2002

Mobile computing & law enforcement: An Examination of its application in the field and its consequences

Lanny Lockhart Jr

Mobile Computing & Law Enforcement: An Examination of Its Application in the Field and Its Consequences

By

Lanny Lockhart, Jr.

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
Of
Computing and Information Sciences

April 29, 2002

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College
Of
Computing and Information Sciences

Mobile Computing & law Enforcement: An Examination of Its Application in the Field and Its Consequences

I, Lanny Lockhart, Jr., hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 29 APR 02 Signature of Author: _____

Masters of Science in Information Technology

Capstone Thesis Approval Form

Student Name: Lanny Lockhart, Jr.

Student Number:

Thesis Title: Mobile Computing & Law Enforcement: An Examination of Its Application in the Field and Its Consequences

Thesis Committee:

Name	Signature	Date
Prof. Steve Jacobs Chair		4/30/02
Dr. John Klofas Committee Member		4/12/02
Prof. LaVerne McQuiller-Williams Committee Member		4/12/02
Graduate Program Chair		

ABSTRACT

The following study has been conducted in the pursuit of a Masters Degree of Science in Information Technology. The functional purpose of this study was to examine three basic concepts (officer efficiency, safety, and arrest rates) within law enforcement and to attempt to determine if a specific type of information technology (wireless data computers) has had any positive impact on those concepts. To that end, the author has reviewed the history of technology in law enforcement and surveyed a group of patrol officers in the Wilmington Police Department. Difficulties associated with gathering research data from law enforcement agencies has also been noted and described. The results garnered from statistical analysis are covered in detail.

ACKNOWLEDGEMENTS

A number of people have contributed, directly and indirectly, to this project, and I thank all of them.

First of all is the late Dick Lewis. He set me on this path oh so many years ago, and I miss him dearly.

Special thanks to Dr. John Klofas who picked up Dick's mantle and has been burdened with me ever since. He has placed many opportunities before me, and I am thankful for each of them.

Steve Jacobs is gratefully acknowledged for duties accepted and graciously carried out as this project has stumbled on more than one occasion.

A respectful nod is given to the Criminal Justice faculty of RIT for providing me with the academic tools needed to succeed in my chosen profession. Without their efforts I would not be where I am today.

Another nod is presented to Prof. Elizabeth L. Lawley for her Defense input which has strengthened this document and this researcher.

To the late Gene Roddenberry for creating a universe that started my love affair with technology.

Most of all to my beloved bride Joy, whose love, support, and good humor were the guiding stars that kept me on course through all of the dark times.

To two girls,

My beloved bride Joy and my daughter Mal

TABLE OF CONTENTS

LIST OF TABLES

LIST OF DIAGRAMS

Mobile Computing & Law Enforcement: An Examination of Its Application in the Field and Its Consequences

Introduction

The United States criminal justice system, particularly that of the 1990s, has easily been one of the most technologically advanced such systems in the world. Examples include:

- Police helicopters are using infrared sensors to track suspects;
- Patrol cars are carrying video cameras to monitor both officers and suspects, and the recorded imagery is being used to good effect in courts across the country (Seaskate, Inc., p. 60);
- Officers now wear the latest body armor and carry a number of different less-than-lethal and lethal weapons;
- The time-honored crime-fighting method of fingerprinting has evolved into highly effective Automated Fingerprint Identification Systems (AFIS) allowing police officers greater flexibility and speed in identifying suspects[1]; and
- DNA testing has aided in countless cases where little other physical evidence was available.

The most recent high-tech addition for police officers has been wireless notebook computers. These devices are now being installed in patrol cars across the United States, and officers are connecting to criminal justice databases without the assistance of dispatchers.

---

[1]For many years, fingerprinting was a solitary art requiring a significant amount of time and expertise for any degree of success.

The question becomes, have wireless notebooks been effective? Vendors and politicians often cite the marvels of wireless data technology to the criminal justice community in press ads and at marketing demonstrations (Capitol Connections, 2000). Police officials across the country often hear of increases in officer efficiency, arrest rates, and safety as a result of the use of this technology, but few facts are presented to support these claims. On the surface, it would make sense to expect an increase in any of these three areas through the advent of modern computing technology, particularly in a paperwork-driven environment such as police work. Since few scientific studies have been conducted to examine the impact of information technology rollouts in the field of law enforcement, it is of vital importance to the criminal justice field for the actual efficiency increases to be determined. Most, if not all, modern police agencies are facing shrinking budgets, and can ill afford to spend allotted tax dollars on flashy, but ineffective technology. Police officials have to be well informed before they decide to purchase expensive computer systems that will be more of a hindrance than a benefit and that cannot be easily replaced.

To that end, this researcher has begun investigating the current state of affairs in the field of law enforcement with regard to the usage of mobile computing technology. Where appropriate, the technology of preference has been examined and discussed. Six police departments have been identified and contacted for relevant information. The results of those contact attempts have been documented.[2] One department in particular, the Wilmington Police Department, was quite willing to be of assistance and allowed this

[2] These results bear consideration in and of themselves due to the conclusions they have produced regarding the current attitude of law enforcement administrators and their technology choices. It is hoped that this first investigation into the new arena of law enforcement and Information Technology will open the door to more studies with a wider base of participating departments.

researcher to survey its patrol officers for their input on technology usage within that department. Those survey results have been analyzed, and conclusions generated from the gathered data. Though specific to that organization and limited in scope, the data retrieved should also be of value as an initial examination of the use of wireless data technology in the field by patrol officers, and when examined for its relevance to the greater law enforcement community.

Literature Review

Despite the apparent ease of adoption inferred from the opening paragraph, most of the advancements in police methodology and technology in the last century have neither been quickly, nor easily adopted (Pursley, 1994, p. 214). Institutional, political, and sociological dynamics exist within the law enforcement community, as in almost any large administrative system, that hinder the acceptance of 'new ideas.' Administrators are hesitant to institute changes in processes, politicians are ever reluctant to release new funds to certain public agencies, and police officers work within a machoistic sub-culture that has its own affect on change acceptance. As a result, changes within the law enforcement community come slowly and, generally, as a result of outward influence, the most notable of which being the court systems (Pursley, 1994, p. 214).

Interestingly enough, once those forces, either internal or external in nature, are applied, the resultant changes typically occur in a rapid, sweeping fashion, over a short period of time. The cycle then repeats, the reluctance to adopt new methods returns until the next wave of external pressure is applied. Additionally, the more than seventeen thousand police departments in the United States tend to adopt new technology in wildly different fashions that often bear little resemblance to each other (Seaskate, Inc., p. 4).

The Federal government attempted to break this cycle during the 1960s and 1970s with the formation of the Law Enforcement Assistance Administration (LEAA) and the Law Enforcement Education Program (LEEP), but that effort produced mixed results (Wrobleski & Hess, 1993, p. 48). The educational assistance component of the LEEP enabled numerous officers to advance in their own educations and was quite successful in advancing the professionalism of American law enforcement (Brule, 1997). At the same time, as described shortly, the technological implementations fostered by the LEAA often foundered. Before looking specifically at laptop computers, it will be beneficial to review the basic history of technology transfer in American law enforcement in order to better understand the principle .

Historical Overview

The history of modern American policing is broken up into three phases: the political era, the reform era, and the community era (Wrobleski & Hess, 1993, pp. 43-51). The first of these three eras was a period of time marked by both widespread police corruption and varied technological adoptions. Covering the years between 1840 and 1930, the political era saw the rapid adoption of new equipment and ideas despite corruptive influences. As Table 1 demonstrates, the various technologies of that time were adopted relatively quickly (upon the discovery/creation of the technology) by different police departments. For example, call boxes made a rapid entry into the field of law enforcement. Created and deployed in Chicago in the early 1880s, the call box was later hailed as a hallmark of police innovation by Chief Francis O'Neill in a 1903 speech before the International Association of Chiefs of Police (Seaskate, 1998, p. 96). The then new ability to directly call for assistance and communicate with headquarters was a

tremendous breakthrough for the average patrol officer and heralded a new age in modern law enforcement[3]. In the Political Era, this achievement would only be eclipsed by Sir Francis Galton's introduction of fingerprinting in 1892 (Johnson, 1988, p. 253).

1850s The first multi-shot pistol, introduced by Samuel Colt, goes into mass production. The weapon is adopted by the Texas Rangers and, thereafter, by police agencies nationwide.	1901 Scotland Yard adopts a fingerprint classification system devised by Sir Edward Richard Henry.
1854-59 San Francisco is the site of one of the earliest uses of systematic photography for criminal identification.	1923 The Los Angeles Police Department establishes the first police crime laboratory in the United States.
1877 The use of the telegraph by police and fire departments begins in Albany, New York in 1877.	1923 The use of the teletype is inaugurated by the Pennsylvania State Police.
1878 The telephone comes into use in police precinct houses in Washington, D.C.	1928 Detroit police begin using the one-way radio.
1880's Call boxes begin appearing in cities across the country.	1930 The prototype of the present-day polygraph is developed.

Table 1: Technology Adoption in the Political Era (Derived from Seaskate's "Police Technology Timeline", 1998, pp. 22 & 64)

The Reform Era, encompassing the years between 1930 and 1980, began as a response to the politically-driven corruption of the prior age and concluded at the end of the civil rights discord of the 1960s and 1970s (Wrobleski, 1993, p. 47). This time frame saw considerable changes in the field of technology and the world at large. Law enforcement, however, only saw major changes in its use of technology at the opposite ends of that fifty-year period. Table 2 displays some of those additions between 1930 and 1980. Police departments quickly went to two-way radio systems in the 1930s and 1940s for both foot and car patrols. They were equally prompt in incorporating

[3]Prior to this point, officers on patrol were "on their own" and had to deal with events without the ability to readily call for reinforcements or to call for guidance from superiors (Seaskate, 1998, p. 1).

automobiles into their departments' daily routines. The acceptance of new technology faded, though, by the end of the 1940s, and most police departments would not alter their overall technical offerings for decades to come.

1930s American police begin the widespread use of the automobile.	1960s The first computer-assisted dispatching system is installed in the St. Louis police department.
1932 The Federal Bureau of Investigation (FBI) inaugurates its crime laboratory, which, over the years, comes to be world-renowned.	1967 The FBI inaugurates the National Crime Information Center (NCIC), the first national law enforcement computing center. NCIC is a computerized national filing system on wanted persons and stolen vehicles, weapons, and other items of value.
1934 Boston Police begin using the two-way radio.	1968 AT&T announces it will establish a special number – 911 – for emergency calls to police, fire, and other emergency services. Within several years, 911 systems are in widespread use in large urban areas.
1948 Radar is introduced to traffic law enforcement.	1970s The large-scale computerization of U.S. police departments begins. Major computer-based applications in the 1970s include computer-assisted dispatch (CAD), management information systems, centralized call collection using three-digit phone numbers (911), and centralized integrated dispatching of police, fire, and medical services for large metropolitan areas.
1955 The New Orleans Police Department installs an electronic data processing machine, possibly the first department in the country to do so. The machine is not a computer, but a vacuum-tube operated calculator with a punch-card sorter and collator. It summarizes arrests and warrants.	1975 Rockwell International installs the first fingerprint reader at the FBI. In 1979, the Royal Canadian Mounted Police implements the first actual automatic fingerprint identification system (AFIS).

Table 2: Technology Adoption in the Reform Era (Derived from Seaskate's "Police Technology Timeline", 1998, pp. 22-23)

It wasn't until the civil unrest of the 1960s that steps were taken to modernize the technology used in law enforcement. The assassinations of President John F. Kennedy and Martin Luther King, Jr., along with the class riots raging across the United States, brought about the realization that American law enforcement had some fundamental problems within its core organizations. Those problems included procedural disparities,

rampant unprofessional conduct among officers, educational weakness, and poor hiring standards. Coupled with rising crime rates, the performance of law enforcement became a political issue in the 1960s (Seaskate, 1998, p. 2). President Lyndon B. Johnson "appointed the President's Commission on Law Enforcement and Administration of Justice to examine the problem" (Seaskate, 1998, p. 2). That commission's findings, released in 1967, indicated that many police departments could have been using the very same technology as much as 30 years prior, but for various reasons, had not done so. Most departments were still using 1940s technology, like radios, weapons, and out-dated operating procedures, in the late 1960's. The political and social pressures of that era would force the federal government to react and resulted in the creation of the Law Enforcement Assistance Administration (LEAA) (Northrop, 1995, p. 259).

