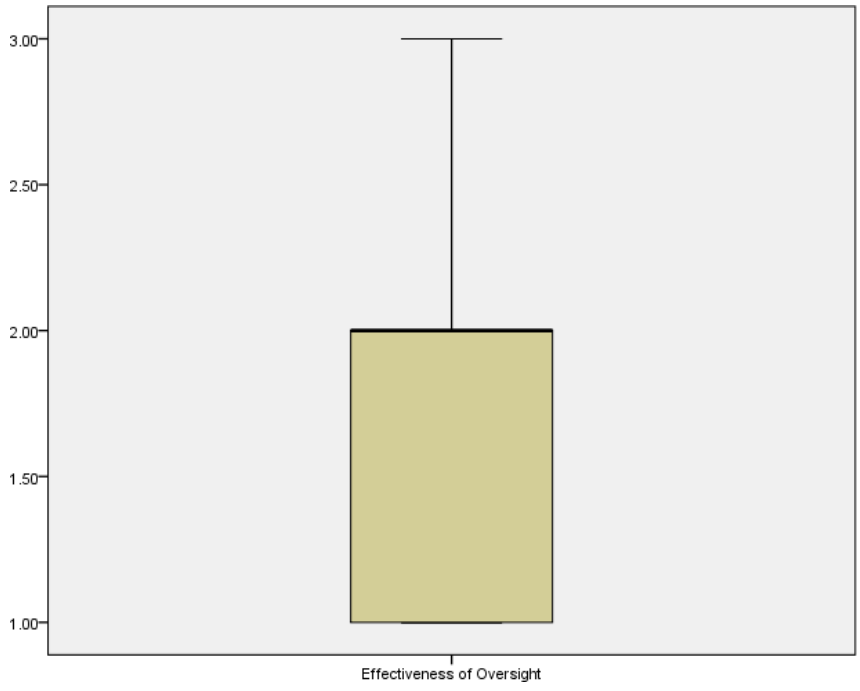


Figure 4

Box Plot of Effectiveness of Oversight



Hypothesis 1

Hypothesis 1 stated that the implementation of a clear and concise DAVID-specific SOP provides the POC proper oversight of DAVID. A regression analysis was conducted to determine whether variables of SOP ability and SOP quality significantly predicted the effectiveness of oversight of DAVID. The Durbin–Watson statistic was determined as 1.835, which was near the value of 2, indicating that the assumption of independence was not violated. Moreover, the VIF score of 1.499, which was below the value of 10, indicated that the assumption of multicollinearity was not violated. The result of the regression analysis determined that SOP ability is a significant predictor of the effectiveness of oversight of DAVID ($\beta = .497$, $p < .01$). The result showed that an increase in SOP ability score resulted to an increase of .497 in the effectiveness of oversight of DAVID. The model was also determined to be significant ($F(2, 75) = 18.116$, $p < .01$, $n = 76$). The predictor variables also explain 31.3% in the variance of the effectiveness of oversight of DAVID variable. Therefore, there was sufficient evidence to conclude that the implementation of a clear and concise DAVID-specific SOP provides the POC proper oversight of DAVID.

Table 5

Regression Analysis Result for Effectiveness of Oversight with SOP Variables as Predictors

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.	Collinearity Statistics Tolerance	Collinearity Statistics VIF
1	(Constant)	0.871	0.182		4.784	0.000		
	SOP Quality	0.115	0.111	0.121	1.035	0.304	0.667	1.499
	SOP Ability	0.521	0.123	0.497	4.246	0.000	0.667	1.499

a. Dependent Variable: Effectiveness of Oversight; $F(2,75) = 18.116$, $p < .01$, Adjusted $r^2 = .313$, n = 76

Hypothesis 2

Hypothesis 2 stated that the requirement of ethics training on database access and usage by DAVID users provides the POC proper oversight of DAVID. A regression analysis was conducted to determine whether variables of ethics training ability and ethics training quality significantly predicted the effectiveness of oversight of DAVID. The Durbin–Watson statistic was determined as 2.182, which was near the value of 2, indicating that the assumption of independence was not violated. Moreover, the VIF score of 4.062, which was below the value of 10, indicated that the assumption of multicollinearity was not violated. The result of the regression analysis determined that neither ethics training quality ($\beta = .168$, $p = .548$) nor ethics training ability ($\beta = .261$, $p = .351$) was a significant predictor of the effectiveness of oversight of DAVID. The model was determined to be significant ($F(2, 46) = 4.564$, $p = .016$, n = 47). The predictor variables also explained 13.4% in the variance of the effectiveness of oversight of the DAVID variable. Therefore, there was insufficient evidence to conclude that the

requirement of ethics training on database access and usage by DAVID users provides the POC proper oversight of DAVID.

Table 6

Regression Analysis Result for Effectiveness of Oversight with Ethics Training Variables as Predictors

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	0.990	0.267		3.716	0.001		
	Ethics Training Quality	0.200	0.331	0.168	0.606	0.548	0.246	4.062
	Ethics Training Ability	0.296	0.314	0.261	0.942	0.351	0.246	4.062

a. Dependent Variable: Effectiveness of Oversight; $F(2,46) = 4.564$, $p = .016$, Adjusted $r^2 = .134$, n = 47

Hypothesis 3

Hypothesis 3 stated that the implementation of a DAVID-specific acceptable use policy provides the POC proper oversight of DAVID. A regression analysis was conducted to determine whether variables of AUP ability and AUP quality significantly predicted the effectiveness of oversight of DAVID. The Durbin–Watson statistic was determined as 2.113, which was near the value of 2, indicating that the assumption of independence was not violated. Moreover, the VIF score of 1.816, which was below the value of 10, indicated that the assumption of multicollinearity was not violated. The result of the regression analysis determined that AUP ability was a significant predictor of the effectiveness of oversight of DAVID ($\beta = .437$, $p = .003$) . The result showed that

an increase in AUP ability score resulted in an increase of .437 in the effectiveness of oversight of DAVID. The model was also determined to be significant ($F(2, 64) = 13.304$, $p < .01$, n = 65). The predictor variables explained 27.8% in the variance of the effectiveness of oversight of DAVID variable. Therefore, there was sufficient evidence to conclude that the implementation of a DAVID-specific acceptable use policy provides the POC proper oversight of DAVID.

Table 7

Regression Analysis Result for Effectiveness of Oversight with AUP Variables as Predictors

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.	Collinearity Statistics Tolerance	Collinearity Statistics VIF
1	(Constant)	0.860	0.191		4.513	0.000		
	AUP Quality	0.127	0.122	0.148	1.037	0.304	0.551	1.816
	AUP Ability	0.419	0.137	0.437	3.054	0.003	0.551	1.816

a. Dependent Variable: Effectiveness of Oversight; $F(2,64) = 13.304$, $p < .01$, Adjusted $r^2 = .278$, n = 65

Hypothesis 4

Hypothesis 4 stated that the application of a consistent, standardized disciplinary system with regard to DAVID usage violations provides the POC proper oversight of DAVID. A regression analysis was conducted to determine whether variables of disciplinary procedure ability and disciplinary procedure quality significantly predicted the effectiveness of oversight of DAVID. The Durbin–Watson statistic was determined as 1.890, which was near the value of 2, indicating that the assumption of independence was

not violated. Moreover, the VIF score of 3.374, which was below the value of 10, indicated that the assumption of multicollinearity was not violated. The result of the regression analysis determined that disciplinary procedure quality (β = .163, p = .385) and disciplinary procedure ability (β = .362, p = .056) were not significant predictors of the effectiveness of oversight of DAVID variable. The model was determined to be significant (F(2, 74) = 12.428, p < .01, n = 65). The predictor variables also explain 23.6% in the variance of the effectiveness of oversight of DAVID variable. Therefore, there was insufficient evidence to conclude that the application of a consistent, standardized disciplinary system with regard to DAVID usage violations provides the POC proper oversight of DAVID.

Table 8

Regression Analysis Result for Effectiveness of Oversight with Disciplinary Procedure Variables as Predictors

		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	1.004	0.184		5.473	0.000		
	DP Quality	0.141	0.161	0.163	0.874	0.385	0.296	3.374
	DP Ability	0.391	0.201	0.362	1.939	0.056	0.296	3.374

a. Dependent Variable: Effectiveness of Oversight; F(2,74) = 12.428, p < .01, Adjusted r^2 = .236, n = 75

Participants were asked to identify the most effective strategy in managing DAVID. A total of 37 participants responded that having a clear concise SOP was most effective. A total of 21 participants responded that enforcing a consistent and

standardized disciplinary procedure was most effective. On the other hand, participants were also asked to identify the least effective strategy in managing DAVID. The result of the analysis determined that 43% of participants (n = 37) responded that a requirement of ethics training on handling sensitive data was least effective, followed by a required acknowledgement of an AUP (n = 21, 24.4%).

