Themis: Research Journal of Justice Studies and Forensic Science

Volume 4 Article 9

5-10-2016

The Utilization of Mobile Technology for Crime Scene Investigation in the San Francisco Bay Area

Marc LoGrande
San Jose State University

The Utilization of Mobile Technology for Crime Scene Investigation in the San Francisco Bay Area

Abstract
The research presented aims to explore factors affecting the decision to adopt a mobile crime scene investigation application in police departments throughout the San Francisco Bay Area. To accomplish this goal, the mobile technology acceptance model was used in designing a survey for data collection. This model utilizes four categories to interpret the factors that influence a police officer's decision to accept or reject mobile technologies: performance, security and reliability, management style, and cognitive acceptance. Nine police departments were sampled through a series of in-person and over-the-phone interviews to obtain data regarding factors affecting the adoption of a mobile crime scene investigation application. Results suggest that if a mobile crime scene investigation application were made available, a vast majority of the police departments in the Bay Area would implement this new technology.

Keywords
police technologies, crime scene investigation, mobile technologies, cloud storage

The Utilization of Mobile Technology for Crime Scene Investigation in the San Francisco Bay Area

Marc LoGrande

Abstract

The research presented aims to explore factors affecting the decision to adopt a mobile crime scene investigation application in police departments throughout the San Francisco Bay Area. To accomplish this goal, the mobile technology acceptance model was used in designing a survey for data collection. This model utilizes four categories to interpret the factors that influence a police officer's decision to accept or reject mobile technologies: performance, security and reliability, management style, and cognitive acceptance. Nine police departments were sampled through a series of in-person and over-the-phone interviews to obtain data regarding factors affecting the adoption of a mobile crime scene investigation application. Results suggest that if a mobile crime scene investigation application were made available, a vast majority of the police departments in the Bay Area would implement this new technology.

VOLUME IV • 2016

Introduction

Exponential strides in technological advancements occurring in recent decades are substantially influencing police practices. Such technologies include the telegraph, two-way radios, computer-aided dispatch, and the implementation of mobile display terminals in patrol cars, which allow for access to crime information databases, report writing, and electronic submission of reports from the field to the station (Colvin & Goh, 2005). One recent technological advancement utilizes mobile technology for data collection and transmission. Research shows that the utilization of mobile technology improves police problem-solving abilities (Lindsay, Jackson, & Cooke, 2011). When used to aid police in criminal cases, this type of technology is referred to as "teleforensics" and involves the use of communications and other advanced technologies to transmit data in real time to remote locations (Homeyer & Quigley, 2014). Teleforensics has inspired the design of mobile crime scene investigation applications that aim to improve the efficiency of evidence documentation and note taking by cutting out the use of the traditional pen and paper system. Additionally, teleforensics enables data transmission in real time using cloud technology, which also provides forensic laboratories with readily accessible data.

Recently, CrimePad arose as the ideal professional grade crime scene mobile application and is marketed as the "future of criminal investigation" (Byrne, 2014). The first version of CrimePad was released by Visionations April 10, 2013. CrimePad is compatible with Apple, Windows, and Android operating systems and requires a browser IE 10 or higher, Chrome, Safari, or Android Chrome. Police departments in California, Virginia, Tennessee, and other small departments that

asked to remain anonymous have adopted this technology (Byrne, 2014). This application allows users to document and record all aspects of a crime scene including: access logs, notes, evidence, sketches/diagrams, photographs, processing techniques, and interviews. This is essential for the adoption of a mobile crime scene investigation application, because crime scene investigators (CSIs) currently utilize photography, measurement tools, and diagram software to accurately reproduce a crime scene. Additionally, CrimePad keeps a secure electronic record for every case in the cloud, a centralized server located on the internet, enabling the transmission of readily accessible data in real time between devices. Supplemental features that CrimePad does not include, and should be considered, are voice transcription and report templates; these features can aid more efficient note taking and reduce time spent writing reports after processing a crime scene.

Despite the apparent advantages of CrimePad, developers must overcome inherent obstacles to ensure that mobile technologies are adopted within the realm of crime scene investigation. One such obstacle pertains to data security: the need to securely store and transfer data in real time between devices. Robust data security is essential for the adoption of a mobile crime scene investigation application, which would obstruct preexisting policing methods. Research shows that officers may be disinclined to accept new technology if it interferes with preexisting models or patterns of policing (Colvin et al., 2005). Departmental resources are also critical to consider when analyzing the adoption of new technology as some police departments receive more funding than others. Skogan and Hartnett (2005) found that under-resourced departments tend to reject the idea of new technology due to the lack of financial

capital. These factors must be reviewed to understand the transition from traditional crime scene investigation methods to the adoption of mobile technology within crime scene investigation.

