The Impact of the Digital Society on Police Recruit Training in Canada

by

James G. Robertson

A thesis submitted to the School of Graduate and Postdoctoral Studies in partial fulfillment of the requirements for the degree of

Masters of Arts in Education

Faculty of Education

Ontario Tech University

Oshawa, Ontario, Canada

December 2019

THESIS EXAMINATION INFORMATION

Submitted by: **James Robertson**

Master of Arts in **Education**

Thesis title: **The Impact of the Digital Society on Police Recruit Training in Canada**

An oral defense of this thesis took place on **November 29, 2019** in front of the following examining committee:

Examining Committee:

Chair of Examining Committee	Dr. Bill Hunter
Research Supervisor	Dr. Bill Muirhead
Examining Committee Member	Dr. Christopher O'Connor
Examining Committee Member	Dr. Jennifer Laffier
External Examiner	Dr. Chris Giacomantonio, Halifax Regional Police

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

Abstract

This research study examines the recruit training of police officers in Canada in light of society's increasing dependence on digital technologies, systems, and devices. The study employed qualitative interviews with eight participants from recognized police recruit training academies in Canada. An extensive review of the literature indicates that societies face increasing cyber-crimes and crimes involving digital evidence. This, along with police agencies' adoption of digital tools, software, systems, and devices, have created policing environments where officers need proficiency to understand and use digital technologies. This study uses a theoretical framework of technology adoption, called UTAUT (Unified Theory of Acceptance and Use of Technology) alongside a grounded theory approach to understand the impact, challenges, and opportunities for digital literacy skills development at the basic recruit training academies. Findings from the interviews reveal that there is a need for Canadian police officers to be digitally literate in order to provide policing services to an increasingly digital crime landscape.

Keywords*:* police training; recruit training; digital literacy; UTAUT; digital technology

AUTHOR'S DECLARATION

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize Ontario Tech University to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize Ontario Tech University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

The research work in this thesis that was performed in compliance with the regulations of Ontario Tech's Research Ethics Board/Animal Care Committee under REB Certificate number 15156.

JAMES ROBERTSON

STATEMENT OF CONTRIBUTIONS

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication. I have used standard referencing practices to acknowledge ideas, research techniques, or other material that belong to others. Furthermore, I hereby certify that I am the sole source of the creative works and/or inventive knowledge described in this thesis.

ACKNOWLEDGEMENTS

I would like to thank a number of people who contributed to this thesis. I appreciate the support of the Canadian Association of Chiefs of Police (CACP). I would like to thank the participants who volunteered their time and experience to this study. Thanks to Dr. Bill Muirhead for supervising this thesis. Thanks as well to my supervisory committee, especially Dr. Christopher O'Connor for supporting this research from the outset. Finally, I owe a debt of gratitude to my family and my wife, without whose support none of this research could have happened.

Table of Contents

Table 1: *Common Acronyms*

Acronym	**Description and Definition**
HMIC	Her Majesty’s Inspectorate of Constabulary
UTAUT	Unified Theory of Acceptance and Use of Technology
TAM	Technology Acceptance Model
IT	Information Technology
IoT	Internet of Things
ICT	Information and Communication Technologies
SWGDE	Scientific Working Group on Digital Evidence
GPS	Global Positioning Satellite
PBL	Problem-based Learning
GIS	Geographical Information System
IP	Internet Protocol
BWC	Body-worn Camera
OPP	Ontario Provincial Police
RCMP	Royal Canadian Mounted Police
RNC	Royal Newfoundland Constabulary
UNESCO	United Nations Educational, Scientific and Cultural Organization
LMS	Learning Management System
NIJ	National Institute of Justice

Chapter 1: Introduction

1.0 Overview

The purpose of this study is to examine the impact of an increasingly digital society on police training in Canada and add to the current literature surrounding police training in Canada. The goal of the research is to gain views from police training experts at accredited institutions across Canada who are directly involved in basic recruit training of frontline police officers to understand the ways in which police recruit training academies are changing as a result of the widespread adoption, acceptance, use, and ubiquity of digital devices, systems, tools, and software.