Table 9

Frequencies and Percentages of the Most Effective (Q5a) and Least Effective (Q5b) Strategy in Managing DAVID

		Frequency	Percent
Q5a	Having a clear concise Standard Operating Procedures	37	43.0
	Requiring Ethics Training on handling sensitive data	6	7.0
	Requiring acknowledgement of an Acceptance Use Policy	12	14.0
	Enforcing a consistent and standardized Disciplinary Procedure	21	24.4
	Total	76	88.4
Missing	System	10	11.6
Total		86	100.0
Q5b	Having a clear concise Standard Operating Procedure	5	5.8
	Requiring Ethics Training on handling sensitive data	37	43.0
	Requiring acknowledgement of an Acceptance Use Policy	21	24.4
	Enforcing a consistent and standardized Disciplinary Procedure	8	9.3
	Total	71	82.6
Missing	System	15	17.4
Total		86	100.0

Summary

A total of 86 participants responded to the survey questionnaire, but eight responses were deleted because of missing values. The data analyses included responses from 78 participants. Data gathered in the study were analyzed using regression analyses

to test the hypotheses posed in the study. The results of the regression analysis determined that there was sufficient evidence to conclude that the implementation of a clear and concise DAVID-specific SOP provides the POC proper oversight of DAVID. This result supported the hypothesis (H_1), which posited that once applied, SOPs allow for an increased ability of the POC to effectively oversee and deter potential access violation in DAVID and that the null hypothesis can be rejected. There was also sufficient evidence to conclude that the implementation of a DAVID-specific AUP provided the POC proper oversight of DAVID. This result supported the hypothesis (H_3), which posited that the implementation of an AUP allows for an increased ability of the POC to effectively oversee and deter potential access violation in DAVID and that the null hypothesis can be rejected. However, the results of the regression analyses did not determine ethics training quality and ability nor disciplinary procedure quality and ability as significant predictors of the effectiveness of oversight of DAVID. The data revealed for the ethics training hypothesis (H_2) could not reject the null hypothesis, and therefore the requirement of ethics training on database access has no statistical impact on the ability of the POC to effectively oversee and deter access violations (H_0). Likewise, the data revealed for the disciplinary procedure hypothesis (H_4) could not reject the null hypothesis, and therefore the application of a consistent, standardized disciplinary procedure has no statistical impact on the ability of the POC to effectively oversee and deter access violations (H_0). A significance level of .05 was used for all analyses. Chapter 5 will discuss in greater detail the importance and relevance of these results, as they can greatly impact the creation of effective policy and strategies to manage DAVID and deter access violations.

Chapter V

DISCUSSION

This study examined the correlation between four specific types of general deterrence and their impact on oversight within Florida's Driver and Motor Vehicle Information Database (DAVID). The higher the importance the POC places on a general deterrence strategy provided by their agency, the more effective they will be at performing their oversight duties in DAVID. SOPs, ethics training, AUPs, and disciplinary procedures, as an independent variable of general deterrence, were hypothesized to be the most effective tools to enhance the dependent variable of oversight by the POCs who manage the database. The independent variables consisted of two subsections: quality and ability. Quality referred to the exact wording, process, or policy of the independent variable by the POC's agency. Ability referred only to the existence of the independent variable within the POC's agency. As will be shown in more detail, POCs, in every case, viewed the independent variable's ability to be higher than the quality regardless of the overall correlative strength. The results of the data supported the hypotheses and indicated a strong correlative effect between SOPs and AUPs on oversight. However, the data did not support the hypotheses of ethics training and disciplinary procedures as having strong correlative effects on oversight, though disciplinary procedures approached strong correlation. As there are no known published research materials on DAVID oversight at the time of this study, the following discussion provided by the researcher, expands on the existing general deterrence literature. This chapter also examines the demographics of the POCs and the agencies they represent, as

well as the relevance, application, and potential impact of SOPs, ethics training, AUPs, and disciplinary procedures on POC oversight and future policy development and changes within DAVID.

POC and Agency Demographics

Demographically, the research survey was distributed to a diverse representation of POCs from various police agencies throughout the State of Florida. The research intended to conduct a full census survey of POCs from all municipal police agencies in Florida, but this goal was hindered by the normal phenomenon of survey nonresponse. A total of (n = 239) agencies were contacted by phone by the researcher in effort to minimize survey nonresponse. Though a full census was unsuccessful, this effort to first make contact by phone proved highly effective as 143 agencies expressed interest in taking the survey. Of the 143 agencies that expressed interest and received an email containing the anonymous link to the survey instrument, (n = 86) POCs logged into the survey and took some action in answering questions to generate data. However, another limitation was encountered in the data collection in that only (n = 78) POCs completed enough questions to generate measurable data. This meant the survey produced a true response rate of 54.5%, which was still remarkably high, as the typical response rate for an online survey is about 20-30% (Qualtrics XM, 2022). Consequently, while type II errors were avoided in the overall results, the statistical power of the survey was reduced and thus resulted in the inability to reject the null hypotheses in two of the four research hypotheses to be discussed later in more detail.

Two notable discoveries were made in the chosen survey distribution method concerning the demographics of participants. The first discovery was that the

aforementioned decision to make personal contact with each agency's POC to request participation as opposed to sending an unsolicited email may have been a key factor in the higher number of responses. However, the second discovery was that when survey respondents were given the option to skip questions, gaps in the data collection emerged. The participants' ability to skip questions was a requirement by the IRB as noted in the IRB Research Statement, which appeared in the survey introduction (refer to Appendix A). Nonetheless, missing data values from skipped survey questions were cleansed, and the results were extrapolated using the data provided by the POCs.

The demographics of the POCs indicated a fairly even representation of agencies from North Florida, including the panhandle, Central Florida, and South Florida. Central Florida had a slightly higher representation at nearly 49% but still within a normal distribution range compared to the other two geographic areas. Agency size, on the other hand, skewed much higher in favor of representation of smaller agencies that contained 50 or less officers. The survey results showed that agencies with 50 or fewer officers accounted for approximately 56% of the respondents, which was notably higher than the 44% participation rate of larger agencies consisting of more than 50 officers. Nevertheless, this difference was to be expected, as the majority of municipal police agencies in Florida are smaller in size, as indicated by online resources such as the Florida Department of Law Enforcement and Police1.com (FDLE, 2021; Lexipol, 2021).

The skill level of the participating POCs in the survey skewed significantly higher to the those with 5 years or more of experience, as they represented nearly 63% of all respondents. This difference may be attributed to POCs being tenured personnel within an agency where their position does not customarily experience attrition. Another

notable demographic area shown by the research revealed that agencies overwhelmingly permit DAVID access to their personnel who can demonstrate a specific need for it. According to the results of the survey, over 78% of the POCs indicated that this was the standard they used to grant access to DAVID. Here again, this result was to be expected, as DAVID is an important law enforcement tool, and a POC making access too restrictive could hinder the performance of an officer's duty.

Based on the demographic questions, the survey results consisted of municipal police agencies that are representative of agencies throughout the entire state with agency size consistent with the population of agencies as a whole. The survey also revealed that the POCs who participated are highly experienced and grant access to DAVID based on their judgment of personnel demonstrating a need to use it. The results of this research did not test for the size of the agency nor the experience level of the POC as a moderator on the effect of the independent variables.

Historical Context of Descriptive Statistics

The survey given to the POCs asked two questions that were not part of the analysis but created for the sole purpose of providing historical context of the problem for readers. Specifically, questions identified as Q6a and Q6b asked how many known or suspected violations of DAVID had occurred within the POC's agency over the past five years (five years is the limit of DAVID data collection). Because the results of the data analysis are based on the proposition that there is a problem with DAVID access violations, these two questions quantified how much of a problem actually exists. According to the survey responses of all who chose to answer, the mean number of known violations for the past five years was (n = 128), and the mean number of suspected

violations for the past five years was (n = 100). Note, some of these violations may have been committed by the same user, but DAVID does not calculate the number of violations based on the number of people who violate, only the number of actions that violate the DPPA (i.e., looking up photographs, looking up addresses, improperly using the emergency contact information, etc.). Also, when a respondent provided the answer of 10 or greater, for the purposes of the calculation, 10 was chosen as the number, even though there might have been significantly more violations. For this reason, these known and suspected violation counts should be viewed as a minimum. The problem of DAVID access violations has been thus shown and will be addressed in the following discussions of the research questions.