That agency's primary goal was to provide "grants to government agencies, educational institutions, and private organizations to improve law enforcement" (National Archives and Records Administration, 2000). Especial attention was given to increasing the overall technical sophistication of American police departments. Funds were made available to agencies for the procurement of all types of technology: including crime labs, computer hardware, and computer software (Seaskate, 1998, p. 34). In this regard the LEAA was quite successful. Countless police departments were able to acquire new equipment, particularly computer hardware & software, at little or no cost to the parent department. As Kraemer, King, and Northrop note, the "LEAA contributed nearly $50 million to state and local government criminal justice and law enforcement agencies to fight crime. This funding was overmatched by other federal agencies such as the Federal Bureau of Investigation (FBI) and the states and local governments themselves"

(Northrop, et al, 1995, p. 259). Unfortunately, as often happens in any industry where large infusions of cash lead to technology buying sprees, most of this expensive equipment was either under-utilized, or simply sat in original shipping containers. As G. Thomas Steele recalls, "A lot of computers were bought with LEAA money. Many were still in their packing crates, not even installed, when I saw them" (Seaskate, 1998, p. 34). These failings were caused by a combination of factors, the two largest being lack of funds for adequate training and a fundamental lack of understanding as to the intracies of information technology deployments. The former remains an issue today and is just as unforgivable now as it was then (Seaskate, 1998, p. 4). The latter, as perceived by the researcher, was simply a byproduct of the "newness" of information technology at that time in history.

This state of affairs continued well into the 1980s, at least on the local level. At the federal level, however, the FBI had been moving forward with the National Crime Information Center (NCIC) since the late 1960's. Embracing technology in the fight against crime had long been a motto for the FBI, and NCIC was to become the crowning achievement of that philosophy, at least with regard to information technology. By 1967, NCIC was recording annual transactions, meaning requests for data by dispatchers, in the millions and had become an unequivocal success (The Investigator, 2000). The growing success of NCIC would have another, perhaps unexpected, dramatic affect on the use of information technology in law enforcement – local law enforcement now had access, though limited, to a nation-wide database of criminal records (also limited in size and scope), and those opportunities would fuel more changes in how patrol officers operated in the field.

Within two decades of the arrival of the FBI's NCIC system, it had become a fairly standard procedure for patrol officers, upon pulling over a suspect vehicle, to perform a routine lookup against NCIC records (Northrop et al., 1995, p. 262). Through the 1970's and into the 1980's, this task was accomplished via a radio dispatcher operating a remote terminal at a centralized police location. Functionally, the process involved having a patrol officer identify a suspect vehicle and note the relevant identification information of the driver and/or the vehicle. The officer would then radio in this data to the aforementioned dispatcher. Often the officer's requests would have to wait in a queue until the dispatcher had available time to process his specific request. This process could take up to several minutes. The cumulative delays made this a tedious process that begged for improvement.

The impact of the system's inefficiencies becomes more telling as the Community Era of policing is examined. Wrobleski and Hess (1993) describe this era, starting in 1980, as that time when "many police departments are beginning to become "customer-oriented" " (pp. 50-51). Police departments became more like businesses in that they were far more concerned with the needs of community members, referring to the general public that they served and not just the criminal element usually associated with police work, than they had been in the past and were willing to change to meet those needs. This attitude began to foster an open atmosphere that quickly resulted in new procedures and technical needs for patrol officers. Even as community policing grew beyond mere buzzword status and police departments across the United States started reshaping their operational mentalities to encompass this 'new' approach, improvements in information technology were imparting greater power into the hands of the average officer.

1980 Police departments begin implementing "enhanced" 911, which allows dispatchers to see on their computer screens the addresses and telephone numbers from which the 911 emergency calls originated.	1993 More than 90 percent of U.S. police departments serving a population of 50,000 or more are using computers. Many of them are using them for such relatively sophisticated applications as criminal investigations, budgeting, dispatch, and manpower allocation.
1990sDepartments in New York, Chicago, and elsewhere increasingly use sophisticated computer programs to map and analyze crime patterns.	1996 The National Academy of Sciences announces that there is no longer any reason to question the reliability of DNA evidence.

Table 3: Technology Adoptions in the Community Era (Derived from Seaskate's "Police Technology Timeline", 1998, pp. 23-24)

The introduction of Mobile Data Terminals (MDTs) to patrol cars marked one such improvement in this arena. Those officers fortunate enough to work in a department that embraced this technology in the early 1980s, such as the officers in the San Antonio PD, were now able to access NCIC records directly from their patrol cars, bypassing dispatchers and waiting queues (SAPD, 2000). Though primitive by today's technical standards, these devices gave equipped officers the ability to acquire the information that they needed more quickly. These devices led to the eventual adoption of notebook computers in the 1990s. Wireless data networks, like Cellular Digital Packet Data (CDPD) and ARDIS, sprang up in that decade, and competing protocols would battle back and forth in the police market. As processor speeds increased and mobile computers became smaller, notebook computers became a more common sight in police departments across the United States, replacing traditional MDTs in patrol cars. As laptops became more prevalent, vendors and politicians alike would argue that notebook computers were having a positive affect on the fight against crime, and that officers were benefiting from their use.

Is this true, though? Northrop, Kraemer, and King's 1995 study, "*Police Use of Computers*", would tend to agree with that generalization (p. 262). To be more accurate, though, the focus of their study was more towards the training of officers in the use of computers and less on perceptions of efficiency, arrest rates, and safety as a direct use of information technology by officers on patrol. In the course of their research, they did note that certain statistical increases in arrests and warrant searches had occurred in the period between 1976 and 1988 as a result of patrol officer lookups. Their research, however, also included dispatch-aided information gathering and did not distinguish between MDT and dispatch usage. Nor did it distinguish between the types of MDTs (notebook-based versus traditional MDT). In the following study, it is the progression from MDTs to notebooks that is of the greatest interest. The researcher's hypothesis is that patrol officers, as a result of using wireless data technology, will perceive an increase in arrest rates, overall efficiency, and "safety".

Initial Research Design

The initial design of this study was to attempt to answer these questions by gathering and analyzing pertinent data from selected police departments. That selection process was to include identifying police departments using specific technologies and having certain departmental characteristics (see Table 4). Once identified, those departments would be contacted directly with a request for available data, preferably in raw format, as to officer efficiency, arrest rates, and safety reports.[4] This data would be broken down into Pre-adoption and Post-adoption categories. Those categories would

[4] Both prior to and immediately following technology adoption.

then be statistically analyzed for patterns and trends. Appropriate conclusions would be drawn from that analysis and be published accordingly.

Technological Specifications

- CDPD network topology
- Notebook computers using wireless CDPD modems
- Directly access criminal justice databases such as NCIC from a properly outfitted patrol vehicle.

Departmental Characteristics

- State police agency, sheriff's department, or local (metropolitan) police department.[5]
- Various technological components for a period of time exceeding one year.
- Technologies deployed beyond any 'pilot' projects (prior to that 12-month period).[6]

[Note that not all departments contacted met all criteria.]

Table 4: Technological and Departmental Selection Criteria

Using the factors from Table 4, various police departments were identified as likely candidates and contacted for available data. The list[7] is as follows:

- A state police department
- A regional sheriff's department
- A metropolitan police department
- A federally-sponsored police department
- A federal agency's uniformed police department
- Wilmington Police Department (Delaware)

This portion of the research effort produced results that resulted in difficulties that were not entirely unexpected, but were nonetheless undesirable.

---

[5] The nature of this study, with its core examination of patrol-oriented law enforcement, obviates examining federal agencies like the DEA and FBI.

[6] Like many organizations, police departments often use small pilot projects to test new technologies.

[7] As per faculty recommendation, the names of those organizations contacted, but who did not participate in this study have been concealed.

This researcher's first candidate, the regional sheriff's department, did, at the deputy-level, express an interest in assisting with this study and were quite helpful in the initial stages of the research. Unfortunately, when events began to require top-level approval from that county's sheriff, all interactions with that department ceased, and further contact attempts were ignored.[8] The second candidate department, a state police force, was also initially very open to discussions, and a first meeting provided a substantive amount of information about the use of mobile technology in that agency. At the conclusion of that meeting[9], however, this researcher was informed that he would not be able to access any raw data from that agency. Their representative expressed concern that other recently adopted programs might adversely affect the outcome of any analysis of what little data that they possessed, and similarly, that they did not keep accurate records of the nature required in the original study design. Follow-up contact attempts, made when the study design was modified to its current form, went unanswered as well.

After the failure with that state police force, this researcher posted to the National Institute of Justice's technology website, "JustNet", (at http://www.nlectc.org) in public forums dedicated to law enforcement technology, known to be frequented by law enforcement officers.[10] At the same time, an opportunity to meet with the primary communication/technology officer in the Wilmington Police Department arose and was taken on December 20, 2001. This meeting with Master Sergeant John S. Martin produced a considerable amount of data and affirmed his department's willingness to assist in this research effort. He provided a number of technical details about their

---

[8] Contact methods included phone calls/voicemail and email messages.
[9] This meeting occurred on 10 Oct 00 and lasted approximately 2.5 hours.
[10] Ironically this attempt resulted in contacts from officers asking for information from this researcher and not the other way around.

technical configurations (current as of that date), including data on how and why certain purchasing decisions were made. Additionally, he went on to confirm this researcher's experience that many departments are not properly (or not at all) tracking certain data associated with their new technologies. Accordingly, he admitted that his department would not able to provide any raw data with regard to the original study design concept. He did, though, express that his department might be willing to undergo a study survey oriented towards patrol officers and their use of mobile technology.

Upon consultation with thesis committee faculty members, a modified design approach was agreed upon. From that point on, the design model was to generate a survey instrument for delivery to patrol officers actively using the technology under study. Additional decisions made by Committee Chair Stephen Jacobs were to allow the participating police departments the opportunity to review the finished thesis prior to publication and to allow them the option to have the document 'classified'.[11] A survey instrument specific to the Wilmington PD was generated and provided for committee review & advisement in January 2001. In February 2001 it was given to WPD for final approval upon review, and the actual delivery took place in March 2001. The delivery process will be outlined later in this document.

While this process was being undertaken, the original state police force was approached a second time for inclusion in this survey process. Again, email and voicemail were left unanswered. Simultaneously, two separate federal police forces were approached and given organization-specific survey instruments for examination, but declined to participate. Contact attempts with a third uniformed federal police agency

[11] Essentially this option provides for any participating department to require that personnel and/or organizations have their written permission prior to any access of the completed document.

were also unsuccessful.[12] By June 2001, it was apparent that other departments were not willing to be included in this study, at least not at this stage, and thesis completion requirements/timetables restricted this researcher's ability to continue searching for willing participants. As a result, a decision was made to move forward with the available data from the Wilmington Police Department and to begin final analysis of the available data.[13]

Technology Assessment

Cellular Digital Packet Data (CDPD)

Though other network topologies have vied for the law enforcement/emergency services market, most noticeably ARDIS and RAM/Mobitex, Cellular Digital Packet Data (CDPD) appears to have emerged as the primary wireless data network of choice for most American law enforcement agencies. A casual search of the Internet for "police & CDPD" will literally find thousands of references to police departments converting to CDPD networks. At the time that this study was initiated in 1999, that number was far less. Delaware adopted CDPD in a statewide initiative as its public safety data network in 1998 (Wartell, 2001, p. 1).

CDPD was designed to be an industry standard for digital data communications, developed by a consortium consisting of six (out of seven) Regional Bell Operating Companies (RBOCs), IBM, and other telecommunication companies (Dayem, 1997, p. 47). In essence, the CDPD wireless network operates within the confines of existing cellular networks alongside ordinary cell phones. The data technology functions inside

---

[12] And this despite having a 'friendly ear' connected to each of those departments. As concluded later, having a direct contact in a police department can often open formerly 'sealed' doors.