This paper will explore the adoption of a mobile crime scene investigation application in police departments throughout the San Francisco Bay Area. The study herein qualitatively analyzes data collected through a survey to determine the acceptance and use of an application of this nature. The following section presents a literature review discussing the technology acceptance model for policing and current research on data security and transmission within the cloud.

Literature Review

The Technology Acceptance Models

The Technology Acceptance Model (TAM), developed by Fred Davis in 1989, served as the basis for three subsequent variations of the original model (Lindsay, Jackson, & Cooke, 2011). The TAM assesses factors that influence the implementation of new technologies within organizations in order to determine why users accept or reject the technology. The original model uses two variables - perceived usefulness and perceived ease of use - to explain how such factors influence users' decisions regarding the technology presented. The TAM produced viable results in a variety of different settings, confirming its validity (Lindsay et al., 2011). This consistency is critical in researching the adoption of technology in the policing context. Unfortunately, external factors, such as organizational culture and management style, are not featured in the original TAM, so TAM 2 and TAM 3 were created to incorporate these external factors.

The Technology Acceptance Model 2

The TAM 2, a modified version of the original TAM that was introduced by Venkatesh and Davis in 2000, expanded the original model to incorporate social influence and cognitive instrumental processes (Lindsay et al., 2011). The incorporation of social influence suggests that a technology will become increasingly accepted with increased system experience. These factors stress the perceived usefulness of the technology, disregarding the perceived ease of use. Therefore, the TAM 2 is an inadequate model for assessing factors influencing the adoption of technology in a police context.

The Technology Acceptance Model 3

The TAM 3, developed by Venkatesh and Bala in 2008, includes additional perceived usefulness elements and perceived ease of use factors. This addresses the notion that an individual can complete a task whether an organization has suitable technical support and whether potential users display the required level of comfort linked to operating new technology (Lindsay et al., 2011). Despite this model's ability to thoroughly assess the perceived usefulness and the perceived ease of use of a technology, it is based on individual factors as opposed to the overall implementation context as a whole.

Applied Technology Models

Colvin and Goh (2005) used the original TAM developed by Fred Davis, which infers that police officers' acceptance levels rely on the ease of use and the usefulness of the product, to explain why police officers accept or reject new technologies. Colvin and Goh (2005) found a four-factor model to be more effective when measuring police officers' acceptance of the new technology. The four factors are: ease of use, usefulness, information quality, and timeliness. Colvin and Goh

(2005) found that information quality and timeliness are also vital factors in considering the acceptance of such technology.

In a separate research study, Lindsay et al. (2011) used a qualitative approach to perform an in-depth investigation of factors affecting user acceptance of mobile technologies amongst police officers. This was accomplished by using a combination of the three TAMs to reengineer a model that was better suited for a mobile policing context. Results indicated four significant overarching categories: performance, security/reliability, management style, and cognitive acceptance. In this study, the main barriers to achieving officer acceptance were low awareness of the benefits associated with the technology and reduced functionality. To promote product acceptance, organizations should ensure that officers are knowledgeable of the benefits associated with using the technology and also provide thorough demonstrations and clear communication of operating procedures

Mobile-Technology Acceptance Model

The mobile-TAM was developed to address factors beyond the fixed technology environment in which TAM 2 and TAM 3 reside to incorporate wider organizational factors to increase officer acceptance of mobile technologies. The mobile-TAM, a high-level model that encompasses elements from Davis' original TAM in addition to police specific contributions, applies to a variety of police contexts. This model highlights four categories to explain the factors that influence a police officer's decision to accept or reject mobile technologies. The categories are: performance, security and reliability, management style, and cognitive acceptance (Lindsay, Jackson, & Cooke, 2014). Management style and cognitive acceptance stems from Davis' original TAM, which uses a two variable system: perceived ease

of use and perceived usefulness. For example, perceived ease of use can refer to the battery life of the mobile device, while the perceived usefulness can include the mobile technology's ability to transmit and store data. The level of training, officer involvement, and information for mobile data terminals are embedded within the management style category (2014). The subjective norms of data security and organizational culture affect cognitive acceptance. These factors support the wide implementation of mobile-TAM in a police context.

Data Security

Data security is essential to the adoption of a mobile crime scene investigation application. Rong, Nguyen, and Jaatun (2012) explore the idea of cloud computing, discuss related security challenges, and emphasize technological approaches that can improve cloud security. Cloud computing provides convenient, on-demand access to a shared pool of data, allowing access to resources without requiring detailed knowledge of the underlying technologies (Rong et al., 2012).