Research Question 1

Research Question 1 asked, "How effective is the implementation of a clear and concise DAVID-specific standard operating procedure in allowing the POC to effectively manage and deter access violations?" Hypothesis 1, in relation to Research Question 1, posited that when the implementation of a DAVID-specific SOP is applied, there will be an increased ability by the POC to effectively oversee and deter potential access violations. The issuance of an SOP is a form of general deterrence and is hypothesized to be a predictive factor on oversight and deterrence of access violations. The hypothesis was tested, and the data revealed the existence of an agency's SOP, indicated as the ability, was a statistically significant predictor on the effectiveness of oversight by the POC ($\beta = .497$, $p < .01$) . Conversely, when the POCs were asked to weigh specifically on the wording in which their agency's SOP spelled out their oversight responsibilities, indicated as quality, there was no statistical significance ($\beta = .121$, $p = .304$). The model

showed that once the SOP quality and SOP ability were combined to determine their effect on the dependent variable of the effectiveness of oversight, there was a moderately, strong correlation ($p < .01$, $r^2 = .313$). Though both quality and ability questions were closely related, the POCs interpreted the two questions distinctly different. This difference indicated that as a general rule, POCs believed an SOP to be an effective oversight and deterrence tool; however, they did not believe the exact words currently within the text of their SOP achieved that goal. One potential solution to remedy that discrepancy would be to have the oversight responsibilities of the POC more concisely indicated by the agency within the SOP.

The findings in this research relating to Research Question 1 concerning SOPs are also consistent with literature by Schniepp (2015), who argued that SOPs should be clear, concise, and easily deciphered, as well as that by Gough and Hamrell (2010), who added that SOPs must be understandable to those carrying them out. In particular, the POCs interpretation on the quality of SOPs on their oversight aligns closely with Kallaman (2006), whose research centered on the reduction of liability and the importance of defining administrative duties established by an SOP. Moreover, the POCs' (n = 37, 43%) selection of having a clear and concise SOP as being the most effective tool in helping them manage and deter potential access violations shows a consistent linear relationship as to the overall effectiveness of SOPs on oversight and deterrence. Though a complete census was unable to be completed, the existence of a moderately strong correlation between SOPs and oversight suggests that the FLHSMV, to ensure proper oversight and compliance, should consider requiring a DAVID-specific SOP in the MOU for any agency utilizing the database.

Research Question 2

Research Question 2 asked, "How effective is the requirement of ethics training on database access and usage by users in allowing the POC to detect and prevent an access violation?" Hypothesis 2, in relation to Research Question 2, posited that the requirement of ethics training on database access and usage will show an increased ability by the POC to effectively oversee and prevent access violation. The requirement of ethics training is a form of general deterrence and is hypothesized to be a predictive factor on oversight and deterrence of access violations. The hypothesis was tested, and the data revealed that the quality of present ethics training showed no significance on the effectiveness of oversight by the POC ($\beta = .168$, $p = .548$). When the POCs who represented agencies that provide ethics training on database access were asked if the present ethics training allows for effective management, indicated as ability, the results also showed no statistical significance ($\beta = .261$, $p = .351$). The model showed that once the ethics training quality and ability were combined to determine their effect on the dependent variable of the effectiveness of oversight, only 17.2% of the data fit into the regression model ($p = .016$, $r^2 = .172$). In both cases, the POCs were clear by their responses that they did not believe ethics training would help them in their oversight nor be an effective general deterrence measure to prevent access violations. This response is notably consistent with the majority of the those surveyed (n = 37 or 47%) who also chose ethics training as the least effective tool in helping them manage DAVID and deter potential access violations. The results here indicated no statistical relationship between ethics training and POC oversight, but it should also be taken into consideration that a smaller sub-sample of the overall aggregate of POCs answered this question (n = 47).

Though it is not fully understood why many of the POCs chose to not answer the questions regarding ethics training, one explanation could be that the POCs view ethics training in a similar manner that the officers themselves view it; it is time spent training that could be put be to better use. Additional research on ethics training impact on DAVID oversight will be needed to answer this question more firmly.

While these results run counter to the literature on the necessity of ethics training, they do align with the argument by scholars that personnel oftentimes prefer other coursework they feel directly relates to their job. For example, Etter and Griffin (2011) described officers' views of ethics training as "fluff" that is not directly related to their job. Similarly, de Schrijver and Maesschalck (2015) noted that new recruits described ethics training as unnecessary and felt that their time could be better spent on more interesting coursework, such as firearms and self-defense. These findings are further complicated by the fact that ethics training is rarely offered by agencies and seldom sought by officers (Morgan et. al, 2000), which may explain why this independent variable scored low in the survey. However, ethics training should not be summarily disregarded as a tool in comprehensive DAVID oversight. Ethics are an important part of law enforcement and help instill trust by the community in those sworn to uphold the law. FLHSMV, prior to giving any individual access to DAVID, may consider requiring them to review ethical responsibility in the form of an online video tutorial, reading material, or an instructor led course. Once the DAVID user completes such ethics training, the POC would need to verify the completion of the required training (i.e., certificate, test score, etc.) as a condition of access and then grant it accordingly. This approach may serve as both a deterrent and a reminder to those who may abuse their access to DAVID

as well as to those managing it to take extra precaution in handling confidential and sensitive information.

Research Question 3

Research Question 3 asked, "How effective is the implementation of a DAVID-specific acceptable use policy enforced by a POC in allowing the POC to effectively manage and prevent access violations?" Hypothesis 3, in relation to Research Question 3, posited that when the implementation of an acceptable use policy specific to DAVID is applied, there will be an increase in the ability of the POC to effectively oversee and deter access violations. The implementation of an AUP is a form of general deterrence and is hypothesized to be a predictive factor on oversight and deterrence of access violations. The hypothesis was tested, and the data revealed that agency-issued AUPs, indicated as ability, are a statistically significant predictor on the effectiveness of oversight by the POC ($\beta = 0.437$, $p = .003$). However, when the POCs who represented agencies that currently require an AUP on database access were asked if the specific wording in their AUP allows for effective management, the results showed no correlation ($\beta = 0.127$, $p = .304$). The results here are similar to the results in the SOPs, where only the ability showed a correlation on oversight, but no correlation on quality. However, the model indicated that once the AUP quality and ability were combined to determine their effect on the dependent variable of the effectiveness of oversight, a correlation was shown ($p < .01$, $r^2 = .278$). The POCs appear to indicate on the one hand that the use of an AUP will help them effectively perform their oversight and manage DAVID, but the exact wording in the AUP they currently use may not necessarily achieve that goal. While the results bear a striking resemblance to the SOPs, SOPs differ in that they define

the function, process, and purpose for agency personnel, whereas AUPs define the rights, responsibilities, sanctions, and privileges of using a database. In both cases, defining how DAVID is to be used as well as the expectations of usage are a significant predictor of oversight and deterrence, but how they are presently worded appears to be a weakness that the POCs have identified.

The results of the AUP as a significant predictor on oversight closely aligns with the literature discussed earlier. As Thomas et al. (2015) explained, AUPs define expectations by users and also restrict the way a database can be used. Holmes (2003) similarly explained that an effective AUP not only monitors use of assets and establishes that no expectation of privacy exists, but they prohibit improper employee use and require the protection of sensitive information. In contrast to the survey responses, the POCs appeared to agree with Thomas et al. (2015) and Holmes (2003) in that they believed that, generally, the function of AUPs are effective and help them perform their oversight, but the ones currently in use lack the wording needed for them to carry out the directive. This finding dovetails two important points by Holmes (2003). First, AUPs can only be an effective general deterrent if they give proper legal notice and explain any potential disciplinary action (Holmes, 2003). Secondly, organizations should not merely generate an AUP as a bureaucratic, perfunctory process but also ensure that employees read, understand, and acknowledge them (Holmes, 2003). Lack of clarity and/or the failure of DAVID users to read, understand, and acknowledge the AUP diminishes the AUP's deterrent effectiveness.