[13] The weakness that this presents toward the overall study is reviewed in the "Project Weakness" section of this document.

of that infrastructure through the same radio frequencies (Wireless Forum, 1998, radiotec.html). Diagram 1.0, as seen below, represents the basic concept:

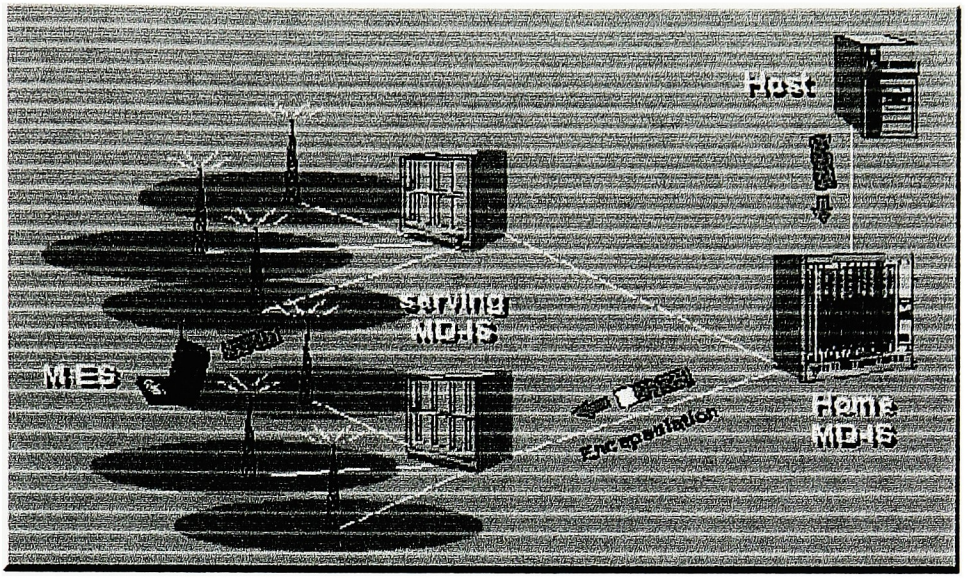


Figure 1: CDPD Basic Network Design (Sochan and Chen, tpdmobile.html)

The wireless notebook represents the mobile worker, in this case a sheriff's deputy, and the wireless data signal is sent to the nearest cellular tower. At the tower, the signal is processed by the Mobile Data Base Station (MDBS) and transmitted via digital landline to the Mobile Data Intermediate Systems (MDIS) (Dayem, 1997, pp. 97-100). This component, simply put, provides the functionality upon which the mobile user communicates with the relevant end-user services. In this example, the sheriff's deputy is directly interacting with a state-run server that process NCIC checks. Naturally the process is far more complex than described here, but this level of complexity is sufficient for the purposes of this study.

With the ongoing growth of the cellular infrastructure in North America, coverage for CDPD continues to expand rapidly. Installing a CDPD-based wireless network would only necessitate the addition of mobile base stations to existing cellular phone towers

(Wireless Forum, 1998, netreuse.html). Otherwise, the physical infrastructure of the network is not changed. Estimated cellular usage is around 55 million users in the United States, and that adds up to a lot of cellular towers (Parker, 1998, p. 106). That existing physical infrastructure allows cash-strapped police departments to make the most of their capital funds while gaining a capable wireless data network that meets their geographic requirements.

From a software perspective, CDPD is similar to RAM/Mobitex in its design. CDPD is a digital technology that relies on data packets sent in short bursts. CDPD uses forward error correction to minimize data transmissions and re-transmissions (Wireless Forum, 1998, mobiledn.html). As the packets are sent, they are encoded with error correction bits that allow the receiving equipment to use sophisticated decoding algorithms to recover lost data without asking for fresh transmissions (Wireless Forum, 1998, fec.html). This process of data recovery at the handheld unit level greatly increases the efficiency of the network while simultaneously minimizing the costs of use by decreasing the packets sent. Another example of the efficiency of the CDPD network is that multiple units can use the same radio channel. This is accomplished in the same fashion as local area Ethernet networks: when a device doesn't need to "speak", it is silent. If it has something to "say" (transmit a file or message, for example), then the mobile unit will accordingly transmit its data.

In fact, CDPD uses an open specification that allows it to interface with the Internet Protocol standard so that applications and mobile units have the greatest versatility with other network protocols (Dayem, 1997, p. 99). Specifically, by supporting the Transmission Control Protocol/Internet Protocol (TCP/IP), CDPD allows

for the use of the most common Internet Protocols; such as Simple Mail Transfer Protocol, Telnet, File Transfer Protocol, and Hypertext Transfer Protocol. This means that the mobile units in the field are able to use the same operating systems that can be found in offices and at police departments. Having the same operating systems on both mobile and stationary units can cut down on training costs and minimize user difficulties in the field. Similarly, as the operating systems evolve on the desktops, the mobile units running CDPD can be easily upgraded to the newer operating systems with a minimum of software changes. Such units can also access the Internet without the addition of custom software applications: software that usually comes with a hefty price tag.

Of course, using mobile computers with Internet capabilities requires that police departments make architectural decisions with their data networks to preclude officers from indulging in unacceptable behaviors (surfing inappropriate websites, playing network computer games, reading personal email, etc). The Wilmington Police Department is an example of an agency that has taken such steps. Master Sergeant Martin described his department's procedures to reduce these unacceptable behaviors, which include removing media bays (floppy drives and CD-ROM drives) from field units.

Table 5: Disadvantages of using CDPD

Speed • Provides raw data rate at the speed of 19.2 kbps. May not be sufficient for transmission of digital images (in a timely fashion)
Coverage • Limited coverage inside certain types of structures and rural areas.

One area of contention in the advancement of CDPD has been in the arena of information security. CDPD does use a built-in security system design that involves three components: Airlink encryption, authentication, and authorization (Dayem, 1997, p. 100). However, components within that design have been criticized due to the possibility of exploitation attacks against the encryption scheme used in the protocol. Yair Frankel, a noted researcher in the field of cryptography, and associates are among the critics of CDPD's security model. They have often been cited with regard to the faults of CDPD data security, particularly the opportunity for "man in the middle" attacks. Their work, *Security Issues in a CDPD Wireless Network*, describes this fault in detail and their recommended replacement protocol (Frankel, et al, 1995). In particular, their concern is with the Diffie-Hellman key exchange between the Mobile End User and the Mobile Serving Function.

The counter-argument to this concern is described here, in the words of some CDPD's founders:

> *The specification team recognized that such authentication credentials have a finite lifetime. If a mobile unit's authentication credentials were static over time, the secret could be copied and used to mimic the valid unit. To prevent this, the CDPD specification team defined the ability for the CDPD network to either periodically or at the service provider's discretion, update a mobile unit's authentication credentials. In this way, any particular authentication credential only has value during the period of time deemed useful by the network operator. (Taylor et al., 1996, node98.html)*

Taylor et al. (1996) were well aware of the intended uses of their protocol and attempted to provide a functional 'real world' solution to the task of wireless data communications.[14] To their credit, CDPD has stood the test of time and is widely utilized across North America, without any significant *acknowledged* penetrations of those existing networks.

Speed

- Provides raw data rate at the speed of 19.2 kbps
- Connectionless and instant network access

Protocols

- Open-standard network based on Internet Protocol (IP) and OSI Connectionless Network Protocol (CLNP)
- Compatible with existing TCP/IP and UDP/IP applications
- Standards-based design allows for competitive bids in software and hardware purchases, thereby reducing some costs in acquisitions (and/or upgrades)

Reliability and Security

- User authentication
- Less chance of data error (compared to voice transmissions)
- Air-link encryption to prevent eavesdropping

Availability

- Uses existing cellular networks
- Provides wireless Internet access

Cost Effectiveness

- Transmits data in small packets
- Fully digital, low error rates, higher speed (19.2 Kbps)
- Lower cost than analog wireless connections
- Connection-based system

Table 6: Benefits of using CDPD

[14] Naturally both issues can be examined for greater technical detail, but this examination is at a sufficient technical level for the purposes of this study. Readers interested in a deeper analysis of either issue are directed to read the aforementioned cites.

Wilmington Police Department & Wireless Data Technology

Law enforcement has certainly demonstrated its willingness to adopt this network topology over other offerings. The State of Delaware and its various police departments have been among the many American law enforcement agencies in the last decade to migrate towards wireless data communications. The Wilmington Police Department (WPD), one of Delaware's 43 law enforcement agencies, has been using CDPD-enabled notebook computers since approximately mid-1999 (Martin, 2000).[15] WPD is authorized to field 289 sworn officers, but presently only has 280 officers on the force. The force has 56 marked cars in used daily.[16] Of that 280, roughly 160 are designated as *Patrol Officer* and perform the duties associated with that status. These officers patrol a metropolitan area of approximately 73,000 residents. At the same time, Wilmington is also known as the "corporate capital of the world". As a result, downtown Wilmington is a hub of business activities with a large number of daily commuters coming in and out of the city environs.

Through the benefit of state grants, WPD was able to purchase, install, and operate Panasonic Toughbooks. The organization is capable of fielding 80 mobile units, but is only fielding 48 active units at present. The intended goal is to have 75 active units, with five available as 'hot standbys' (for maintenance purposes). The department uses a combination of models and operating systems, as detailed in Table 8. Their intention is to solidify to one operating system as time and resources allow. The individual units are 'assigned' to specific patrol units (as opposed to assigning them to

---

[15] Note that the following details are accurate as of 20 December 2000, the date of the initial interview with Master Sgt. John S. Martin. Some details may have changed during the writing of this study.

[16] Certain details about the operations and infrastructure of the Wilmington PD were considered too 'sensitive' for civilian disclosure.

individual officers), but are not hardwired to the patrol units. A docking station allows for relatively easy swapping of faulty units. During the course of the interview with Master Sergeant Martin, this researcher's attention was directed towards one such unit in his office awaiting repairs. He did not, however, have details regarding overall operational performance of the units from a maintenance perspective.[17] Lastly, the Input/Output components (floppy and CD-ROM drives) of each unit have been removed to prevent unauthorized tampering by officers. The department prefers to block access to sites like AOL and MSN, and removing the I/0 hardware from the units helps to limit such activity (but does not completely eliminate it).

Table 7 Wilmington Police Department Hardware and Operating System Details

Model (40 of each)	Operating System	CDPD Modem
CF-27 233MHz	Windows 95B	Spyder (internal)
CF-27 300MHz	Windows 98	Sierra SB300 (internal)

The actual CDPD network access is provided by Bell Atlantic, paid for through Delaware state contracts. This CDPD network covers the entirety of Delaware, with the expected areas of poor/non-existent connectivity. The department did consider purchasing a separate radio-based infrastructure, but the anticipated cost of such a dedicated system was too expensive. WPD has its own Internet Protocol (IP) Address block, also provided by Bell Atlantic. The specifics as to allotment of addresses to individual devices were not provided, for obvious reasons.[18]

---

[17] That issue is addressed in the survey section of this document.

[18] For those readers without an Information Security background, maintaining strong control of one's network design is a good step toward keeping that network more secure. It is always best to allow only 'trusted' personnel to have access to the organization's network topology map and IP map. Such details, once released to the public, only facilitate the attacks of computer criminals against that network.

The department uses four software applications as a matter of course. E-mail has a straightforward purpose, and is provided at the state level. Delaware state law requires that all law enforcement reports be of a standard format. A 3270 emulator allows for access to the Delaware Criminal Justice Information System (DELJIS). The third application used by WPD is the Enhanced Police Complaint system (EPC), a state-run central database critical to the Delaware Real-Time Crime Reporting System (RTCR) (Wartell, 2001, p. 3). This application allows officers to complete any report, short of accident reports. The final application, known simply as the Enforcer software, is for accessing National Crime Information Center (NCIC) databases. This direct access to state and federal databases is, as discussed previously, an integral driving factor behind providing patrol officers with wireless data communications. Has this access, though, had any discernable impact on the Wilmington patrol officer? Have they seen any increases in efficiency, arrest rates, or their own 'safety' while on patrol as a result of using this technology? The Wilmington Police Department's patrol officers have been given a survey designed to uncover the answers to those questions. It is this researcher's hypothesis that in all three cases the responding officers would have seen increases in their efficiency, arrest rates, and level of safety as a result of using this wireless data technology.