1.1 Context: The Digital Society

From the first computers in the 1950's to today's Internet and beyond, humanity has increasingly become dependent on computers and digital technologies (Wydra & Hartle, 2015). Today's digital society is made possible by the evolution of digital technology from the stuff of science fiction to our current reality; in a sense, society has evolved with and because of technology (Chaouchi & Bourgeau, 2018; Council of Canadian Academies, 2014) to the point where "society is now wholly reliant on digital technologies for all aspects of life" (Horsman, 2017, p.449). Digital technology has impacted all facets of life; from the way we eat, sleep, live, work, entertain, exercise, parent, relax, learn, and shop (Savona & Mignone, 2004). It has impacted every field and profession, government and business (Choo, 2011; Nuth, 2008; Grabosky & Smith, 2017). Virtually everything Canadians do is touched by technology in some way. Canadians spend more time online than any other country in the world (Public Safety Canada, 2018). We live in a digital society (Goodison, Davis & Jackson, 2015; Wall & Williams, 2013; Koper, Taylor & Kubu, 2009).

The term *digital society* is a concept that recognizes how information technology is an embedded part of the larger social entity and is incorporated into our everyday lives (Hanna, 2016; Stratton, Powell & Cameron, 2017). Today, technology has become intrinsic to society and seems to be a natural component of our personal lives (Faith & Bekir, 2015), so much so that access to digital information, primarily via the Internet, is considered by many to be a basic human right (Damodaran & Burrows, 2017) and integral to people's lives (Her Majesty's Inspectorate of Constabulary (HMIC), 2015). According to Horsman (2017), the Internet has over three billion daily users – a figure that has tripled year after year. That number has increased to 4.3 billion users (Kemp, 2019). According to Chaouchi and Bourgeau (2018) our digital society "is now totally dependent on the biggest network ever, the Internet; one of the major human inventions" (p.1). The development of the Internet, mobile computing, and cellular telephony has transformed modern society (Holt, 2018).

The Internet connects the millions of digital information systems that are required in order for society to function. As Evans and Reeder (2010) state, "That the nation and the world are now critically dependent on cyber infrastructure is no longer a matter of debate" (p.1). Cobb (2016) supports this assertion, stating that "the world relies on information systems" (p.1). Information technology (IT) infrastructure is growing exponentially (Dawson & Thomson, 2018; Hitchcock, Holmes, & Sundorph, 2017), as are the number of digital devices and the number of technology users (Dawson & Thomson, 2018).

Digital devices, such as smartphones, cameras, wearable activity monitors, and other computing devices and sensors that connect to the internet, either directly or via management software, are growing exponentially in number (Craiger, Pollitt, & Swauger, 2005) and represent what is commonly referred to as the Internet of Things, or IoT (Public Safety Canada, 2018). Public Safety Canada (2018) predicts that the number of IoT devices will exceed 25 billion devices by the year 2020. Nearly all aspects of life are now dependent on Internet-enabled devices (Holt, 2018). Most individuals today have a mobile device (MacNeil, 2015). In every sense, the proliferation of technology in today's society continues to grow at an exponential rate (Sturgeon, 2015).

1.1.1 Information and Data are the "new oil" in a Global Economy

The engine that drives society's dependence on digital technology is information, or, more specifically, digital information in binary form, also referred to as data. People, devices, sensors, computer hardware and software are constantly creating data, using data, and making decisions based on information. Data, when compiled, analyzed, and contextualized creates new information, resulting in a cycle of information production and analysis. It is this information that moves society. The automobile, when introduced in the early part of the 20th century transformed society. Automobiles made the world smaller because they allowed people and things to cross greater spaces in less time, and oil was the fuel that moved the automobile.

Data has been referred to by many scholars as the new oil, in the sense that it fuels the next vehicles of society – computers and networks. The similarities do not end there. Both oil and data can be mined, and, like oil, data in its raw form has little use - requiring refinement in order to be used effectively and efficiently. Both oil and information are commodities of tremendous value to people, businesses, and governments alike. Oil, in its time, supported and enhanced existing industries while concurrently creating new industries, and data has done the same, creating the current digital society. Those in control of the supply and management of oil became some of the wealthiest people on earth. "Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft—look unstoppable. They are the five most valuable listed firms in the world" ("The world's most", 2017, para. 1). Data is the engine of digital technology, and society relies heavily on digital technology to run.