Research Question 4

Research Question 4 asked, "How effective is a consistent, standardized disciplinary procedure regarding DAVID usage violations in allowing the POC to proactively detect and prevent an access violation?" Hypothesis 4, in relation to Research Question 4, posited that the application of consistent, standardized disciplinary procedure regarding DAVID will show an increase in the ability of the POC to effectively oversee and deter access violations. The application of disciplinary procedures is a form of general deterrence and is hypothesized to be a predictive factor on oversight and deterrence of access violations. The hypothesis was tested, and the data revealed that disciplinary procedure quality is not a statistically significant predictor on the effectiveness of oversight by the POC ($\beta = .163$, $p = .385$). There is, however, a caveat to disciplinary procedure ability that must be examined and explained. When POCs were asked to weigh the strength of having a disciplinary procedure regarding DAVID as a method of management and deterrence (shown as the ability), the results, while reported as no significance, fell just outside of the 95% confidence level ($\beta = 0.362$, $p = .056$). This specific result suggests with a larger population sample, a $p < .05$ would be achieved. Consequently, the model indicated that once the disciplinary procedure quality and ability were combined to determine their effect on the dependent variable of the effectiveness of oversight, only 25.7% of the data fit into the regression model ($p < .01$, $r^2 = .257$). Therefore, the results here demonstrate a consistent interpretation by the POCs that disciplinary procedures are not an effective tool in DAVID management. This finding was also confirmed by the independent variable comparison question when the POCs failed to identify disciplinary procedures as being the most effective tool on oversight (n = 21 or 24.4%). Likewise, when the POCs were

asked if disciplinary procedures were a least effective tool as compared to the others, only a small number of POCs indicated such (n = 8 or 9.3%) noting all 86 survey takers answered this section.

The results of the effectiveness of disciplinary procedures on oversight were perhaps the most surprising of the study because discipline would seem to be a quintessential example of general deterrence. While the results of disciplinary procedures did not pan out as anticipated, great caution should be taken when interpreting this particular outcome as a negative. Referring back to the literature on the disciplinary procedure independent variable, Vick (2016) and the U.S. Department of Justice (2016) both pointed out that disciplinary procedures must be swift, proportionate, and certain. Recall that each of the independent variable questions had two subsections. The first one identified in the survey as the *quality* question of the variable directly asked the POCs how their own agency currently applies the independent variable. The second one identified as the *ability* question of the variable asked the POCs to weigh how well the variable allows them to personally perform oversight. Reviewing the disciplinary procedure results, the quality question had a beta weight of 0.163 while the ability question had a beta weight of 0.362. While no statistical significance was determined due to high p-values and the inability to reject the null hypothesis, the same pattern in the difference between ability and quality beta weights, as seen in the other independent variables, remained consistent. This difference may be interpreted in a manner congruent with the literature that found that consistent, standardized disciplinary procedures could be better predictors on oversight even though many agencies' current procedures were lacking. If, for example, the Ivkovic et al. (2016) argument that the fairness of discipline

determines the likelihood of misconduct were applied, then the result of the study would suggest that the POCs might not see a fair system of punishment administered by their respective agencies. Likewise, the Klockars et al. (2005) survey on misconduct further supported this point in that officers learned to evaluate the seriousness of their misconduct by observing how their department detected and disciplined their behavior. These examples would help explain the general deterrence issue with the quality and ability of the disciplinary procedure questions, as the POCs interpreted the two questions independently of one another.

Implication of the Findings

In retrospect, it is clear that the survey exposed a consistent theme among all the independent variables. SOPs, ethics training, AUPs, and disciplinary procedures among the agencies appear to be lacking a clear and consistent application. In each of the aforementioned research question discussions, the interpretation of the *quality* of each of the independent variables tended to score lower than the interpretation of the *ability*. Note, the ability results are the crux of this research and the issue being studied, and these results are the ones used to determine predictability. Even so, the researcher expected to obtain a similar result between the quality and ability questions, but this did not occur for a variety of reasons that can be explained from issues identified in the literature review and in the forthcoming limitations of the study section. This research indicates that the *ability* of two of the four independent variables, excluding ethics training and disciplinary procedures, were, at a minimum, significant predictors on DAVID oversight, while simultaneously, showing that what is currently in place for each had no correlation. More specifically, two of the four independent variables, SOPs and AUPs, showed a significant

correlation on POC oversight, while ethics training and disciplinary procedures did not. However, all four independent variables showed no significance when surveying the *quality* on how well they presently impact oversight. This discovery was one of the most important takeaways from the research: the need to reexamine the present policy and practice of DAVID management, from the MOU down to the line officers who use the database in their daily routine. The results also indicate a need for further study on why the POCs interpreted the current policies and practices as being ineffective in helping them with oversight, as well as a comprehensive review to identify the strengths and weaknesses of such practices. From a public administration perspective, the results show a need for administrators to become proactive and to implement policies that promote effective oversight and discourage violations of DAVID access from the onset, rather than waiting to respond to a violation and exposing their agency to civil liability.

Limitations of the Study

This study of DAVID oversight had several limitations that must be readily identified. First, the number of survey participants was lower than anticipated and thus lowered the power of the study. To avoid type I and type II errors with a 95% confidence level, with a population of (n = 239) possible observations, the number of participants required is (n = 148). While the researcher attempted a census of all 239 possible observations, only 143 agreed to participate and of the 143, only 86 actually participated. This low outcome became increasingly problematic when survey respondents chose to not answer some of the questions in the survey, further reducing the observations of each independent variable. This reduction was most notable in the ethics training question when only 47 POCs chose to answer, causing too high of a p-value, $p = .351$ and thus

resulting in statistical insignificance and the inability to reject the null hypothesis. Conversely, 86 POCs chose to answer questions on disciplinary procedures ability, resulting in $p = .056$.

A second limitation is this study is that it only focused on POCs representing municipal police agencies. DAVID is accessed by local, county, state, and federal agencies as well as by the courts, private entities, and other non-law enforcement agencies, totaling (n = 957) at the time of this research. While the selection to use only municipal police agencies was by design and to avoid issues with multicollinearity, there remains the possibility that agencies not identified as municipal police agencies in Florida would yield different results, especially considering the majority of agencies are not municipal. For example, tax collector offices, child protection services, judicial offices, etc. might have viewed the independent variables differently enough to show a more definitive correlation between the independent and dependent variables.

A third limitation of the study is that only one POC from each agency represented took the survey. According to FLHSMV, an agency may appoint as many POCs as needed to fulfill the role of oversight. Larger agencies may have many POCs, whereas smaller ones may have only one. For the purposes of this study, only one POC per agency was invited to take the survey to avoid skewed and duplicated numbers in the demographics, as well as to avoid oversampling in the independent variables. Due to the IRB Category 2 exemption (see Appendix B), the information recorded by the investigator does not allow the identity of the respondents to be readily ascertained. For this reason, multiple POCs from the same agency would skew demographic questions because the investigator would have no way to remove duplications without knowing

who provided the duplicate answers. However, POCs, even within the same agency, may have different views on the effectiveness of the independent variables, which creates a limitation of the study.

Furthermore, this study limited the investigation to only four specific independent variables: SOPs, ethics training, AUPs, and disciplinary procedures. Because many types of general deterrence strategies can be employed, this study can only draw conclusions and make recommendations on the four presented. Any future study based on these four variables will also be limited; however, this does not preclude a future study from examining other general deterrence variables to compare and contrast to this research or expanding on these four variables to address the limitations identified in this study.