Methods

Population

The population examined consisted of Wilmington Police Department police officers. The only requirements for members of the force were that they be on active duty, assigned to patrol duty, and have had access to the technology in question as a

patrol officer. It was hoped that by following the sampling method listed below that these requirements would be properly met.

Sampling Method

The sampling method used with the WPD was non-random and consisted of two separate deliveries. The first delivery was to the Second Shift patrol group, and the second to the Third Shift patrol group. Both deliveries took place in the same 24-hour period and in the same fashion. In both circumstances, the survey tool was presented to the oncoming patrol shift during their pre-shift briefing, and completed survey forms were gathered prior to the end of those briefings.[19] This sampling method yielded 32 completed surveys.

Survey Design and Scale

An extensive search of prior related efforts was performed to provide this study with an applicable scale from any previous study. That search was conducted from and at various locations, including RIT's electronic databases (via the Wallace Memorial Library's online interface). Additionally, keyword searches of the World Wide Web, using phrases like *law enforcement, CDPD, police, results,* etc, were carried out with few results of an academic nature.[20] Nearly all of the material generated as a result of these searches was of a popular or business nature. The few exceptions, though not directly applicable to this survey design, are listed in the citation section of this document. As a result, the researcher was forced to build questions based on prior undergraduate work and direct experience in the field of Information Technology.

---

[19] The patrol shifts were those made available by Wilmington PD administration, hence the non-random sampling method. The other shift was not available.

[20] Note that these searches also included a variety of Boolean expressions to minimize straight-line logic errors.

The design of the survey instrument was straightforward and general in form. Of the thirty-one questions in the survey tool, six were demographic in nature. Those questions contained references to the respondent's sex, race, education, and age. The other two demographic questions, RANK and length of SERVICE as a Patrol Officer, were added. With the exception of AGE and RANK, the questions were prepared for analysis as interval-level data. RANK was modified during the data analysis phase and became interval-level data.[21] AGE was modified via the RECODE command found in SPSS. Twenty-one of the remaining questions were gathered as ordinal data and provide the primary focal points for the data to be acquired. The remaining four questions were broad in design and were included to allow the respondents to make general statements about the technology in their department.

Methods of Statistical Analysis

The types of statistical analysis available for use in this study were affected by the nature of the survey instrument, and each test was chosen with an eye to the maximum benefit possible from its use. Statistical analysis was conducted using SPSS, versions 10.1 and 11.[22] As seen in the Command File (Appendix D), the first statistical tool to be run against the QUES1 through QUES21 variables was the RELIABILITY command. This test is used to test the internal validity of the associated variables. All of the variables were then tested for frequency-related information via the FREQUENCIES command. Some variables were tested only for *mode*, while others were tested for all measurements of *frequency*, including *mean, median, etc.* The final statistical analysis

---

[21] "Patrolman" became a "1", "Corporal" became a "2", and so on, as the survey data was manually placed into the DAT file.

[22] Note that the *Command File* was created for use with SPSS running on a VAX/VMS cluster, but was utilized with the aforementioned Windows versions of SPSS.

performed against the acquired data was the *cross tabulation* of certain variables in specific sequences. The SPSS command used for this purpose was CROSSTABS. Each of these tests included options for *chisq* and *counts*.

Results

Reliability

As noted previously, the first statistical test performed was for *reliability*. The QUES1 through QUES21 variables have a *reliability ALPHA* of .7715 – the closer to 1.0 that the *reliability ALPHA* is, the more reliable the data is considered to be. In this case, with a score of .7715, the data gathered can be considered fairly reliable for the purposes of this study, considering the sample size. Table 8 displays the output from the RELIABILITY command.

Table 8: RELIABILITY Output for Ques1 - Ques21

RELIABILITY ANALYSIS - SCALE (ALL)	
Reliability Coefficients	
N of Cases = 27.0	N of Items = 21
Alpha = .7715	

Frequencies Variables

The second series of analyses involved the following variables: SEX, SERVICE, RACE, RANK, and EDUC. These variables, because of their *nominal* level of measurement, could only be tested for *mode*. As a result, this test only gives a measure of the most commonly occurring value in each variable. For SEX, the breakdown consisted of three female officers and twenty-nine male officers. SERVICE provided a somewhat expected response in that 78.1 percent of respondents had 1-5 years of service

in patrol duty. Similarly, the RACE variable had a fairly uniform spread of races, as seen in Table 9.

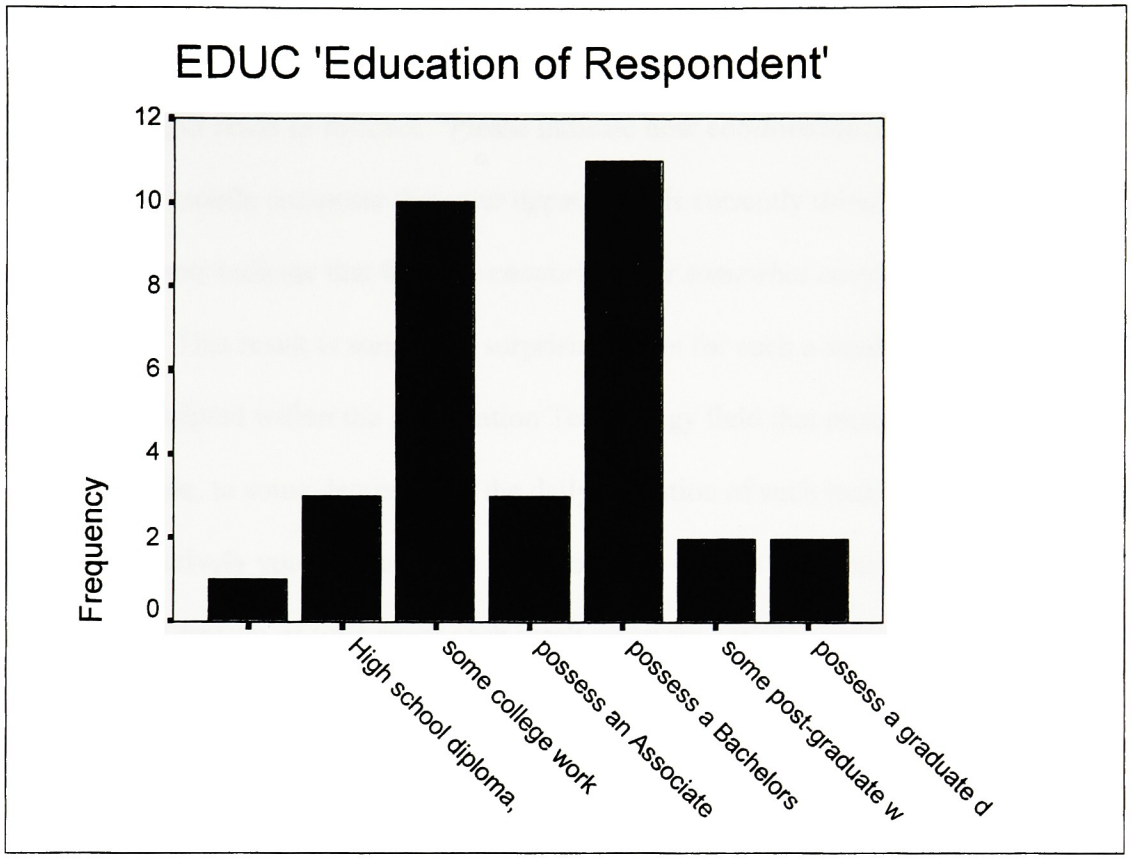
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Black	7	21.9	21.9	21.9
	Hispanic/Latino	2	6.3	6.3	28.1
	White	23	71.9	71.9	100.0
	Total	32	100.0	100.0	

Table 9: Race of Respondent

RANK displayed another expected return of 25 Patrolmen, 6 Corporals, and 1 Master Sergeant.[23] Of these five variables, EDUC proved the most interesting in its results. According to the data acquired, roughly 56.4 percent of respondents had either an Associates, Bachelors, or Masters degree (or some combination thereof), and another 31.3 percent indicated that they had some level of college work. As described previously in this document, the educational level of law enforcement officers had been a concern in the 1960 - 1980s. This appears to be less of an issue now, at least for the Wilmington Police Department. Follow-up studies should be able to more accurately answer this issue.

[23] A minor flaw in the survey instrument surfaced here. 'Patrolman' should have been less gender specific.

Table 10 Education of Respondent



The remaining variables, QUES1 through QUES21, were also processed for *frequency* statistical results. These variables were, of course, the main questions in the survey instrument, and it was expected that the data gleaned from these questions would either confirm or deny this researcher's hypothesis. The questions were broken down into the basic categories of comfort level (with regard to home, work, and mobile computer use), hours of use per week, MDT operational aspects, software type (ECP, DELJIS, and Enforcer – their impact with regard to the three research issues), and three final 'overall' questions (that focused solely on the overall research issues of efficiency,

arrest rates, and safety).[24] The results of that analysis were in many respects quite surprising. Those questions and their results are noted below.

QUES5 reads as follows: "Please indicate how comfortable or uncomfortable you are with the mobile computer that your department is currently using". 93.8 percent of the respondents indicate that they are *comfortable* or *somewhat comfortable* with the technology. This result is somewhat surprising, even for such a small sample size, as it is generally accepted within the Information Technology field that most *users* are uncomfortable, to some degree, with the daily operation of such technology. At the same time, the relatively young ages of the patrol officers may be influencing this question's results. The amount of time spent each week using the mobile computer may also be affecting that set of responses, as seen by the replies to QUES6. Seventeen of the 32 respondents indicated that they used the mobile computers between two to ten hours a week, and 13 respondents replied that they used the devices for more than ten hours a week. The patrol officers also seemed to feel that the mobile computers were fairly easy to operate, as seen in Table 11. Similarly, 93.7 percent of the officers found that the technology was either *easy to adapt to* or *not difficult to adapt to* (QUES9). The officers were, though, somewhat divided as to the reliability of the mobile computers; 34.4 percent answered that the units were not reliable (QUES7).[25]

---

[24] The survey instrument erroneously references DELJIS as DCJIS. Said instrument, in its entirety, is contained in Appendix A.

[25] This point was reiterated in the open-ended section of the survey instrument. Numerous officers took the time to mention the unreliability of the units when used in a certain section of the city of Wilmington.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid STRONGLY DISAGREE	1	3.1	3.1	3.1
DISAGREE	2	6.3	6.3	9.4
AGREE	25	78.1	78.1	87.5
STRONGLY AGREE	4	12.5	12.5	100.0
Total	32	100.0	100.0	

Table 11: QUES8 'MDT's ease of operation...'

Survey questions QUES10 through QUES18 focused on the three different types of software utilized by Wilmington Patrol Officers, and the data gathered from those questions is as follows:

- 83.8% of respondents *agreed* or *strongly agreed* that the Enhanced Police Complaint software made them more efficient (QUES10), while 87.1% said the same regarding the DCJIS (DELJIS) software (QUES16). These as compared to the 62.6% who responded that the Enforcer software had allowed them to be more efficient (QUES13).[26]
- 71.4% of respondents either *disagreed* or *strongly disagreed* with the statement that the EPC software had increased their arrest rates (QUES11). This result closely paralleled that of QUES14; 71.4% had that same feeling about the Enforcer software. The only difference was in intensity of *disagreement*. The differences were less obvious for the DCJIS (DELJIS) software. For this question, only 51.6% *disagreed* or *strongly disagreed* as to arrest rate increases while 48.4% *agreed* that using this software had increased their arrest rates.

[26] Note that the sample size was 31 responses for QUES10 and QUES16 versus 28 for QUES13.