Data are created in volumes almost beyond measure. Domo.com, a leading website in global data calculations, state “By 2020, there will be 40x more bytes of data than there are stars in the observable universe…the numbers are staggering” (Domo.com, 2019, p. 1). Increasingly powerful computers and software are able to analyze these data to generate intelligence. Digital information – in the form of big and wide data - now represents arguably the most valuable commodity in the world. Yet there is a lack of qualified personnel entering the workforce who are equipped to safeguard and steward digital information (Herrod, 2018; Hartman, 2017; HMIC, 2016; VanDerwerken & Ubell, 2011). This skills gap issue is not local or even national, but global in nature (Cobb, 2016; Public Safety Canada, 2018). Information Security is one of the fastest growing field globally (Cobb, 2016; Harkin, Whelan & Chang, 2018), yet Herrod (2018) reports that there are over 300,000 unfilled information security jobs in the United States today. Other authors, such as Hartman (2017) place that number as high as 500,000 job vacancies. Workforce projections for entry-level information security professionals will reach a 1.9 million worker short-fall in 2019 (Suby & Dickson, 2015).

Multiple authors (Cobb, 2016; Dawson & Thomson, 2018; Herrod, 2018) argue that simply focusing on the number of digitally skilled employees is not sufficient, and that the focus should be on the technical and non-technical skills required as well as the way we develop cyber talent. Hoffman, Burley and Toregas (2016) state that even if the information security vacancies were to be filled by graduates, those graduates are not sufficiently prepared to perform the requirements of these roles. Cobb (2016) and Herrod (2018) both identify that the emphasis in information security is on non-technical skills, which implies that non-technical workers can fill these roles. Cobb (2016) finds that “a wide range of people can be trained to become effective cybersecurity professionals” (p.1).

This cyber skills gap has an impact on crime, and therefore on policing and law enforcement. Without adequate defenders, digital assets (such as information and data) are vulnerable to attack (Cobb, 2016; techUK, 2016). The combination of increasing attack surface caused by the digital society and IoT, along with the high valuation of data and a lack of qualified personnel to protect digital information has contributed to the rapid rise of cyber-related crime (Garcia, 2018). Other contributing factors to the growth of cybercrime are jurisdictional challenges in responding to the globalization of crime, the changing paradigms of criminals, the creation of new crime types, and the inadequacy of current legislation.

1.1.2 Cyber-related Crime

The digital society has provided an environment that has allowed crime to flourish (Horsman, 2017), resulting in the popularization of the term "cybercrime", which Cunha, Patel, Moura dos Santos & Celestino (2016) define as "any activities performed outside the law by/with the help of any electronic device" (p.182). Multiple authors report that cybercrime is on the rise (Bossler & Holt, 2012; Cockcroft, Shan-A-Khuda, Schreuders & Trevorrow 2018; Hitchcock et al., 2017), is growing exponentially (Cunha et al., 2016; techUk, 2016), and "is increasing in frequency, scale, sophistication and severity" (Harkin et al., 2018, p.519). New technologies bring new and easy opportunity for criminality (Nuth, 2008). Digital technology has become the subject, object, tools, and symbols of crime (Savona & Mignone, 2004), to the point where cybercrime and cyber threats have become top national security issues (Choo, 2011; Goodman, 2015; Stanciu & Tinca, 2017; Wall & Williams, 2013).

Cybercrime has earned its lofty perch on national security agendas through the costs involved, the harm potential, and the acknowledgement of national infrastructure's dependence on digital technologies (Bilodeau, Lari & Uhrbach, 2019; Goodman, 2015). The literature varies on the actual cost of cybercrime (both real and projected) due to challenges such as underreporting, lack of awareness of victimization, direct and indirect losses, and uncertainty surrounding applicable legislation (Custers, 2012; Goodman, 2015; Holt, 2018). Hitchcock et al.

(2017) found that fraud alone in the United Kingdom costs nearly £200 Billion. Wolf (2013) reports that the FBI has seen its cybercrime caseload increase 1200% over the last few years and Bossler and Holt (2012) estimated the costs of cybercrime to be hundreds of billions of dollars annually. Harkin et al. (2018) report cybercrime costs exceeding one trillion dollars.