Future of DAVID and Other Databases

DAVID, allowing authorized users to search and obtain vital information containing Florida driver records, is one of the most widely used motor vehicle databases. It is a valuable tool, not only for FLHSMV, but for investigations by law enforcement and other government agencies. DAVID, in recent years, has developed new requirements for users to help minimize abuse. Every two years, for example, users must take and pass an exam that covers the rules and requirements of using the information in DAVID. The exam is similar to the literature concerning AUPs, where users must acknowledge the expectations of using the database. However, where the DAVID exam fails to meet the requirement of understanding and acknowledging an AUP, as discussed in this research, is the exam does not cover the aspects of an AUP nor ask questions that pertain to an AUP concerning DAVID. In addition, users may repeat the DAVID exam until they achieve a passing score of 80%. The unlimited ability to retake the DAVID

exam becomes a perfunctory action by the user, who can achieve a passing score without preparation or study. Another requirement of DAVID (2021) is that users, each time they log on, must now acknowledge a warning that states the following:

> All data contained within the DAVID system is sensitive and privileged information and shall be handled accordingly. To maintain the integrity of this information, the records will be accorded proper management and security, and will only be accessed and used by authorized personnel in accordance with state and federal law. Activity associated with any aspect of the DAVID system is subject to detailed monitoring and audits to protect against improper or unauthorized use. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, dissemination, sharing, copying, or passing of DAVID information to unauthorized users and could result in civil proceedings against the offending agency and/or criminal proceedings against any user or other person involved. Violations or misuse may also subject the user and the user's agency to administrative sanctions and possible disciplinary action by their agency and could result in DAVID access termination. Accessing the DAVID system by any individual or agency constitutes their consent to the monitoring of all activities, as well as consent to the suspension or termination of their access privileges during or following any audit that determines misuse of the system. Digital images are restricted for use pursuant to S.322.142(4), Florida Statutes - images include photographs and signatures. (DAVID, 2021)

Once the user clicks on a checkbox acknowledging the warning, they can access DAVID freely and without further restriction. While, on the surface, this warning would appear to be an extensive and effective deterrent against misuse, a study by Obar and Oeldorf-Hirsch (2020) argued that users of media that requires acknowledgment of a terms of service do not read the terms and find them to be a nuisance. Obar and Oeldorf-Hirsch (2020) go on to report that people ignore terms of service to pursue their ends of digital production without being inhibited by the means. This is to say, users of DAVID know that they must click the checkbox to access the information they need, regardless of the warning. Therefore, other means of education and deterrence are needed to ensure that the usage terms of DAVID are acknowledged and understood.

Florida State University developed a newer derived database known as ELVIS to provide more comprehensive data from both in-state and out-of-state queries, criminal histories, and more audit trails for review by the system managers (Florida State University, 2022). ELVIS touts advanced authentication access, often referred to as two-factor authentication, desktop and mobile access, ease of access to reports, and free access to FCIC/NCIC (Florida State University, 2022). Arguably, this system may replace DAVID in the near future as the standard for vehicle database queries. However, this research would apply the same independent variables to ELVIS as it did to DAVID by asking if the application of SOPs, ethics training, AUPs, and disciplinary procedures provide proper oversight and prevent access violations. ELVIS is more advanced and more secure, but who or what deters a user from misusing the information once they are in the database? ELVIS is an improvement over DAVID in that it allows for a better audit trail for system managers (POCs), which should make tracking a violation by the

POC easier after it happens. Despite these improvements, the purpose of general deterrence strategies is to prevent the violation in the first place, not just respond to it after it occurs. Furthermore, with ELVIS allowing access to an even greater amount of sensitive information, deterrence and oversight is of the utmost importance. Like DAVID and ELVIS, other databases such as NCIC, FCIC, N-DEx, LEEP, and NGI, present the same question for the system manager that was presented to the POCs in this study. Does the application of general deterrence strategies of SOPs, ethics training, AUPs, and disciplinary procedures impact oversight and prevent access violations? Future research on this question, as it relates to other databases, are beyond the scope of this study but will be needed to obtain a definitive answer.

Recommendations

DAVID is an important law enforcement tool that needs safeguards to prevent misuse by users. The survey questions that were answered by the POCs who oversee the database revealed some weaknesses in the present safeguards that need to be addressed by the FLHSMV. One such safeguard improvement is to ensure that general deterrence strategies are codified in the MOU. FLHSMV should require that for an agency to allow access to its database, that agency must have an SOP that addresses DAVID use, defines the procedures for DAVID access, and delineates the role and responsibilities of both the POCs and the users. In addition, the FLHSMV should require each user to sign and acknowledge an AUP that clearly explains expectations for how the information within DAVID is to be used and handled, defines unacceptable behaviors with regard to the information, and outlines the potential penalties for violating the AUP. These signed AUPs would then stay on file for the entire time the user has access to DAVID. While

ethics training and disciplinary procedures were seen as less effective methods of oversight and deterrence, they too may still serve a key role in reducing the likelihood of an access violation and exposing of the agency to civil liability. For instance, the FLHSMV may choose to provide a short training session by way of an online tutorial or video that expresses how to use the information properly and ethically. This training can be provided as a prerequisite to users' initial access and then repeated at the same time as the biannual exam. Disciplinary procedures concerning DAVID misuse must be consistent, proportionately severe, and certain. To accomplish this level of seriousness, violations of DAVID must be spelled out by the agency, even if they only mirror the state law, indicating that a violator shall face criminal charges, civil penalties, and be held personally responsible for any and all fines. These punishments must appear not only in the AUP, but on the DAVID logon screen and as part of the ethics training. The POCs' oversight responsibility would then be to ensure that these items and procedures exist within the agency and that all requirements are completed by the user to retain access credentials.

A final note on recommendations stems from survey question Q7, which was discussed earlier in the methodology section of this study. This question asked the POCs if they would more easily be able to perform their audit duties in DAVID if DAVID users were required to enter an associated case number, court case number, or computer aided dispatch call number for each DAVID search. Of the 79 respondents who answered this question, (n = 54, 68%) answered in the affirmative. Question Q7 was not designed, nor should it be viewed for statistical analysis of the effect of the independent variables on the dependent variable, but rather as a test question to form the basis for the following

recommendation. FLHSMV should update DAVID to require the case number, court case number, or computer aided dispatch call number for each and every new search conducted in DAVID. With this requirement, the user would be affirming the lawfulness of their search activity, and once the POC conducts their quarterly audit, they would readily see the case numbers and could cross-check the search accordingly. In addition, this requirement would be a deterrent in that it would force users to acknowledge their understanding that every search would be tagged with a case number for easy audit by the POC. If the DAVID user, for any reason, were not assigned to a call or court case, but wished to search DAVID, FLHSMV should provide a *no call assigned* choice. This selection would raise an audit flag to the POC that a user is performing a blind search within the database that may or may not be related to lawful activity, and the search should be further scrutinized. This function change should also be updated in the MOU, the SOPs, and the AUPs, all of which function as deterrents and provide fair warning to DAVID users that the use of DAVID needs to be for lawful activity. Entering false information into the case number field would constitute a violation of the DPPA and subject the user to criminal and civil liability.

Conclusion

This study used multiple regression to examine and test four independent variables of general deterrence on POC oversight of Florida's DAVID. The four independent variables tested were SOPs, ethics training, AUPs, and disciplinary procedures, and they were hypothesized to show a predictive correlation on POC oversight of DAVID as well as to help the POCs deter access violations. The analysis showed that the correlation between SOPs and AUPs on oversight were most effective,

while the correlation on ethics training and disciplinary procedures were not effective. Mitigating factors such as lower survey participation and skipped questions might have accounted for the non-correlation of ethics training and disciplinary procedures that were explained in the study limitations. The overall analysis revealed that two of the four variables had a measurable impact on the ability of the POCs to perform their duties, therefore, the theory of general deterrence by way of the independent variables held consistent with the overall goal of the study.

The extant literature on SOPs matched the results of the study and also opened potential avenues of future research on how they can be better applied in database management. Likewise, extant literature on AUPs matched the results of the study and opened potential avenues of future research on how they can be better applied to database management. Conversely, the literature on ethics training and disciplinary procedures ran counter to the study, but their difference can be explained in the reduced number of participants.

This goal of this research study was to expand the body of knowledge in the field of public administration by examining the complex relationship between policies that govern law enforcement databases and how they impact the oversight and behaviors of those who use them. Continued research on the relationship between the behaviors that violate policies and procedures and the use of general deterrence to effectively manage and prevent those violations is quintessential in DAVID management. Thus, an inherent mission of the FLHSMV, the numerous agencies who use DAVID, and the POCs who provide oversight should be to furnish tools and education to the users such that they give pause and influence them against committing an access violation. If the FLHSMV,

agencies, and POCs work together to implement tested and proven strategies to achieve this mission, they can achieve the proper use and security of information contained within DAVID, reduce the agencies' risk of civil liability, and most importantly, build and foster community members' confidence that their personal and confidential information is used solely for lawful purposes by those entrusted to use it.

REFERENCES

Agency for Health Care Administration. (2013). *Review of the Agency's Data Exchange MOU with DHSMV.* Tallahassee: Office of the Inspector General. https://ahca.myflorida.com/Executive/Inspector_General/Internal_Audit/docs/FY2013-2014/13-15ReviewoftheAgency'sDataExchangeMOUwithDHSMV.pdf

Andenaes, J. (1970). The morality of deterrence. *The University of Chicago Law Review, 37*(4), 649-664. https://doi:10.2307/1598839

Apel, R. (2013). Sanctions, perceptions, and crime: Implications for criminal deterrence. *Journal of Quantitative Criminology, 29*(1), 67-101. https://doi.org/10.1007/s10940-012-9170-1

Ashworth, L. D. (2007). Quality-control: Standard operating procedures-an essential tool for developing quality preparations. *International Journal of Pharmaceutical Compounding, 11*(3), 226-228.