- With regard to an increase in 'safety' as a result of using this technology, the responses for both EPC (QUES12) and Enforcer (QUES15) were roughly the same; approximately 70% *disagreed* or *strongly disagreed.* As with the previous section, the results for DCJIS (DELJIS) were much closer; 54.8% *disagreed* or *strongly disagreed* while 45.2% of respondents (thirty-one of thirty-two officers) *agreed* or *strongly agreed* that this software made them 'feel safer' while on duty (QUES18).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STRONGLY DISAGREE	1	3.1	3.4	3.4
	DISAGREE	17	53.1	58.6	62.1
	AGREE	9	28.1	31.0	93.1
	STRONGLY AGREE	2	6.3	6.9	100.0
	Total	29	90.6	100.0	
Missing	System	3	9.4		
Total		32	100.0		

Table 12: QUES21 'Overall, the adoption of MDT's has made you feel safer...'

When asked for overall impressions of the mobile technology in use in their department (as presented in QUES20 and QUES21), the officers' responses were somewhat divided. When presented with the statement, *"Overall, the adoption of the mobile computers in your department has increased your arrest rate"*, 18 officers *disagreed* while the remaining twelve did *agree*. When the same general question was asked about safety, the responses were even more divided, as Table 12 shows. There was little division among respondents with the statement, *"Overall the adoption of the mobile computers in your department has made you more efficient with your time while on the*

job". Only one of twenty-nine responding patrol officers did **not** feel more efficient. The significance of this statement will be addressed later in this document.

The complete set of *frequency* analyses results are in Appendix F.

Crosstabs

The third and final set of statistical analyses involved performing *cross tabulation* of variables. Specifically, the variables RACE, RANK, AGE, EDUC, SERVICE, and SEX were tested individually against the variables of QUES1 – QUES21. Additionally, *cross tabulation* testing was performed on an ad hoc basis as interesting and/or unexpected results occurred.[27] Overall, the breakdown of the independent variables against the dependent variables provided various revelations, particularly when compared against the results from the *frequency* analysis as described previously. The following items from the *cross tabulation* analysis are worthy of comment.

Unfortunately the sample set only contains three female officers, and one of those three officers did not answer the majority the dependent variable questions (QUES10 through QUES21) of primary interest, so the data gleaned from the variable SEX is too limited for any practical use within this study.

The RACE variable has a breakdown of seven Black officers, two Hispanic officers, and twenty-three White officers. An examination of this variable against QUES1 through QUES6 shows no significant differences between the different racial types except that the Black officers generally seem more comfortable with the technology. The same examination against QUES7 through QUES9 reveals a similar general result, with the exception of QUES8, *"the mobile data terminal (MDT) is easy to*

[27] As the results were being examined, the researcher noted interesting responses from a respondent with a graduate degree. While comparing those results, a CROSSTABS was run to determine that respondent's gender.

operate... " in which all seven Black respondents *agreed* that the units were easy to operate. For the survey questions QUES10 – QUES18, the responses provided tended to be more evenly distributed within the Black respondents than within the White respondents. When presented with the question of overall efficiency, as in QUES19, the races answered as seen in Table 13.

		DISAGREE	AGREE	STRONGLY AGREE	Total
Black	Count	1	4	2	7
	% within RACE 'Race of Respondent'	14.3%	57.1%	28.6%	100.0%
	% within QUES19 'Overall, the adoption of MDT's has made you more efficient...'	100.0%	17.4%	33.3%	23.3%
	% of Total	3.3%	13.3%	6.7%	23.3%
Hispanic /Latino	Count		1		1
	% within RACE 'Race of Respondent'		100.0%		100.0%
	% within QUES19 'Overall, the adoption of MDT's has made you more efficient...'		4.3%		3.3%
	% of Total		3.3%		3.3%
White	Count		18	4	22
	% within RACE 'Race of Respondent'		81.8%	18.2%	100.0%
	% within QUES19 'Overall, the adoption of MDT's has made you more efficient...'		78.3%	66.7%	73.3%
	% of Total		60.0%	13.3%	73.3%
Count		1	23	6	30
	% within RACE 'Race of Respondent'	3.3%	76.7%	20.0%	100.0%
	% within QUES19 'Overall, the adoption of MDT's has made you more efficient...'	100.0%	100.0%	100.0%	100.0%
	% of Total	3.3%	76.7%	20.0%	100.0%

Table 13: QUES19 'Overall, the adoption of MDT's has made you more efficient...'

The analysis of RANK and the QUES1 – QUES21 variables is also hampered by the relatively small sample size, so accurate statistical conclusions are limited. Keeping the study limitations in mind, a brief review of the survey answers for this variable does provide a few possibilities for future survey designs. More specifically, it is a generally

accepted fact within the Information Technology field that supervisors will have more difficulty with new technology.[28] In the case of this study, however, the study's sole Master Sergeant did not generally respond in such a fashion. He typically answered the survey questions on 'comfort' with a *somewhat comfortable* (QUES1 – QUES6). He did not find the mobile computer to be reliable, nor easy to adapt to, but he did indicate that the each type of software had increased his efficiency, but not his arrest rates or his feeling of 'safety'. When asked, however, about QUES20, *"Overall, the adoption of the mobile computers in your department has increased your arrest rate"*, he *agreed,* along with the five responding Corporals, that they had increased his arrest rate. Generally, the Master Sergeant's replies indicate the same type of positive and negative reaction to the technology as seen in the lower ranks.

AGE, much like the two preceding variables, has only a few significant items for consideration. The results acquired are fairly generally distributed, with the slight exception of the two oldest ranges, 33-37 years and 38-42 years. For most of the survey questions between QUES1 and QUES21, the respondents in these categories tended to cluster together. For example, their responses for QUES7 through QUES8 were generally parallels of each question. Two surprising items are to be found in their responses to QUES20 and QUES21. Four of six respondents in these two age ranges did not *agree* that the mobile computers had increased their arrest rates, while four of the respondents, ages 33-37, also did not 'feel safer' as a result of the adoption of the technology by their department. The sole 38-42 respondent did 'feel safer' (QUES21). Though by no means conclusive, these results do allow for some fascinating theorizing –

[28] This 'factoid' is often associated with the age of the user as well. At the time of this study's writing, the researcher was not aware of any formal studies to confirm or deny this commonly held belief.

theorizing which can only be answered by deeper/larger research efforts, of the same type as this study.

The variable EDUCATION, when processed by the CROSSTABS command, produces the following items of significance:

- Officers with Bachelors degrees are more likely to answer with a *disagree* or a *strongly disagree* when asked about being 'safer' (QUES12 and QUES15) as a result of using the Enforcer and EPC software packages. They are less likely to respond so decisively when the software package is DCJIS (DELJIS) (QUES18).
- Similarly, they respond in the same fashion when asked about arrest rates (QUES11 and QUES14) while using the Enforcer and EPC software packages, but are somewhat more evenly divided when the same question (QUES17) is posed with regard to DCJIS (DELJIS).
- While ten Bachelors degree holders did *agree* that the overall adoption of mobile computers had increased their efficiency (QUES19), the majority *did not agree* that that adoption had increased their arrest rates or their feelings of safety (QUES20 and QUES21).

The full results obtained from CROSSTABS analysis can be found in Appendix F.

Conclusions

Findings

The results obtained in this study are actually contrary to expectations. As stated previously, the researcher's hypothesis was that patrol officers, as a result of using wireless data technology, would perceive an increase in arrest rates, overall efficiency,

and safety. As borne out by the data, this hypothesis was only partially supported. The primary research questions of officer efficiency, arrest rates, and safety were posed with an expectation that the majority of the responding officers would have seen a positive increase in, or at least a change for the better, in each area. As has been seen, such was not the case for WPD patrol officers. The predominate response from these police officers, with the exceptions noted above, was uniformly that they **did not** believe that the wireless data technology had positively affected their ability to make arrests nor had it made them feel safer. Simply put, the officers did not see any significant positive changes in either area. At the same time, the officers strongly indicated that the technology implemented **had** increased their levels of efficiency. They were particularly vehement with regard to the DELJIS software. The fact that 87.1% of the officers polled responded, either by agreeing or strongly agreeing with the appropriate research questions, clearly indicates the importance of field access to NCIC databases to patrol officers. This study's findings should indicate to the department's administrators that the officers feel more efficient as a result of the use of wireless data technology.[29] It would appear that direct NCIC access from the field has indeed played some significant role for the Wilmington Police Department's patrol officers and their efficiency.

How much so still remains to be determined and is beyond the scope of this document. More specific/accurate answers to those questions will only be determined if certain technological steps are taken. Specifically, police departments, including WPD, have to begin tracking data such as efficiency reports and officer safety data. They must

---

[29] This study should also inform the department that problems exist within the Northern section of Wilmington, with regard to modem connection & reliability. This detail was noted in the open-ended questions of the survey instrument by four officers. Other officers commented that they would prefer to be issued their own MDT rather than sharing a unit with other officers.

also begin to accurately log arrest data in conjunction with mobile computer use. In order to gain the maximum value from technology, law enforcement has to work with technologists to incorporate these requirements into their existing solutions (and engineer them into new implementations). Departments must, as well, allow technologists access to the acquired data. As discussed earlier, the primary reason for the relatively small sample size of this study was the hesitancy of approached police departments, with the obvious exception of the Wilmington Police Department, to provide access to such data. It is true that misuse of acquired data could be detrimental to police departments, but proper training of technologists will mitigate against most, if not all, risks. Failure to accept any of these requirements will only force law enforcement to continue acquiring new technology in the expensive haphazard fashion it has used for decades. Fortunately, in the case of the Wilmington Police Department, it seem this is not the hazard it is for numerous other police departments.

Impact of Research

As the next section will clarify, the weaknesses of the study's design, scope, and acquired data do limit the effectiveness of this study, and hence its applicability on any large scale (in its current form as an introductory analysis of technology usage on a small scale). The overall impact of this study's research on the fields of Information Technology and Criminal Justice, due to its weaknesses, will in most respects be negligible. This study does have merit as it adds to the current body of knowledge in that it covers areas of both fields that have not been fully explored.[30] Those departments considering future/new implementations of wireless data technology could conceivably use this study as a guide in their own technology efforts. Many police departments are

[30] As determined by a search of current literature databases.

either not currently tracking, or are not capable of tracking, certain types of end-user data. Efficiency records, officer safety reports, and arrest rate changes are three types of data that would be of considerable assistance to technologists for use in gauging the relative 'success' of any law enforcement-oriented technology implementation (besides the data's more obvious benefits to law enforcement). The results found in this study could help both technologists and law enforcement agencies properly engineer solutions capable of easily tracking the types of end-user data that existing solutions apparently cannot.

Project Weaknesses

This study is critically flawed in a number of areas. The first is in the sampling method used. Within the Wilmington Police Department, a more accurate sampling method would have been to randomly select patrol officers from a complete roster and deliver the survey instrument to those officers. This method would have provided a potentially higher number of returns, thereby enhancing the accuracy of the statistical analysis. It would have also allowed for greater diversity in the population analyzed.

Second, more than one police department should have been included in the data gathering process.[31] It must be noted, however, that constraints within the police department selection process limited options in this regard. As described in previous sections, all but one department refused to provide data, or be part of any survey process. This fact, along with certain time constraints, forced the researcher to use the single available police resource to its best effect. Regardless of the contributing factors, the relatively small scale prevents the study from being more widely applicable in the field of law enforcement.

---

[31] Alternately, a larger police force, such as the Philadelphia police department, should have been surveyed. Using the statistical methods detailed above and below on a department with over a thousand officers would have provided a greater amount of research data from which to draw appropriate conclusions.

Lastly, the questions in the survey instrument could have been of a superior design. For example, the questions could have been less gender-specific. The lack of similar studies to compare/base this study against also worked against the survey design. As a result, Likert scale questions could not be used. An option should have been in place, where appropriate for question material, to allow the respondent to select 'non-applicable'. Another choice should have been to allow respondents to indicate when the technology actually created decreases in tested areas. An unexpected assumption was that the technology would only be of a positive nature and not negative. The survey instrument should have also been designed for quantitative analysis, rather than qualitative analysis. This design alteration would presumably provide a deeper data pool, thereby allowing for deeper statistical analysis; researchers would then be able to make more measurable determinations as to the effect of technology on the field of law enforcement. Future surveys of this nature should bear these flaws in mind and plan accordingly in their own designs.