Calam (2017) states that “[c]rime itself is changing” (p.4). Digital technologies have enabled criminals to commit traditional crimes in new, technologically enriched ways (Cunha et al., 2016; Brown, 2015; Holt, 2018; MacNeil, 2015). The Internet has allowed traditional crimes to be committed using digital tools (Bossler & Holt, 2012; Calam, 2017; Faith and Bekir, 2015; Hitchcock et al., 2017; Nuth, 2008). A division in crime types has been created, with the literature tending to distinguish *cyber* crimes from *real world* crimes (Bossler & Holt, 2013), where the *cyber*crime is “the online double of their terrestrial counterparts, differing by medium and reach but not by nature” (Stratton et al., 2017, p.22). The Internet, Internet-connected devices, and other technological advancements now allow for traditional crimes to be executed in new and enhanced ways (Wall, May-Chahal & Chistyakova, 2015; Savona & Mignone, 2004).

In addition to facilitating the committing of traditional crimes such as domestic abuse, human trafficking and sexual exploitation of children (Calam, 2017; Hitchcock et al, 2017), digital technologies have created a new frontline of crime (Choo, 2011; Hitchcock et al., 2017) and provides the environment and tools for the creation of entirely new crimes (MacNeil, 2015). Holt (2018) identifies a number of *new* crimes, such as malware, viruses, ransomware, and Denial of Service (DoS) attacks, while the UK House of Commons (2018) lists other crimes including online fraud and sexual exploitation. Stratton et al. (2017) presents an exhaustive list of new crimes, including hacking, financial theft (Brown, 2015), identity fraud, illegal marketplaces that enable the selling of illegal goods and services (Calam, 2017), child sexual exploitation, cyberbullying, cyberstalking (Nuth, 2008), revenge pornography (Hitchcock et al., 2017), information privacy breaches, data theft, digital piracy (Bossler & Holt, 2013), and online sex work. Nuth (2008) adds to this list by also identifying cyber money laundering, cyber vandalism, and hacktivism. These crimes did not exist before the Internet (Calam, 2017).

Craiger et al. (2005) note that in addition to seeing the impact of technology on old and new forms of crime, we are also seeing the creation and proliferation of a new kind of computer criminal (p.5). Digital technologies have not only created new targets, victims, methods of attack, and attack surface, they have also enabled the criminals who would commit crime. The profile of a cyber-criminal, or *hacker*, is no longer that of an anti-social teenager in their parent's basement striving for peer recognition or personal challenge. Rather, cyber criminals are often educated (Horsman, 2017), organized (Brown, 2015), sophisticated, well-funded professionals (Wall & Williams, 2013) who represent a global network of like-minded peers who work together, share knowledge and ideas, revel in successes, validate one another, and market their skills (Goodman, 2015). To wit, we are seeing "the persistent maturation of cyber-criminals" (Wydra & Hartle, 2015, p.224).

The availability of information that enables the digital society also allows for cybercriminals to educate themselves on how to commit digital crime (Horsman, 2017; Wall & Williams, 2013). Information and Communication Technologies (ICT) create an environment where anyone can become a criminal (Savona & Mignone, 2004), to the point where Nuth (2008) finds that technology draws people to commit crime who might not normally do so (p.444). Public Safety Canada (2018) lists multiple types of cybercriminals, including hackers, insiders, criminal networks, nation states, terrorist organizations, and state sponsored actors. As the cybercriminal has evolved, so too has their motivation for committing crime. According to Choo (2011), cybercrime is primarily motivated by financial gain, and both organized crime and nation state sponsored malicious cyber activity are growing (Goodman, 2015; Public Safety

Canada, 2018; Wall & Williams, 2013).

Perhaps the most concerning growth area of cyber criminality emerges when seen through the lens of terrorism. Several authors, (Bossler & Holt, 2012; Calam, 2017; Heal, Cowper & Olligschlaeger, 2006; Horsman, 2017; Nuth, 2008) have identified the role of digital technology as an enabler of terrorism. This may come in the form of using digital technologies such as social media to identify and recruit followers, communicate targets, organize attacks (Choo, 2011), and crypto currencies to receive payment (Goodman, 2015). Silberglitt et al., (2015) report the use of the non-public web, or *Dark Web*, as the forum for cyber criminals and terrorists to buy and sell weapons, drugs, and malicious software.

The dark web, crypto currencies, and cyberterrorism are just a few of the new frontiers for digital crime and police, whose role in society is to prevent and respond to crime, are not prepared to address crime in these spaces (Cockcroft et al., 2018; Hitchcock et al., 2017; UK House of Commons, 2018; Silberglitt et al., 2015). As Blandford (2014) points out, policing now occurs in technologically intense environments, a sentiment echoed by Council of Canadian Academies (2014), who describe these environments as ever-changing and complex. Bossler and Holt (2013) believe that law enforcement need to have a greater role in responding to cyber-related offences. However, the police are hampered in their efforts by several factors, including issues with jurisdiction, legislation, and digital evidence.