There are private, public, community, and hybrid based clouds. For the purpose of this study, a community-based cloud was utilized. Community-based clouds allow members of a closed community, such as members of a forensics team, to share resources. With any type of cloud, a traditional security challenge follows; the privacy and confidentiality of user data is the most critical security concern. To prevent leaks of confidential data stored in the cloud, the use of homomorphic or incremental encryption is suggested by Rong et al. (2012).

Homomorphic encryption uses a mathematical algorithm to add the encrypted data and decrypts the results, resulting in functionality equivalent to applying the algorithm to the unencrypted data (Naone, 2011). For example, if you want to

add 4 and 5, the encryption software encrypts the data so that 4 becomes 22 and 5 becomes 63; the encrypted data is sent to the cloud and processed, where the result, 85, can be downloaded and decrypted to provide the final answer, 9 (Naone, 2011). This is advantageous because it provides data security within the cloud. Data is not decrypted until it is downloaded from the cloud, preserving the integrity of the data within the cloud. However, homomorphic encryption runs too slowly due to its numerous operations and would require further development to accompany a widely useable framework.

Incremental encryption aims to modify preexisting functions instead of re-computing them. This method reduces the computation time of cryptographic functions, an underdeveloped area of homomorphic encryption. Despite the numerous technological approaches that can improve cloud security, there is currently no universal method (Rong et al., 2012).

Unfortunately, a concerning issue often arises when data reaches the cloud service provider, which is a third-party data center. The cloud service provider plays an important role in data management and is able to view data items without the data owners' permission. This can reveal confidential information such as medical records, financial charts, and crucial evidence pertaining to ongoing investigations that should not be exposed to outside parties. Koo, Hur, and Yoon (2012) propose a framework using attribute-based encryption to increase the compatibility of cloud storage services, which provides secure one-to-many communications. The proposed framework of Koo et al. (2012) enhances searching efficiency and provides rich detail, guaranteeing data security. This can be accomplished through a new searchable encryption framework that exploits attribute-based encryption with scrambled attributes to

compensate for the restrictions set fourth by old keyword-based searches (Koo et al., 2012). Old keyword-based searches generate two types of private keys: one to access encrypted content and one for the decryption of the encrypted content, thus resulting in double the key storage requirements, which restricts the one-to-many communication property. The new searchable encryption system utilizes an owner-specific access policy and keyword searching set to retrieve data. Accessing secured content in the cloud requires the user to create passkey terms that adequately match those found in the encrypted systems keyword/content database (Koo et al., 2012). Passkey terms are utilized exclusively by the cloud for retrieving encrypted content, preventing the cloud service provider from gaining access to confidential data; instead, only keywords related to the content are revealed without sacrificing the restrictions of attribute-based encryption.

Sanyal and Iyer (2013) delve into a different mechanism for securely transmitting data in and out of the cloud using the Advanced Encryption Standard (AES). The cloud requires encryption processes to create a virtual private storage system that maintains confidentiality and integrity of data. The AES, a new cryptographic algorithm, uses keys of 128, 192, and 256 bits. The AES cipher consists of a basic operation called round, which is repeated a number of times. The number of rounds in AES depends on the key length: 10 rounds for 128 bits, 12 rounds for 192bits, and 14 rounds for 256 bits (Sanyal et al., 2013). As the key length increases, the encryption becomes more complex and harder to crack. This outlines the essence of the strong encryption power of AES, which aims to provide safety while transmitting and security while storing data. In cloud computing, the data sender sends data to the AES model, where

the cryptographic algorithm encrypts the data and sends it to the cloud service provider to store. Upon retrieval, the cloud service provider will send the encrypted data to the requested site, where the AES model will decrypt the data and supply the content in plaintext. When compared to other available security techniques in cloud computing, AES is among one of the most trusted techniques for providing data security within the cloud (Sanyal et al., 2013). The downfall of AES is the software's inability to prevent data loss; if the access keys that pertain to certain data are lost, that encrypted data will remain in the cloud unable to be deciphered.