Appendix B holds a revised survey instrument that bears questions created out of these lessons, and would presumably acquire data with greater value to both Information Technology and Criminal Justice.

Discussion

The area of convergence between the field of Criminal Justice and Information Technology is relatively new. As a result, few technologists have emerged to direct research efforts in this area. The final section of this document will describe three suggested research areas for technologists' future efforts. Those areas are direct outpourings of this study's efforts, and conducting that research will require specific

knowledge and skills. These are the same skills and knowledge that this author has been developing through his Masters work. This section will briefly detail how the coursework pursued by the author can be applied to those future research efforts (and peripherally how they applied to the current research effort).

The Masters of Science in Information Technology (MSIT) requires certain core courses and two concentrations for each graduate student.[32] The core courses are "Information Integration", "Fundamentals of Telecommunications", and "Theories of Interactive Computing". Though other concentrations can be selected, this researcher's Masters concentrations are in Telecommunications Management and Telecommunications Technology. Courses taken by the author include "Network Management", "Telecommunication Policy and Standards", "Current Themes in Technology", "Enabling Technology & Trends in Telecommunications", "Network technology", "Transmission Systems", "Distributed Systems", "Software Testing", "Economics of Software Development", and "Software Project Management".

In-depth as they may be, these courses can, for the purposes of this discussion, be broken down into the general categories of networking, technology analysis, and software development. Each course topic has contributed positively in the current research effort in one or more fashions and should apply equally well in future research efforts. The networking courses have provided the author with the knowledge needed to understand existing networks (ATM, Frame Relay, and Ethernet) as well as the ability to branch out into wireless networking. This was of particular interest to the researcher as police data networks are understandably wireless-based. The course "Transmission Systems" gave the researcher an opportunity to examine CDPD networking in the classroom

[32] Accurate as of 1997.

environment and to then take the knowledge gained out into the field. This researcher is now familiar with the critical factors of wireless data networks (signal strength, wave dispersion, and interference issues, for instance) and also the tools to measure same. Similarly, those studies, combined with the lessons learned from this study, will enable the researcher to more accurately conduct future technology research on law enforcement networks.

An example of such would be in how to address the reliability issue with the Wilmington Police Department. The researcher can now create processes by which to map out the patrol regions of WPD, test the available notebooks for signal strength against those maps, and produce results depicting reliability patterns. Those results can then be used to rectify existing reliability patterns (by identifying areas needing more cellular coverage) and to test new hardware against an existing baseline. The former directly impacts on current operational issues, and the latter addresses, to a degree, some of the usual issues associated with technological upgrades. Having an existing baseline against which to measure new technology allows a department to more accurately gauge the worthiness of a new system against the cost of installing it. If new hardware doesn't improve the performance and/or reliability of a system, why spend tax dollars on the upgrade?

The other areas of technology analysis and software development have similarly played important roles in this researcher's thesis effort.[33] "Current Themes in Technology" and "Distributed Systems" are two courses in the MSIT program that allowed the author to interpret the interactions, both material and theoretical, of the

[33] Though the software development courses will have a greater impact on future research efforts than when compared against the current research effort.

wireless notebooks and the law enforcement databases. It is highly relevant to be able to abstractly model how an end user is accessing, retrieving, and altering data across a network.[34] Understanding processes of this nature is the first step toward being able to interpret how such processes are actually performing in the field. The concept is not limited solely to data manipulation, but also applies to the interactions between humans and computers. As noted previously by this author, HCI factors may have played a significant role in how the patrol officers responded to the survey questions. The depth of that impact bears consideration in new research. Fortunately, "Theories of Interactive Computing" is a core MSIT course focusing on the topic of HCI and should serve as a valuable resource in future research projects (by this author).

Technology, if history is any valid indicator, will only continue to advance and change form. For patrol officers, technology will *probably* continue to shift towards a greater reliance on wireless data communications while in the field. It is entirely possible to envision a day when patrol officers are using some form of wireless handheld device to perform their NCIC and state law enforcement database checks as they speak to suspects (rather than sitting in a car typing at a notebook). Good HCI design would include an icon on each screen that the officer can easily select in situations where she needs immediate backup.[35] For example, the officer might have seen a weapon or illegal material in the vehicle without the suspects realizing that the officer had seen the items. Without alerting the suspects by calling for backup, the officer could simply 'hit a button' on the handheld, as if entering normal data, and the unit would broadcast the 'immediate backup' signal to other patrol cars and/or other handheld devices in the patrol area. The

[34] Regardless of the network topology in question
[35] Without making it so 'easy' that the end user inadvertently selects this option by mistake during normal workflow.

suspects have no reason to panic or react violently even as other officers arrive on-scene to aid in the arrest. A relatively simple concept involving nothing more complex than an alerting subroutine, but this researcher has yet to see the principle described in any other forum or in use in the field.

Areas of Future Research

During the course of this research study the researcher noted three items for consideration in future research efforts. The first is with regard to the officers' responses to the 'comfort' questions in the survey instrument. A sizable 93.7% stated that the mobile computers were easy to adapt to (upon the introduction of the new technology). Similarly, a majority also felt that the operation of the technology was not difficult. These two issues are often seen as barriers in technology rollouts, but neither seems to have had a serious impact on the WPD. It is a widely held, yet un-codified, belief in the field of Information Technology that older end-users often have the most difficulty adapting to new technology or to changes in existing technology. Yet the data gained in this study alludes to the conclusion that factors like age and rank do not necessarily affect how officers react to the technology. If further research bears out these facts, those widely held beliefs may have to be re-examined more deeply across different industries. From a technologist's perspective these observations alone are worthy of more research and analysis.

The second item noted for future research consideration is a result of officer input from the open-ended questions in the latter section of the survey instrument and hand-written notes in the margins of the main question section. The officers remarked that they would have a greater level of satisfaction from the technology if only it were more

reliable. Those comments were directed specifically towards network reliability in the Northern section of Wilmington and towards the notebook modem. Unfortunately, exact descriptions of the reliability issues were not provided by those respondents, limiting the opportunity to draw more direct conclusions in this study. The fact, though, that some respondents took the opportunity to write out the issue by hand indicates that it has had some impact on their interaction with the technology, thereby affecting their responses to the primary research questions of officer efficiency, safety, and arrest rates. If Information Technology is to provide its maximum benefit to the field of law enforcement, it must be able to identify, isolate, and eliminate unreliable software and hardware from field use. Accordingly, future research should be conducted to accomplish these tasks.

The final future research item identified by the researcher is the possibility of human-computer interaction (HCI) on the officers' perceptions with regard to the technology and the research questions.[36] At least one officer noted that the software used by the department provided too much detail, and another remarked that the software interface was not intuitive enough for prompt usage. Both of these comments cast a light on how HCI is or is not being considered in the development of computer software and hardware in the law enforcement field specifically and criminal justice in general. It is entirely reasonable to assert that computer systems designed from the 'ground up' for patrol officers, with HCI factors firmly applied in the development and engineering processes, would dramatically affect how officers react to the research questions of efficiency, arrest rates, and safety. Advanced voice recognition, and intuitive touch-pad

[36] A relatively new field in Information Technology, HCI focuses on how humans interact with computers and methods for improving interactions for both humans and computers.

display screens are two such emerging technologies, which if introduced properly into field applications, could have substantial positive impacts in these areas. The original concept of windshield-based heads-up screens could also dramatically affect these research topics. This researcher strongly suggests that future research efforts be directed to examining the proper use of HCI in law enforcement technology.

This convergence between the fields of Information Technology and Criminal Justice is uncharted territory and therefore has many issues that will provide fodder for future researchers. The areas suggested above are only the tip of the iceberg for what should be a most productive union. The union, though, first needs to be joined by both parties.

References

Armstrong, T. & Dixon, D. (1999). Rugged mobile computers help evacuate those in Georges' path. The Police Chief, vol. 66 18-22.

Babin, L. (1996). Police Use of the Internet. Ottawa, Ontario: Royal Canadian Mounted Police.

Brule, Paul (1997). Oral Lecture in Senior Seminar courses. Rochester Institute of Technology, Rochester NY.

Capitol Connections (2000). CIO Award. Available at http://www.das.state.ut.us/cc/november/cioaward.html. Last seen on 27 Dec 00.

Dayem, Rifatt A. (1997). Mobile Data & Wireless LAN Technologies. Upper Saddle River, NJ: Prentice Hall PTR.

Frankel, Y., Herzberg, A., Karger, P.A., Krawczyk, H., Kunzinger, C.A., and Yung, M.(1995). Security issues in a CDPD wireless network. IEEE Personal Communications. Volume 2, Number 4, August 1995. pp. 16-27

Fitzgerald, J. D. & Cox, S. M. (1994). Research Methods in Criminal Justice: An Introduction. Chicago, IL: Nelson-Hall, Inc.

Hagan, F. E. (1993). Research Methods in Criminal Justice and Criminology, Third Edition. Toronto, Canada: Maxwell Macmillian Canada, Inc.

Hedgepeth, K. (1999). A Cutting-edge Mobile Communications Solution. The Police Chief, vol. 66 23-24.

Joseph, A. D. (2000). Privacy and Security in Wireless Networks (Part II). Available at: www.cs.berkeley.edu/~adj/cs294-1.f00/L9.pdf. Last seen 10 Feb 02.

Johnson, H.A. (1988). History of Criminal Justice. Anderson Publishing Co. [no address in text]

Keenan, M. L. (1999). PDA's solve the crime. Communications News, vol 36, issue 1 46-49.

Law Enforcement Technology for the 21st Century: Conference Report. May 15 - 17, 1995 http://www.nlectc.org/pdffiles/confrep.pdf : last seen on 1 Jan 01.

Marshall, K. B. (1998). Mobile data access increases officer efficiency. FBI Law Enforcement Bulletin, vol. 67, issue 6. 6-9.

Martin, J. S. (Master Sgt., Wilmington Police Department). Oral interview on 20 December 2000.

McQuade, S. (2001). "The Co-evolution and Complexity of Information Technologies and Money Laundering". GMU

Meyers, J. (1997). Walking the data beat. Telephony, vol 232, issue 20. 34.

Muller, N. J. (1998). Desktop Encyclopedia of Telecommunications. New York, NY: McGraw-Hill.

National Archives and Records Administration (2000). "Records of the Law Enforcement Assistance Administration [LEAA]". Available at http://merrimack.nara.gov/guide/rg423.html#423.2. Last seen 29 Dec 00.

Newton, H. (1998). Newton's Telecom Dictionary: The Official Dictionary of Telecommunications. New York, NY: Flatiron Publishing.

Northrop A., Kraemer, K. L., & King, J. L. (1995). Police Use of Computers. Journal of Criminal Justice, Vol. 23, No. 3, 259-275.

Norusis, M. J. (1990). The SPSS Guide to Data Analysis for Release 4. Chicago, IL: SPSS, Inc.

Pauley, J. L. (1998). Meeting today's law enforcement challenges with technology. The Police Chief, vol 65, issue 10. 12.

Pursley, R. D. (1994). Introduction to Criminal Justice, Sixth Edition. New York, NY: Macmillian Publishing Company.

Rich, T. E. (1995). The Use of Computerized Mapping in Crime Control and Prevention Programs. Washington, D.C.: U.S. Dept. of Justice, National Institute of Justice.

SAPD (2000). SAPD Communications Unit (website). Available at http://www.ci.sat.tx.us/sapd/communications.asp?res=1400&ver=true. Last seen on 5 Jan 02.

Seaskate, Inc. (1998). The Evolution and Development of Police Technology. Available at http://www.nlectc.org/. Last seen on 27 Oct 00.

Sochan, J.T. and Chen, H. PhD. Tucson Police Department COPLINK Mobile Computing Technology Assessment. Available at http://ai.bpa.arizona.edu/go/datawarehousing/publications/tpdmobile/tpdmobile.html. Last seen on 24 Mar 02.