Bayley, B. K. (2012). Organizational ethics training: A proactive perspective. *The Journal for Quality and Participation, 35*(2), 15-19.

Bishopp, S. A., Worrall, J., & Piquero, N. L. (2016). General strain and police misconduct: The role of organizational influence. *Policing, 39*(4), 635-651. https://doi.org/10.1108/PIJPSM-10-2015-0122

Bourne, J., & Powell, L. (2020, Nov 24). *10 investigates: Government workers abusing access to your private info face new consequences*. WTSP. https://wtsp.com/article/news/investigations/10-investigates/government-private-information-abuse/67-2ddbb412-a70b-4cf7-ae28-22484aab6205

CALEA. (2021). *Law Enforcement - Standards Titles*. www.calea.org/node/11406

Chalfin, A., & McCrary, J. (2017). Criminal deterrence: A review of the literature. *Journal of Economic Literature, 55*(1), 5-48. https://doi.org/10.1257/jel.20141147

Chambliss, D., & Schutt, R. (2013). *Making Sense of the Social World: Methods of Investigation* (4th ed.). Sage.

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information and Computer Security, 25*(2), 118-136. https://doi.org/10.1108/ICS-03-2017-0013

DAVID. (2021). *Advanced Record Search*. https://david.flhsmv.gov/DAVID/Search

de Schrijver, A., & Maesschalck, J. (2015). The development of moral reasoning skills in police recruits. *Policing, 38*(1), 102-116. https://doi.org/10.1108/PIJPSM-09-2014-0091

de Treville, S., Antonakis, J., & Edelson, N. M. (2005). Can standard operating procedures be motivating? reconciling process variability issues and behavioural outcomes. *Total Quality Management & Business Excellence, 16*(2), 231-241.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy: SSIS. *International Journal of Information Management, 31*(3), 201. https://doi.org/10.1016/j.ijinfomgt.2010.06.001

Donner, C., Maskaly, J., & Fridell, L. (2016). Social bonds and police misconduct. *Policing, 39*(2), 416-431. https://doi.org/10.1108/PIJPSM-10-2015-0109

Driver Privacy Protection Act (DPPA), 18 U.S. Code § 2721. (1994). https://www.law.cornell.edu/uscode/text/18/2721

Escambia County Corrections. (2017, Feb 09). *Memorandum of understanding for governmental access to driver and vehicle information database (DAVID).* https://www.agenda.myescambia.com/docs/2017/REGBCC/20170316_3796/11825_MOU%2003-02-2017.pdf

Etter, G. W., & Griffin, R. (2011). In-service training of older law enforcement officers: An andragogical argument. *Policing, 34*(2), 233-245. https://doi.org/10.1108/13639511111148861

Fan, M. D. (2012). Panopticism for police: Structural reorm bargaining and police regulation by data-driven surveillance. *Washington Law Review, 87*(1), 93-138.

FDLE. (2021). *Network of Florida Fusion Centers*. Florida Department of Law Enforcement. https://www.fdle.state.fl.us/FFC/Regional-Fusion-Centers

FDLE. (n.d.). *Crminal Justice Agency Links*. Florida Department of Law Enforcement. https://www.fdle.state.fl.us/CJSTC/Publications/Criminal-Justice-Agency-Links.aspx

Federal Bureau of Investigation. (n.d.). *National Crime Information Center (NCIC)*. Criminal Justice Information Services. https://fbi.gov/services/cjic/ncic

FLHSMV. (2020). *Open Government Office of the Inspector General.* https://flhsmv.gov/resources/open-government/office-of-the-inspector-general/

FLHSMV. (2021). *Courts and law enforcement: Driver and vehicle information database*. https://www.flhsmv.gov/courts-enforcement/david/

Flink, W. L. (1995). Judical application of the law enforcement code of ethics. *The Police Chief, 62*(2), 27-30.

Florida State University. (2022). *About Elvis*. ELVIS Florida. https://www.elvisflorida.org/About/ELVIS

Flowers, B. F., & Rakes, G. C. (2000). Analyses of acceptable use policies regarding the internet in selected K-12 schools. *Journal of Research on Computing in Education, 32*(3), 351.

Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why users (fail to) read computer usage policies. *Industrial Management & Data Systems, 108*(6), 701-712. https://doi.org/10.1108/02635570810883969

Ford, C. (2015). *Understanding Q-Q- Plots*. University of Virginia Library. https://data.library.virginia.edu/understanding-q-q-plots/

Galarnyk, M. (2018). *Understanding Boxplots*. Towards Science. https://towardsdatascience.com/understanding-boxplots-5e2df7bcbd51

Gardner, L. (2017, September 17). *I-TEAM: Unauthorized searches made on law enforcement database*. News4Jax. https://www.news4jax.com/news/2017/09/27/i-team-unauthorized-searches-made-on-law-enforcement-database/

Gely, R., Cheramie, A., R., & Chandler, T. D. (2016). An empirical assessment of the contract based exception to the employment-at-will rule. *Employee Responsibilities and Rights Journal, 28*(1), 63-78. https://doi.org/10.1007/s10672-015-9273-6

Gough, J. M., & Hamrell, M. P. (2010). Standard operating procedures (SOPs): How to write them to be effective tools. *Drug Information Journal, 44*(4), 463-468.

Gurman, S. (2016, Sep 28). *AP: Across US, police officers abuse confidential databases*. Associated Press. https://apnews.com/699236946e3140659fff8a2362e16f43/ap-

across-us-police-officers-abuse-confidential-databases#:~:text=But%20the%20AP%2C%20through%20records,times%20between%202013%20and%202015.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Harris, C. J., Chierus, K., & Edson, T. C. (2015). The prevalence and content of police discipline matrices. *Policing, 38*(4), 788-804. https://doi.org/10.1108/PIJPSM-10-2014-0113

Helfers, R. C., Reynolds, P. D., & Maskály, J. (2020). Prior discipline and performance among police officers: Does organizational fairness matter? *Criminology, Criminal Justice, Law & Society, 21*(3), 1-16.

Hickman, M. J., Powell, Z. A., Piquero, A. R., & Greene, J. (2016). Exploring the viability of an attitudes toward ethical behavior scale in understanding police integrity outcomes. *Policing, 39*(2), 319-337. https://doi.org/10.1108/PIJPSM-11-2015-0130

Holmes, J. (2003). Formulating an effective computer use policy. *Information Strategy, 20*(1), 26.

Hughes, T. (2001). Police officers and civil liability. *Policing, 24*(2), 240-262. https://doi.org/10.1108/13630510110390972

Huriash, L. J. (2017, Feb 09). *Trooper who pulled over speeding cop loses privacy lawsuit against Miami officers*. Sun Sentinel. https://www.sun-sentinel.com/local/broward/fl-sb-jane-watts-miami-case-20170208-story.html

Ivkovic, S. K., Peacock, R., & Haberfeld, M. (2016). Does discipline fairness matter for the police code of silence? answers from the US supervisors and line officers. *Policing, 39*(2), 354-369. https://doi.org/10.1108/PIJPSM-10-2015-0120

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods, 8*(4), 49-62. doi:doi.org/10.1177/160940690900800406

Kallaman, J. (2006). Creating a standard operating procedures manual. *Risk Management, 53*(10), 42.

Kaptein, M. (2015). The effectiveness of ethics programs: The role of scope, composition, and sequence: JBE. *Journal of Business Ethics, 132*(2), 415-431. https://doi.org/10.1007/s10551-014-2296-3

Klockars, C. B., Ivkovich, S. K., & Haberfield, M. (2005). *Enhacing Police Intergrity.* National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/209269.pdf

Laerd Statistics. (2018). *Linear Regression Analysis using SPSS Statistics*. Laerd Statistics. https://statistics.laerd.com/spss-tutorials/linear-regression-using-spss-statistics.php

Lexipol. (2021). *Law Enforcement Directory Search*. Police1. https://www.police1.com/law-enforcement-directory/search/

Logan, W. A. (2019). Policing police access to criminal justice data. *Iowa Law Review, 104*(2), 619-677.