1.1.3 Jurisdiction Challenges and the Globalization of Crime

Policing must now be carried out in a borderless community (Calam, 2017; Choo, 2011). Criminals are now in a position to execute crime on a local, national, and even global scale through the use of digital technologies (Brown, 2015; Horsman, 2017; Holt, 2018; Nuth, 2008). According to Bossler and Holt (2012), criminals are no longer restricted by geography and physical access. Cybercrime is borderless, often distant, and committed from anywhere in the world (Wall et al., 2015). Territorial space is no longer a hurdle (Nuth, 2008) – in part because existing legislation and legal frameworks were not designed to support cross-border and international crime (Goodison et al., 2015; Holt, 2018). Another element of cybercrime that presents challenges to police can be found in how digital technologies enable and support the anonymity of the offender(s) (Bossler & Holt, 2012; Wall et al., 2015). The obfuscation of identity and geography, combined with outdated or unclear legal systems present real challenges to policing in a digital world (HMIC, 2015; Nuth, 2008).

1.1.4 Issues with Legislation

Brown (2015) and Wall et al. (2015) both identified that legal loopholes facilitate acts of cybercrime, resulting in many investigations being ignored, mishandled, or dropped by the police and prosecution. Brown (2015) further states that cybercrime "can be technically complex and legally intricate" (p.56). Other authors (Custers, 2012; Horsman, 2017; Stratton et al., 2017), found that there were numerous legal obstacles that negatively impacted police response to digital crimes. Holt (2018) identified gaps in the legal system that are being exploited by cybercriminals. Outdated, ineffective, and inefficient legislation presents a challenge to law enforcement, according to Savona and Mignone (2004) who identified a lack of clarity in legal definitions surrounding digital crime as a primary issue – a finding supported by Custers (2012).

Wall et al. (2015) finds challenges posed by current legislation include a lack of cyber-specific investigative powers, powers of search and seizure of digital evidence (Craiger et al., 2005), authority to enter electronic networks, and power to ensure preservation of data. Holt (2018) found that legislation does not allow for sufficiently severe penalties for cyber offences. Further, a lack of consistency in laws at all levels of government are a challenge (Brown, 2015), and current laws are in need of expansion and revision in order to apply to the current crime landscape (Custers, 2012). Other authors (Calam, 2017; Nuth, 2008; Wexler, 2012) reports that legislative change is slow and uncertain, which contrasts the rapid rate of technological change. Nuth (2008) states, “The problem is that ICTs change so fast that sometimes the law cannot cope with their development. The law-making process is usually long” (p.444). Nuth also identifies that governments may be discouraged from updating laws due to a concern over currency by the time the law is passed.

Gogolin (2010) does not believe legislation has the option of standing still, and expresses concern that the legal system is at risk of collapse if it does not adapt to digital crime. One area of growth that is desperately required is in the area of international legislation, treaties, and agreements (Calam, 2017; Horsman, 2017; Nuth, 2008). Attempts have been made, such as the Council of Europe Convention on Cybercrime (also called the Budapest Convention) in 2001 and revised in 2003. The United Nations attempted similar legislation in 2001 and 2002. The European Union Commission released similar legislation in 2007, and the recent General Data Protection Regulation (GDPR) was enacted in 2018. Canada is a signatory on many of these documents, and the United States have modified many of their own laws to reflect the same principles (Goodison et al., 2015), most notably the USA PATRIOT ACT of 2001 that was created in response to the 9/11 attacks (Goodman, 2015).

Public Safety Canada (2018) expressed that legislation has too narrow a view of cyber-related crime. Several authors (Bossler & Holt, 2012; Custers, 2012; Wexler, 2012) report that unclear legislation has resulted in police officers being unsure of which laws apply to digital evidence. Holt (2018) concurs, stating that legislation needs to be clearer and easier for non-technical officers to follow. Legislation is needed that empowers police to compel the production of digital evidence (Goodison et al., 2015). It seems digital evidence represent the nexus of legislation and cybercrime.