Taylor, M., Waung, W., & Banan, M (1996). Internetwork Mobility: The CDPD Approach. Pearson Education, Inc. Available at: http://www.leapforum.org/published/internetworkMobility/index.html. Last seen 10 Feb 02.

The Investigator (2000). National Crime Information Center: 30 Years on the Beat. December 1996 - January 1997 Issue. Available at http://permanent.access.gpo.gov/lps3213/ncicinv.htm. Last seen on 2 Jan 02

Wartell, Julie (2001). Delaware Real-time Crime Reporting System. Available at: www.delawarepublicsafety.com/newsevents/RTCRDetailedInformation.pdf. Last seen Feb 10, 2002.

Wilson, C. R. (1997). Gang Monikers: The gathering of moniker information can provide law enforcement with a strong investigative edge over increasingly mobile and savvy gang members. FBI Law Enforcement Bulletin, vol. 66, Number 5.

Wireless Data Forum (1998). Proven Radio Technologies. Available at: http://www.cdpd.org/public/whatis/radiotec.html. Last seen Jul 19, 1998.

Wireless Data Forum (1998). Proven Radio Technologies. Available at: http://www.cdpd.org/public/whatis/netreuse.html Last seen Jul 19, 1998.

Wireless Data Forum (1998). Wireless Mobile Data Networking: The CDPD Approach. Available at: http://www.cdpd.org/public/whatis/whatis.html. Last seen Jul 19, 1998.

Wrobleski, H. M. & Hess, K. M. (1993). Introduction to Law Enforcement and Criminal Justice, Fourth Edition. New York, NY: West Publishing Company.

Appendix A: The Survey Instrument

Computer Usage Survey

Lanny Lockhart, Jr.
Rochester Institute of Technology
302-661-1455

Introduction

This is an anonymous survey, and is part of an Information Technology Master's Thesis research effort at the Rochester Institute of Technology. The goal of this survey is to examine the usefulness of mobile computer systems in a metropolitan police department from the perspective of a patrol officer. Accordingly, the questions in this survey are designed to measure your opinions on the utility of the mobile computer systems since their introduction into your department. Your participation is voluntary. The data gained from these surveys will be analyzed through the use of a data analysis package known as SPSS, or Statistical Package for Social Science.

The resultant information gained from the returned surveys will be used in a non-critical fashion for the purposes of thesis completion. All hard data will be kept in my possession, permanently. Copies of the completed survey analysis will, however, be available upon request to members of the Wilmington Police Department.

Thank you for your time and assistance.

Lanny Lockhart, Jr.
1001 North Rodney Street
Wilmington, DE 19806
302-661-1455
lhlgcj@osfmail.rit.edu

Computer Usage Survey

Please answer the questions as honestly as possible and to the best of your ability. Circle or fill in blanks as necessary.

1. Sex:
   a. male b. female

2. Your age: _____

3. Race:
   a. Black
   b. Hispanic/latino
   c. White
   d. Asian-American
   e. Other

4. What is your rank? _____

5. How long have you been a Patrol Officer?
   a. 1 to 5 years
   b. 6 to 10 years
   c. 11 to 15 years
   d. 16 to 20 years
   e. 21 + years

Please answer each question as appropriate.

6. Please indicate how comfortable or uncomfortable you are with the computer you use at home (if you do not use a computer at home, please indicate such):
   a. Comfortable
   b. Somewhat comfortable
   c. Somewhat uncomfortable
   d. Strongly uncomfortable
   e. Do not use a computer at home

7. Please indicate how many hours a week you spend using your computer at home:
   a. Less than 2 hours a week
   b. Between 2 and 5 hours a week
   c. Between 5 and 10 hours a week
   d. More than 10 hours a week
   e. Do not use a computer at home

8. Please indicate how comfortable or uncomfortable you are with the desktop computer that your department is currently using?
   a. Comfortable
   b. Somewhat comfortable
   c. Somewhat uncomfortable
   d. Strongly uncomfortable
   e. Do not use a desktop computer at work

9. Please indicate how many hours a week you spend using your desktop computer at work:
   a. Less than 2 hours a week
   b. Between 2 and 5 hours a week
   c. Between 5 and 10 hours a week
   d. More than 10 hours a week
   e. Do not use a desktop computer at work

10. Please indicate how comfortable or uncomfortable you are with the mobile computer that your department is currently using?
   a. Comfortable
   b. Somewhat comfortable
   c. Somewhat uncomfortable
   d. Strongly uncomfortable
   e. Do not use a mobile computer at work

11. Please indicate how many hours a week you spend using your mobile computer at work:
   a. Less than 2 hours a week
   b. Between 2 and 5 hours a week
   c. Between 5 and 10 hours a week
   d. More than 10 hours a week
   e. Do not use a mobile computer at work

Please indicate if you agree or disagree with the following statements:

12. The mobile data terminal (MDT) that your department is currently using is a reliable piece of equipment:
   a. strongly disagree
   b. disagree
   c. agree
   d. strongly agree

13. The mobile data terminal (MDT) is easy to operate:
   a. strongly disagree
   b. disagree
   c. agree
   d. strongly agree

14. The mobile data terminal (MDT) was:
    a. very difficult to adapt to
    b. difficult to adapt to
    c. not difficult to adapt to
    d. easy to adapt to

The following questions should be answered based on your experiences since the adoption of the mobile computers by your department.

15. The "Enhanced Police Complaint" (EPC) software has made you more efficient with your time while on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

16. The "Enhanced Police Complaint" (EPC) software has increased your arrest rate:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

17. The "Enhanced Police Complaint" (EPC) software has made you "safer" on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

18. The "Enforcer" software (used for NCIC checks) has made you more efficient with your time while on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

19. The "Enforcer" software (used for NCIC checks) has increased your arrest rate:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

20. The "Enforcer" software (used for NCIC checks) has made you "safer" on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

21. The software used to access the Delaware Criminal Justice Information System (DCJIS) has made you more efficient with your time while on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

22. The software used to access the Delaware Criminal Justice Information System (DCJIS) has increased your arrest rate:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

23. The software used to access the Delaware Criminal Justice Information System (DCJIS) has made you "safer" on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

24. Overall, the adoption of the mobile computers in your department has made you more efficient with your time while on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

25. Overall, the adoption of the mobile computers in your department has increased your arrest rate:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

26. Overall, the adoption of the mobile computers in your department has made you "feel safer" while on the job:
    a. strongly disagree
    b. disagree
    c. agree
    d. strongly agree

27. Education:
    a. high school diploma, or GED
    b. some college work
    c. possess an Associates degree
    d. possess a Bachelors degree
    e. some post-graduate work
    f. possess a graduate degree

At this time, I would like to pose some open-ended questions about the technology your department is currently using. Please do not feel that you have to fill in any of these questions – they are completely optional. Also, do not hesitate to use the back of this document if extra room is needed.

28. Do you have any comments on the overall reliability of the mobile computing systems that your department is using?

29. Do you have any unique observations to make about that technology?

30. If you could, what features might you have included with the technology?

31. Is there anything else you would like to say about mobile computing or the technology used in your department?

Once again, I would like to thank you for your time and effort. If you have any questions regarding this survey or if you would like a copy of the completed report, I can be reached at the address below.

Thanks again for your time and assistance!

Lanny Lockhart, Jr.
1001 North Rodney Street

302-661-1455

26 Dec 00
Wilmington, DE
19806
lhlgcj@osfmail.rit.edu

Appendix B: The Revised Survey Instrument

This survey instrument has been generated as part of a 'lessons learned' request. It incorporates the various points, issues, and concepts uncovered during the course of this research effort, and place them into a new survey instrument. When the survey instrument is delivered again, it will be in the following format and design.

Information Technology Usage Survey

Lanny Lockhart, Jr.
Technologist
Rochester Institute of Technology
302-661-1455

Introduction

This is an anonymous survey, part of an Information Technology research effort conducted out of the Rochester Institute of Technology. The goal of this survey is to examine the use of the wireless notebook computers (in radio/patrol cars) in your department. Participation is voluntary.

All hard data will be kept permanently in the possession of the researcher. Copies of the completed survey analysis will, however, be available upon request to members of your police department.

Thank you for your time and assistance.

Lanny Lockhart, Jr.
1001 North Rodney Street
Wilmington, DE 19806
302-661-1455
lhlgcj@osfmail.rit.edu

Information Technology Usage Survey

Please answer the questions as honestly as possible and to the best of your ability. Circle or fill in blanks as necessary.

Definition of Terms

Efficiency – time spent writing reports and processing 'paperwork' while in the field, on the wireless notebook computer.
Arrest rates – the actual number of arrests per officer
Safety – This item refers to the officer's sense of safety when in the field as a result of using the wireless notebook computer. A comparison to keep in mind is how a bulletproof vest alters an officer's personal awareness when worn in the field.
Reliability – defined as the level of reliability of hardware and/or software; meaning, does the hardware/software crash, and if so, how often? 'Crashes' are defined as frozen screens/windows, network connectivity problems, or loss of data occurring outside of user error. For the purposes of this study, it will be gauged by number of crashes per shift.
Human-Computer Interaction (HCI) – this concept generally refers to the process by which human beings and computers interact together. In the case of this survey, it directly references how the patrol officer interacts with the hardware and/or software of the wireless notebook computer.

Section I: Demographics

Please answer each question as appropriate.

1. Sex:
    a. Male
    b. Female

2. Your age: _____

3. Race:
    a. African-American
    b. Hispanic/Latino
    c. Caucasian
    d. Asian-American
    e. Other

4. What is your rank? _____

5. How long have you been a Patrol Officer?
    a. 1 to 5 years
    b. 6 to 10 years
    c. 11 to 15 years
    d. 16 to 20 years
    e. 21 + years

6. Education:
    a. High school diploma, or GED
    b. Some college work
    c. Possess an Associates degree
    d. Possess a Bachelors degree
    e. Some post-graduate work
    f. Possess a graduate degree

Section II: Software Applications

Please answer each question as appropriate with regard to the software applications installed and used on your department's wireless notebooks.

7. The software used to access NCIC has impacted the **efficiency** of your radio/patrol duties to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

8. The software used to access NCIC has impacted your **arrest rate** to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

9. The software used to access NCIC has impacted your **safety** during radio/patrol duties in which fashion?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

10. The software used to access state-level criminal justice databases has impacted the **efficiency** of your radio/patrol duties to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

11. The software used to access state-level criminal justice databases has impacted your **arrest rate** to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

12. The software used to access state-level criminal justice databases has impacted your **safety** during radio/patrol duties in which fashion?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

13. The software used to process police complaints (or warrants) has impacted your **efficiency** of your radio/patrol duties to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

14. The software used to process police complaints (or warrants) has impacted your **arrest rate** to which degree?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

15. The software used to process police complaints (or warrants) has impacted your **safety** during radio/patrol duties in which fashion?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

Section III: Reliability

The following questions address the issue of the reliability of the software used on the wireless notebooks, the hardware of the wireless notebooks, and the wireless data network that the notebooks connect through.

16. The software used to access NCIC **crashes** how often per shift? _____

17. The software used to access state-level criminal justice databases **crashes** how often per shift? _____

18. The software used to process police complaints (or warrants) **crashes** how often per shift? _____

19. The wireless notebook computer used by your department **crashes** how often per shift? (Note: this question covers those crashes that are not a result of the above software applications) _____

20. Does the wireless modem card used by the notebook computer have **reliability** problems?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

21. If the wireless modem card does have **reliability** problems, how often per shift do they occur? _____

22. If the wireless modem card does appear to have **reliability** problems, do they occur most often in specific patrol regions?
    a. Very Positive
    b. Positive
    c. No impact/change
    d. Negative
    e. Very Negative

23. If the wireless modem card does appear to have **reliability** problems in certain patrol areas, please list those regions and possibly the number of problems per patrol region.

24. If the wireless modem card does appear to have **reliability** problems, please describe them in detail.

Section IV: Human-Computer Interaction

This section concerns the potential impact of HCI on the patrol officer's use of the wireless notebook computer.