Mauney, M. (2014, Feb 13). *Trooper who stopped speeding cop sues after harassment, privacy violations*. Orlando Sentinel.

https://www.orlandosentinel.com/features/gone-viral/os-trooper-sues-police-agencies-harassment-20140213-post.html

Morgan, B., Morgan, F., Foster, V., & Kolbert, J. (2000). Promoting the moral and conceptual development of law enforce trainees: A deliberate psychological educational approach. *Journal of Moral Education, 29*(2), 203-218.

Nawawi, A., & Ahmad Saiful Azlin, P. S. (2018). Employee fraud and misconduct: Empirical evidence from a telecommunication company. *Information and Computer Security, 26*(1), 129-144. https://doi.org/10.1108/ICS-07-2017-0046

Nixon, T. S., & Barnes, J. C. (2019). Calibrating student perceptions of punishment: A specific test of general deterrence. *American Journal of Criminal Justice : AJCJ, 44*(3), 430-456. https://doi.org/10.1007/s12103-018-9466-2

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Office of the Inspector General. (2018). *DAVID Audits: Audit Report 201718-23.* Tallahassee: FLHSMV.

Pizzi, W. T. (2012). Understanding the United States' incarceration rate. *Judicature, 95*(5), 207-211.

Pogarsky, G., & Piquero, A. (2004). Studying the reach of detterence: Can deterrence theory help explain police misconduct. *Journal of Criminal Justice, 32*(4), 371-386.

Qualtrics XM. (2022). *How to increase survey response rates*. https://www.qualtrics.com/experience-management/research/tools-increase-response-rate/

Remler, D., & Ryzin, G. (2015). *Research Methods in Practice* (2nd ed.). Los Angeles: Sage.

Ruhnka, J., & Loopesko, W. E. (2013). Risk management of email and internet use in the workplace. *The Journal of Digital Forensics, Security and Law : JDFSL, 8*(3), 7-19.

Rushin, S. (2021). Police arbitration. *Vanderbilt Law Review, 74*(4), 1023-1078.

Schniepp, S. (2015). Crafting standard operating procedures. *Pharmaceutical Technology Europe, 27*(12), 65-66.

Sekhon, N. (2017). Purpose, policing, and the fourth amendment. *Journal of Criminal Law & Criminology, 107*(1), 65-129.

Sekhon, N. (2019). Police and the limit of the law. *Columbia Law Review*, 1711-1772.

Senat, J. (2001). Reno v. Condon opens door to more access limits. *Newspaper Research Journal, 24*(2), 63-81.

Slobogin, C. (2017). Policing, databases, and surveillance. *Criminology, Criminal Justice, Law & Society, 18*(3), 70-84.

Statistics How To. (2022). *Durbin Watson Test & Test Statistic*. Statistics How To. https://www.statisticshowto.com/durbin-watson-test-coefficient/

Storm, D. (2016, Sep 28). *Cops run unauthorized searches on confidential databases for revenge, stalking*. Computerworld.

https://www.computerworld.com/article/3124641/cops-run-unauthorized-searches-on-confidential-databases-for-revenge-stalking.html

Strauss, A., & Corbin, J. (2009). *Basics of qualitative research: Grounded theory procedures and techniques.* CA: Sage.

Stucke, M. E. (2014). In search of effective ethics & compliance programs. *Journal of Corporation Law, 39*(4), 769-832.

Thomas, S. L., Rothschild, P. C., & Donegan, C. (2015). Social networking, management responsibilities, and employee rights: The evolving role of social networking in employment decisions. *Employee Responsibilities and Rights Journal, 27*(4), 307-323. https://doi.org/10.1007/s10672-014-9250-5

Timmann, C. (2019). *Driver and Vehicle Information Database System.* Stuart: Clerk of the Court & Comptroller. https://www.martinclerk.com/DocumentCenter/View/121/DAVID-Memorandum-of-Understanding-2019-PDF

Tomlinson, E. C., & Bockanic, W. N. (2009). Avoiding liability for wrongful termination: "ready, aim,...fire!". *Employee Responsibilities and Rights Journal, 21*(2), 77-87. https://doi.org/10.1007/s10672-008-9068-0

Tomlinson, K. (2016). An examination of deterrence theory: Where do we stand? *Federal Probation, 80*(3), 33-38,57.

U.S. Department of Justice. (2016, May). *Five Things About Deterrence.* National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/247350.pdf

Ugrin, J. C., & Pearson, J. M. (2008). Exploring internet abuse in the workplace: How can we maximize deterrence efforts? *Review of Business, 28*(2), 29-40.

Vick, J. (2016). "Putting cruelty first": Liberal penal reform and the rise of the carceral state. *Social Justice, 42*(1), 35-52,146.

Walker, S. (2006). *Police accountability: Current issues and research needs.* Washington, DC: US Department of Justice. https://olp.gov/pdffiles1/nij/grants/218583.pdf

Weeden, M. (2013, Dec). Pyramid scheme. *Quality Progress, 46*, p. 80.

Worden, R., Harris, C., & McLean, S. J. (2014). Risk assessment and risk management in policing. *Policing, 37*(2), 239-258. https://doi.org/10.1108/PIJPSM-12-2012-0088

APPENDIX A:

DAVID Point of Contact Survey Instrument

Introduction Block

You are being asked to participate in a survey research project entitled "The Effect of General Deterrence Variables on Point of Contact Oversight in the Driver and Vehicle Information Database (DAVID)," which is being conducted by Gary Gordon, a student at Valdosta State University. The purpose of the study is to determine how much of an impact the implementation of deterrence strategies have on your oversight and administrative duties in DAVID. You will receive no direct benefits from participating in this research study. However, your responses may help us learn more about managing DAVID in such a way that abuses within the database are less likely to occur. There are no foreseeable risks involved in participating in this study other than those encountered in day-to-day life. Participation should take approximately 10-12 minutes to complete. This survey is confidential and anonymous. No one, including the researcher, will be able to associate your responses with your identity. Your participation is voluntary. You may choose not to take the survey, to stop responding at any time, or to skip any questions that you do not want to answer. Participants must be at least 18 years of age to participate in this study. Your completion of the survey serves as your voluntary agreement to participate in this research project and your certification that you are 18 or older. You may print a copy of this statement for your records.

Questions regarding the purpose or procedures of the research should be directed to Gary Gordon at gbgordon@valdosta.edu. This study has been exempted from Institutional Review Board (IRB) review in accordance with Federal regulations. The IRB, a university committee established by Federal law, is responsible for protecting the rights and welfare of research participants. If you have concerns or questions about your rights as a research participant, you may contact the IRB Administrator at 229-253-2947 or irb@valdosta.edu.

Do you wish to continue to the survey?

- ○ Yes, I want to proceed
- ○ No, I do not want to proceed

Demographics Block

D1 Please indicate the approximate the number of sworn officers in your agency?

- ○ 20 sworn officers or less
- ○ 21 - 50 sworn officers
- ○ 51- 100 sworn officers
- ○ 101 - 200 sworn officers
- ○ 201 or greater

D2 Please indicate the best approximate geographic location of your agency?

- ○ North Florida including the panhandle
- ○ Central Florida
- ○ South Florida

D3 How long have you been a DAVID Point of Contact for your agency?

- ○ Less than 1 year
- ○ 1 - 2 years
- ○ 3 - 4 years
- ○ 5 years or greater

D4 Which level of sworn officers in your agency are granted DAVID access?

- ○ Any sworn officer may be granted DAVID access
- ○ Only sworn officers demonstrating a specific need for DAVID
- ○ Only supervisors and higher

- ○ Only select personnel based on assignment (i.e. detectives, dispatchers)

U1a Are the officers in your agency under a collective bargaining agreement or union?

- ○ Yes
- ○ No

U1b Does the collective bargaining agreement or union in any way limit your DAVID oversight responsibilities?

- ○ Yes
- ○ Maybe
- ○ No

Q1a Does your agency have a Standard Operating Procedure (SOP) that addresses your oversight and how DAVID is to be used by personnel?

- ○ Yes
- ○ No

Q1b The Standard Operating Procedure for DAVID is clear, concise, easily accessible, and spells out my responsibilities as the Point of Contact and responsibilities of personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q1c Based on the wording in the Standard Operating Procedure, I can effectively manage DAVID user access and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q1d If my agency had a clear and concise Standard Operating Procedure for DAVID, I would be able to more effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q2a Does your agency provide or require any Ethics Training on sensitive data use prior to you granting DAVID access to personnel?