Methods

The goal of this research was to explore the adoption of a professional-grade crime scene application in police departments and forensic laboratories throughout the Bay Area. This study sampled CSIs, forensic specialists, and detectives from nine police departments within the Bay Area. Data was gathered through over-the-phone and in-person interviews, which assessed participants' familiarization with current technology (smart phones and tablets), opinions regarding the use of mobile technology for crime scene investigation, and any foreseen implications to adopting this new technology. The survey was designed with respect to the mobile-TAM. In order to interpret decisions to accept or reject mobile technologies, the following categories were utilized: performance, security and reliability, management style, and cognitive acceptance. Data was quantitatively analyzed to determine factors influencing the decisions of police departments surveyed to accept or reject an application of this nature. Nine individuals from eight different police departments and forensic laboratories made up the sample

population. Individuals were chose based on their availability to complete in-person or over the phone interviews.

Results

Results show that six of the nine (66.7%) police departments sampled in this study would adopt a professional-grade crime scene investigation mobile application if all the desired features (Table 1) were included.

Table 1: Comparison of the most valued application features, as indicated by each independent police department and forensic laboratory.

Police Departments	Photographs	Voice Transcription	Measurement Tools	Diagram Software	Report Templates	Case File Storage	Case File Transmission
CPD	x	x	x	x		x	x
FPD			x	x	x	x	x
MVPD	x	x	x	x	x	x	x
SJPD	x	x	x	x	x		
SMCFL-1		x	x	x	x	x	x
SMCFL-2	x	x	x	x	x	x	
SMPD	x	x	x	x			x
SCPD	x	x	x	x	x	x	x
SPD	x	x	x	x	x	x	x

Measurement tools and diagram software were among the most valued application features, requested by all (100.0%) police departments and forensic laboratories sampled in this study. Additionally, other features requested include: video capabilities; Google maps to obtain an aerial view of the crime scene; record of data alterations indicating a date and personnel signifier to maintain evidence integrity; a mobile fingerprint scanner; and access to county databases.

In addition to the application features cited as valuable, however, there were multiple noted foreseen barriers (Figure 2)

to implementing a mobile technology of this nature in a police context.

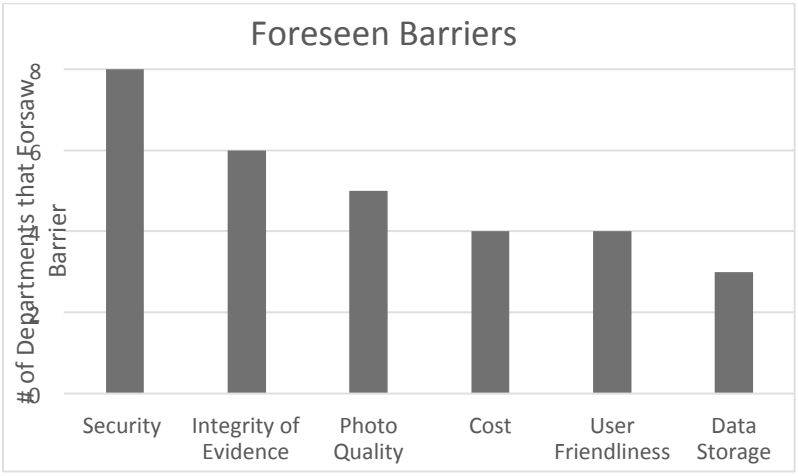

Figure 2: A comparison between the different foreseen barriers threatening to hinder the implementation of a crime scene investigation mobile application.

The survey showed security to be of greatest concern and was cited as a foreseen barrier by eight of the nine (88.8%) police departments and forensic laboratories sampled. This includes security concerns associated with storing data in the cloud and transmitting sensitive data in real time.

Discussion

Results of this study confirm that a majority (66.7%) of police departments in the Bay Area would implement a crime scene investigation mobile application if it were made available with all the desired features (Table 1). The most desired features include: photographs, voice transcription, measurement tools, diagram software, report templates, case file storage, and case file transmission. However, photographs, measurement tools,

and diagram software must be extremely detailed and accurate for these features to be beneficial to investigation. Crime scene photography requires accurate reproduction of crime scene details through detail specific photographs; measurement tools and diagrams would complement photographic crime scene representations. Despite the intensive stress on accuracy, technology that produces viable results already exists: all nine of the police departments sampled already use 3D-diagram software (total station), laser scanners (leica scanner), and high quality digital cameras. These technologies could be incorporated into the mobile crime scene investigation application to condense applications and increase the application's utility.