25. Please indicate how comfortable or uncomfortable you are with the computer you use at home:
    a. Very comfortable to operate
    b. Comfortable to operate
    c. Uncomfortable to operate
    d. Very uncomfortable to operate
    e. Do not use a computer at home

26. Please indicate how many hours a week you spend using your computer at home:
    a. Less than 2 hours a week
    b. Between 2 and 5 hours a week
    c. Between 5 and 10 hours a week
    d. More than 10 hours a week
    e. Do not use a computer at home

27. Please indicate how comfortable or uncomfortable the wireless notebook is to physically operate?
    a. Very comfortable to operate
    b. Comfortable to operate
    c. Uncomfortable to operate
    d. Very uncomfortable to operate
    e. Do not use a mobile computer at work

28. Please indicate how many hours a week you spend using your mobile computer at work:
    a. Less than 2 hours a week
    b. Between 2 and 5 hours a week
    c. Between 5 and 10 hours a week
    d. More than 10 hours a week
    e. Do not use a mobile computer at work

29. How uncomfortable or comfortable is the operation of the NCIC software?
    a. Very comfortable
    b. Comfortable
    c. Uncomfortable
    d. Very uncomfortable
    e. No discernable affect on the end user's patrol activities

30. How uncomfortable or comfortable is the operation of the software that allows access to the state-level criminal justice databases?
    a. Very comfortable
    b. Comfortable
    c. Uncomfortable
    d. Very uncomfortable
    e. No discernable affect on the end user's patrol activities

31. How uncomfortable or comfortable is the operation of the software that processes police complaints (or warrants)?
    a. Very comfortable
    b. Comfortable
    c. Uncomfortable
    d. Very uncomfortable
    e. No discernable affect on the end user

The following questions talk about the potential use of new technologies.

32. Will the introduction of voice recognition capabilities positively or negatively impact your radio/patrol duties?
    a. Very Positive
    b. Positive
    c. No impact/change expected
    d. Negative
    e. Very Negative

33. Will the introduction of touch-pad screens positively or negatively impact your radio/patrol duties?
    a. Very Positive
    b. Positive
    c. No impact/change expected
    d. Negative
    e. Very Negative

34. What features might you request in future technologies?

35. Do you have any final comments about the wireless data notebooks in use by your department?

Once again, I would like to thank you for your time and effort. If you have any questions regarding this survey or if you would like a copy of the completed report, I can be reached at the address below.

Thanks again for your time and assistance!

Lanny Lockhart, Jr.
1001 North Rodney Street
Wilmington, DE 19806
302-661-1455
lhlgcj@osfmail.rit.edu

Appendix C: DAT File

```
012312111214144444332224223223
021251111414154344224334334324
031283112224243333223233333224
041263112122133343223223223224
051311111112323333332234333332
061371221122213332233333333233
071363221121223343213113113115
081363431223222323223223223224
091313111113122344333333333333
101273112214143443 22223223222
111273213424232232211123233225
121301115522222334111113314221
132323115523232333333333333331
141323121255143333223223223222
151313113414143323144344343341
161401122324243341213222222333
171273112414143343223323323232
181331232122224333233222233222
191342211213134334 2  1331   4
201273111213133344333   3334344
211301112121222332223223222222
221253115542343333223223224224
231283112113143443333333333334
241313211213143344223223223226
25226311231314114            6
261253111213231444     44443 2
271263111222222333111113223224
281313122424243334323223333332
291243111514143343323333334332
301313111212122333222222223224
311303111413133343212113223224
321343111313232242223222223322
```

Appendix D: Command File

The following lines of text are the actual COMMAND FILE designed for use in this study. As noted previously, this format was originally created for analysis with SPSS running on a VAX/VMS cluster, but was later imported into the Windows versions of SPSS where the statistical analysis was completed:

```
set width = 80/length = 59
Title Lanny Lockhart, Jr. msthesis 29 Oct 01
file handle msthesis/name = "msthesis.dat"

data list file = msthesis/
        ID 1-2 SEX 3 AGE 4-5
        RACE 6 RANK 7 SERVICE 8 QUES1 9 QUES2 10
        QUES3 11 QUES4 12 QUES5 13 QUES6 14
        QUES7 15 QUES8 16 QUES9 17 QUES10 18
        QUES11 19 QUES12 20 QUES13 21 QUES14 22
        QUES15 23 QUES16 24 QUES17 25 QUES18 26
        QUES19 27 QUES20 28 QUES21 29 EDUC 30

variable label
        ID `Identification Number'
        SEX `Sex of Respondent'
        AGE `Age of Respondent'
        RACE `Race of Respondent'
        RANK `Rank of Patrolman'
        SERVICE `Length of service in patrol duty'
        QUES1 `Comfort level with computer at home...'
        QUES2 `Hours/week using home computer...'
        QUES3 `Comfort level with desktop computer at work...'
        QUES4 `Hours/week using desktop computer at work...'
        QUES5 `Comfort level with mobile computer at work...'
        QUES6 `Hours/week using mobile computer at work...'
        QUES7 `Reliability of MDT...'
        QUES8 `MDT's ease of operation...'
        QUES9 `Adapting to the MDT was...'
        QUES10 `ECP software has made you more efficient...'
        QUES11 `ECP software has increased your arrest rate...'
        QUES12 `ECP software has made you "safer"...'
        QUES13 `Enforcer software has made you more efficient...'
        QUES14 `Enforcer software has increased your arrest rate...'
        QUES15 `Enforcer software has made you "safer"...'
        QUES16 `DCJIS has made you more efficient...'
        QUES17 `DCJIS has increased your arrest rate...'
        QUES18 `DCJIS has made you "safer"...'
        QUES19 `Overall, the adoption of MDT's has made you more efficient...'
        QUES20 `Overall, the adoption of MDT's has increased your arrest rate...'
        QUES21 `Overall, the adoption of MDT's has made you "feel safer"... '
        EDUC `Education of Respondent'
```

```
value labels
        SEX     1 `male`
                2 `female` /
        RACE    1 `Black'
                2 `Hispanic/Latino'
                3 `White'
                4 `Asian-American'
                5 `Other' /
        RANK    1 `Patrolman'
                2 `Corporal'
                3 `Sgt.'
                4 `Master Sgt.'
                5 `Lt.' /
        QUES1           1 `COMFORTABLE'
                2 `SOMEWHAT COMFORTABLE'
                3 `SOMEWHAT UNCOMFORTABLE'
                4 `STRONGLY UNCOMFORTABLE'
                5 `DO NOT USE A COMPUTER AT HOME' /
        QUES2           1 `LESS THAN 2 HOURS A WEEK'
                2 `BETWEEN 2 AND 5 HOURS A WEEK'
                3 `BETWEEN 5 AND 10 HOURS A WEEK'
                4 'MORE THAN 10 HOURS A WEEK'
                5 'DO NOT USE A COMPUTER AT HOME' /
        QUES3           1 `COMFORTABLE'
                2 `SOMEWHAT COMFORTABLE'
                3 `SOMEWHAT UNCOMFORTABLE'
                4 `STRONGLY UNCOMFORTABLE'
                5 `DO NOT USE A COMPUTER AT WORK' /
        QUES4           1 `LESS THAN 2 HOURS A WEEK'
                2 `BETWEEN 2 AND 5 HOURS A WEEK'
                3 `BETWEEN 5 AND 10 HOURS A WEEK'
                4 'MORE THAN 10 HOURS A WEEK'
                5 'DO NOT USE A COMPUTER AT WORK' /
        QUES5           1 `COMFORTABLE'
                2 `SOMEWHAT COMFORTABLE'
                3 `SOMEWHAT UNCOMFORTABLE'
                4 `STRONGLY UNCOMFORTABLE'
                5 `DO NOT USE A COMPUTER AT WORK' /
        QUES6           1 `LESS THAN 2 HOURS A WEEK'
                2 `BETWEEN 2 AND 5 HOURS A WEEK'
                3 `BETWEEN 5 AND 10 HOURS A WEEK'
                4 'MORE THAN 10 HOURS A WEEK'
                5 'DO NOT USE A COMPUTER AT WORK' /
        QUES7           1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
        QUES8           1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
        QUES9           1 `VERY DIFFICULT TO ADAPT TO'
                2 `DIFFICULT TO ADAPT TO'
                3 `NOT DIFFICULT TO ADAPT TO'
                4 'EASY TO ADAPT TO' /
```

```
QUES10          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES11          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES12          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES13          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES14          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES15          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES16          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES17          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES18          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES19          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES20          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
QUES21          1 `STRONGLY DISAGREE'
                2 `DISAGREE'
                3 `AGREE'
                4 'STRONGLY AGREE' /
SERVICE         1 `1 to 5 years'
                2 `6 to 10 years'
                3 `11 to 15 years'
                4 `16 to 20 years'
                5 `21+years'
```

```
        EDUC  1 `High school diploma, or GED'
              2 `some college work'
              3 `possess an Associates degree'
              4 `possess a Bachelors degree'
              5 `some post-graduate work'
              6 `possess a graduate degree' /

Recode AGE (18 thru 22=1) (23 thru 27=2) (28 thru 32=3) (33 thru 37=4)
          (38 thru 42=5) (else=9).
variable labels AGE `Age collapsed into categories'.
value labels AGE 1 `18 - 22 years'
          2 `23 - 27 years'
          3 `28 - 32 years'
          4 `33 - 37 years'
          5 `38 - 42 years'
          6 `43 or more years'.
missing values AGE (9)

reliability variables = QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
                        QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15
                        QUES16 QUES17 QUES18 QUES19 QUES20 QUES21

frequencies variables = SEX SERVICE RACE RANK EDUC
        /statistics = mode
        /hbar

frequencies variables = AGE
        /statistics = all
        /percentiles 25 50 75
        /hbar

frequencies variables = QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
                        QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15
                        QUES16 QUES17 QUES18 QUES19 QUES20 QUES21
        /statistics = all
        /percentiles 25 50 75
        /hbar

crosstabs
/tables = EDUC BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
 /format = avalue tables
 /statistics=chisq
 /cells= count row column
total

crosstabs
/tables = SEX BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
 /format = avalue tables
 /statistics=chisq
 /cells= count row column
total
```

```
crosstabs
/tables = SERVICE BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
  /format = avalue tables
  /statistics=chisq
  /cells= count row column
total

crosstabs
/tables = RACE BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
  /format = avalue tables
  /statistics=chisq
  /cells= count row column
total

crosstabs
/tables = RANK BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
  /format = avalue tables
  /statistics=chisq
  /cells= count row column
Total

crosstabs
/tables = AGE BY QUES1 QUES2 QUES3 QUES4 QUES5 QUES6 QUES7 QUES8
QUES9 QUES10 QUES11 QUES12 QUES13 QUES14 QUES15 QUES16 QUES17 QUES18
QUES19 QUES20 QUES21
  /format = avalue tables
  /statistics=chisq
  /cells= count row column
total
```

Appendix E: Codebook

SPSS Variable Name	Location of Variable	Full Variable Name
ID	1-2	Identification
SEX	3	Sex of Respondent
AGE	4-5	Age of Respondent
RACE	6	Race of Respondent
RANK	7	Rank of Respondent
SERVICE	8	Length of Service
QUES1	9	Question #1
QUES2	10	Question #2
QUES3	11	Question #3
QUES4	12	Question #4
QUES5	13	Question #5
QUES6	14	Question #6
QUES7	15	Question #7
QUES8	16	Question #8
QUES9	17	Question #9
QUES10	18	Question #10
QUES11	19	Question #11
QUES12	20	Question #12
QUES13	21	Question #13
QUES14	22	Question #14
QUES15	23	Question #15

QUES16	24	Question #16
QUES17	25	Question #17
QUES18	26	Question #18
QUES19	27	Question #19
QUES20	28	Question #20
QUES21	29	Question #21
EDUC	30	Education of Respondent

Appendix F: Complete SPSS Test Results

Note: The SPSS results are attached to this document in electronic format on a CDROM.


CD-R
650
74min MB
TDK