- ○ Yes
- ○ No

Q2b The Ethics Training provided by my agency enhances my oversight responsibilities by providing proper guidance to all personnel on how to use sensitive data?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q2c Based on the Ethics Training provided by my agency, I can effectively manage DAVID user access and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q2d If my agency provided Ethics Training on sensitive data use prior to being granted DAVID access, I would be able to more effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q3a An Acceptable Use Policy (AUP) is a document which governs the use of a network or system and covers a wide range of issues surrounding the rights, responsibilities and privileges – as well as sanctions – connected with computer use. Does your agency provide or require you and your personnel to acknowledge an Acceptable Use Policy concerning DAVID?

- ○ Yes
- ○ No

Q3b The wording in the Acceptable Use Policy provided by my agency sets clear expectations of my DAVID oversight and the expectations by agency personnel?

- ○ Strongly agree

- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q3c The Acceptable Use Policy provided by my agency allows me to effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q3d If my agency had an Acceptable Use Policy for DAVID access, I would be able to more effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q4a Does your agency have a Disciplinary Procedure that will be taken against personnel who violate DAVID access?

- ○ Yes
- ○ No

Q4b The Disciplinary Procedure provided by my agency is consistent, standardized, and spells out what steps and punishments will occur if personnel violate DAVID access?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q4c The Disciplinary Procedure enacted by my agency allows me to effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q4d If my agency provided a consistent and standardized Disciplinary Procedure, I would be able to more effectively manage DAVID and deter potential access violations by personnel?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q5a As a Point of Contact, which of the following would be the most effective in helping you manage DAVID and deterring potential access violations?

- ○ Having a clear and concise Standard Operating Procedure
- ○ Requiring Ethics Training on handling sensitive data
- ○ Requiring acknowledgment of an Acceptable Use Policy
- ○ Enforcing a consistent and standardized Disciplinary Procedure

Q5b As a Point of Contact, which of the following would be the least effective in helping you manage DAVID and deterring potential access violations?

- ○ Having a clear and concise Standard Operating Procedure
- ○ Requiring Ethics Training on handling sensitive data
- ○ Requiring acknowledgment of an Acceptable Use Policy
- ○ Enforcing a consistent and standardized Disciplinary Procedure

Q6a How many known usage violations in DAVID have occurred within your agency over the past 5 years? This includes multiple violations by the same person.

- ○ 0
- ○ 1-2
- ○ 3-5
- ○ 6-9
- ○ 10 or greater

Q6b How many suspected usage violations in DAVID have occurred within your agency over the past 5 years? This includes multiple violations by the same person.

- ○ 0
- ○ 1-2
- ○ 3-5
- ○ 6-9
- ○ 10 or greater

Q7 If a DAVID user were required to enter an associated case number, court case number, or CAD call number to each DAVID search, I could more easily perform my audit duties within DAVID?

- ○ Strongly agree

- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q8 Today, I have all the tools necessary to properly perform my oversight duties within DAVID?

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

APPENDIX B:

IRB Exemption Report

Institutional Review Board (IRB)
For the Protection of Human Research Participants

PROTOCOL EXEMPTION REPORT

Protocol Number: 04182-2021 **Responsible Researcher(s):** Gary Gordon

Supervising Faculty: Dr. Carol Glen

Project Title: *The Effect of General Deterrence Variables on Oversight of Florida's Driver and Vehicle Information Database (DAVID).*

INSTITUTIONAL REVIEW BOARD DETERMINATION:

This research protocol is **Exempt** from Institutional Review Board (IRB) oversight under Exemption **Category 2.** Your research study may begin immediately. If the nature of the research project changes such that exemption criteria may no longer apply, please consult with the IRB Administrator (irb@valdosta.edu) before continuing your research.

ADDITIONAL COMMENTS:

- *Upon completion of this research study all collected data (survey responses, email address list, email correspondence, etc.) must be securely maintained (locked file cabinet, password protected computer, etc.) and accessible only by the researcher for a minimum of 3 years. At the end of the required time, collected data must be permanently destroyed.*

☒ ***If this box is checked, please submit any documents you revise to the IRB Administrator at irb@valdosta.edu to ensure an updated record of your exemption.***

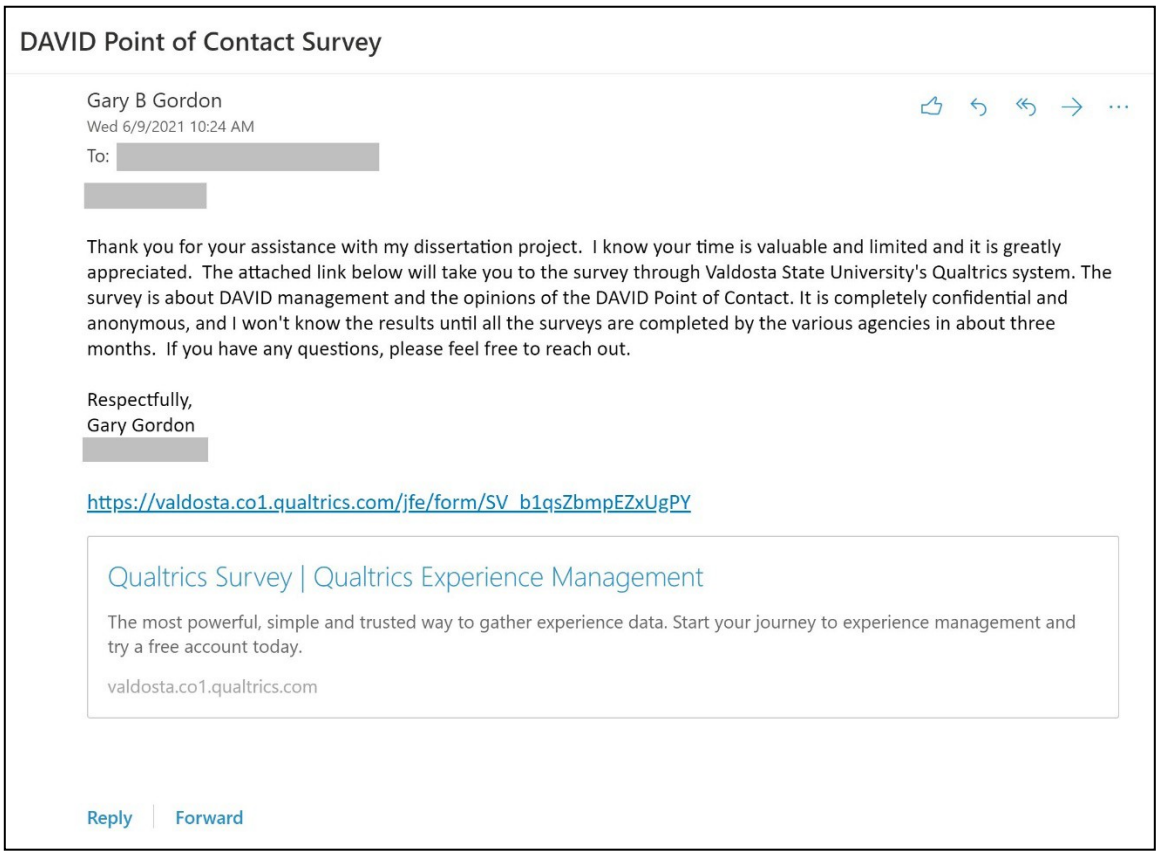
Elizabeth Ann Olphie *06.02.2021*
Elizabeth Ann Olphie, IRB Administrator

Thank you for submitting an IRB application.
Please direct questions to irb@valdosta.edu or 229-253-2947.

Revised: 06.02.16

APPENDIX C:

Email Sample (Redacted)


DAVID Point of Contact Survey
Gary B Gordon
Wed 6/9/2021 10:24 AM
To:
Thank you for your assistance with my dissertation project. I know your time is valuable and limited and it is greatly appreciated. The attached link below will take you to the survey through Valdosta State University's Qualtrics system. The survey is about DAVID management and the opinions of the DAVID Point of Contact. It is completely confidential and anonymous, and I won't know the results until all the surveys are completed by the various agencies in about three months. If you have any questions, please feel free to reach out.
Respectfully,
Gary Gordon
https://valdosta.co1.qualtrics.com/jfe/form/SV_b1qsZbmpEZxUgPY
Qualtrics Survey | Qualtrics Experience Management
The most powerful, simple and trusted way to gather experience data. Start your journey to experience management and try a free account today.
valdosta.co1.qualtrics.com
Reply
Forward