Transitioning from preexisting police practices to new methods involves inherent barriers that must be overcome (Colvin et al., 2005). Results of this study indicate that the most significant barriers to implementing a mobile crime scene investigation application were data security, integrity of evidence, photo quality, cost, user friendliness, and data storage. As expected, data security was of greatest concern and includes concerns of intercepting the transmission of case files, insecurities with cloud storage of case files, and lost or damaged tablets housing sensitive information. Such problems can be countered with AES, which provides protection while transmitting and security while storing data; AES is currently one of the most trusted techniques to provide data security within the cloud (Sanyal et al., 2013). According to a participant from the Fremont Police Department, "most cloud storage systems are more secure than our police departments. People are just less familiar with cloud technologies," (personal interview, April 13, 2015). The cost of software, training, maintenance, and updates

required to maintain the application was also found to be an inherent barrier to implementing this new technology. This parallels the findings of Skogan et al. (2005), which suggest that financial capital can impact the acceptance of new technologies in publicly funded police departments. However, these findings may not be representative, as 66.7% of police departments sampled would implement a mobile crime scene investigation application, regardless of such barriers. The consensus of groups sampled suggests that technological advancements are occurring in the direction of mobile technology and an application of this nature would thrive in Bay Area police departments.

Alternatively, the three police departments (33.3%) sampled that claimed they would not adopt this new technology, preferring current methods of manual crime scene processing. These results, however, show a strong correlation between time on the job and a preference for the current methods of crime scene processing. Among the three individuals surveyed (criminalist, CSI, and forensic specialist) from these departments, the length of experience processing crime scenes was 23 years, 18 years, and 18 months. Results indicate a persistent lack of trust in data security and storage within the cloud among these individuals. Nevertheless, a forensic specialist from the San Mateo County Forensic Lab expressed that she would be more inclined to use new technology if it were more common within professionals in her field (personal interview, April 8, 2015). This is consistent with one of the four categories of mobile TAM, cognitive acceptance, which stems from Davis' original TAM. According to this model cognitive acceptance influences a police officer's decision to accept or reject mobile technologies.

Conclusion

The goal of this research was to explore factors affecting the adoption and implementation of a mobile crime scene investigation application in police departments throughout the Bay Area. Despite evident barriers, the majority of police departments accepted the idea of utilizing mobile technologies for crime scene investigation. This paper provides evidence supporting mobile technologies capable of securely transmitting and storing sensitive data in the cloud. Regardless, there is no current encryption standard that can be trusted in every police context. Further research should focus on developing a reliable encryption technique that is applicable in every police context to ensure the implementation of a mobile crime scene investigation application on a universal scale.

Acknowledgements

The author wishes to acknowledge the officers from the Fremont Police Department, the Mountain View Police Department, the San Jose Police Department; the San Mateo County Forensic Lab, the Sunnyvale Police Department, the Campbell Police Department, the San Mateo Police Department, and Santa Clara Police Department and their officers for participating in this study. The time and input of these individuals was vital to this study and greatly appreciated.

References

Byrne, C. (2014). How an iPad app is transforming the way police work crime scenes. *Fast Company*. Retrieved from http://www.fastcolabs.com/3025289/how-an-ipad-app-is-transforming-the-way-police-work-crime-scenes

Colvin, C., & Goh, A. (2005). Validation of the technology acceptance model for police. *Journal of Criminal Justice,* 5(2), 89-95.

Homeyer, J., & Quigley, A. (2014). Technology: The Trojan Horse of change. *Evidence Technology Magazine.* Retrieved from http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1691&Itemid=1

Koo, D., Hur, J., & Yoon, H. (2012). Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. *Computers & Electrical Engineering,* 12(2), 34-46.

Lindsay, R., Jackson, T., & Cooke, L. (2011). Adapted technology acceptance model for mobile policing. *Journal of Systems and Information Technology,* 16(7), 389-407.

Lindsay, R., Jackson, T., & Cooke, L. (2014). Empirical evaluation of a technology acceptance model for mobile policing. *Police Practice and Research*, 15(5), 186-210.

Naone, E. (2011). Homomorphic encryption making cloud computing more secure. *MIT Technology Review,* 13(1), 1.

Rong, C., Nguyen, S., & Jaatun, M. (2012). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering,* 8(4), 47-54.

Sanyal, S., & Iyer, P. (2013). Cloud computing: An approach with modern cryptography. *International Journal of Engineering,* 12(4), 312-326.

Skogan, W., & Hartnett, S. (2005). The diffusion of information technology in policing. *Police Practice and Research*, 6(5), 401-417.

Sorensen, C., & Pica, D. (2005). Tales from the police: Rhythms of interaction with mobile technologies. *Information and Organization,* 10(6), 125-149.

Marc LoGrande graduated with his bachelor's degree in Forensic Science with an emphasis in Chemistry from San Jose State University in 2015. He is currently working for the family construction business in Southern California while pursuing a career in the field of forensics. Outside of his work responsibilities, Marc enjoys spending time with family and friends, surfing, and traveling.