1.1.5 Digital Evidence

One area where legislation has been particularly challenged surrounds the creation, ownership, identification, collection, processing, and presentation of digital evidence (Cunha et al., 2016; Goodison et al., 2015; Wexler, 2012). Craiger et al., (2005) use the SWGDE definition of digital evidence composed in 1999, which defines digital evidence as "Information of probative value stored or transmitted in binary form" (p.5). Most police departments now recognize the prevalence of digital evidence (Bossler & Holt, 2013; Sturgeon, 2015). Unlike the crimes themselves, which are often traditional offences facilitated by digital technology, digital evidence and physical evidence are vastly different (Goodison et al., 2015) requiring a different set of skills of police officers and investigators (Wall et al., 2015). The National Institute of Justice (2008) produced a document intended to assist police officers in recognizing, seizing, documenting, handling, packaging, and transporting digital evidence, but to date there is no formal legislation in the US that offers this level of guidance or reference (Bossler & Holt, 2012).

The digital society and cybercrime have changed the nature of evidence itself. Prior to the widespread adoption and use of the Internet, most crimes required the physical presence of the perpetrator, resulting in physical evidence that could be collected and analyzed. Evidence consisted of material objects like fingerprints, blood, footprints, and fibers. Digital evidence is non-tangible, and therefore traditional evidentiary practices do not apply.

Some key themes emerged from the literature when researching digital evidence. Among them were the increasing number of cases involving digital evidence (Hitchcock et al., 2016; Sturgeon, 2015), the importance of digital evidence (Cunha et al., 2016), and the sources of digital evidence (Craiger et al., 2005; Goodison et al., 2015; Hanna, 2016; Wydra & Hartle, 2015), but the dominant theme in the literature was the way police personnel identify, preserve, and handle digital evidence (Calam, 2017; Brown, 2015; Holt, 2018; Horsman, 2017; MacNeil, 2015). Digital evidence *triage* was a term that arose in the literature. An offshoot of digital forensics triage, it is the process police officers follow when collecting, transporting, analyzing, and prioritizing digital evidence from a crime or investigation in order to maintain the integrity of the evidence (Hitchcock et al., 2016). The need for frontline police officers to be taught how to conduct digital triage was prominent in the literature, with multiple authors finding that this skillset was either not being taught to frontline officers or was not identified as the responsibility of the frontline first responder (Goodison et al., 2015; Wolf, 2013). Consequences of a lack of evidence triaging included the loss of evidence (Horsman, 2017), the loss of integrity (Wydra & Hartle, 2015), or compromised investigations resulting in cases being dropped (Brown, 2015; Goodison et al., 2015).

The first stage in the digital triage process is the recognition and identification of the presence of digital evidence (Hitchcock et al., 2017), a step that untrained officers will miss (Cunha et al., 2016). The sources of digital evidence are sometimes obvious, such as a computer or smartphone, but are often less so to the untrained first responder (Goodison et al., 2015; Horsman, 2017; Wydra & Hartle, 2015). Other sources of digital evidence include network connections, mobiles, IoT sensors and software logs (Hanna, 2016), websites and web browsing history, online instant message boards and chat rooms (Goodison et al., 2015), pictures, documents, audio and video files, and server logs (Craiger et al., 2005). Other surprising sources of digital evidence include vehicle GPS (Wexler, 2012), personal activity trackers and smart watches, video surveillance cameras, social media communications, bank records, gaming consoles, and smart home devices including video doorbells (Goodman, 2015; Scanlan, 2011). As Goodison et al., (2015) state, “Modern devices can serve as huge repositories of personal information” (p.1).

1.1.6 Nearly Every Crime Has a Digital Trail

Another prominent theme in the literature that relates to digital evidence is that the literature suggests there is a digital element to almost every crime. Harkin et al. (2018) state, “Every crime has a technology-enabled component behind it” (p.530). Calam (2017) states “Almost every crime now has a digital footprint” (p.12). These findings echo those of previous researchers (Bossler & Holt, 2012; 2013; Gogolin, 2010; HMIC; 2015; MacNeil, 2015). HMIC (2015) define the term *digital footprint* as “the trail of data that is left behind by users of digital services” (p.7). Other authors report more subdued estimates of the prevalence of digital evidence, reporting that a digital footprint is present in the majority of criminal offences (Hitchcock et al., 2017; Horsman, 2017). Savona and Mignone (2004) summarize the ubiquity of digital evidence, stating that “computer-related crimes are by definition the largest category of misconducts” (p.10).

The volume of digital evidence, combined with a shortage of qualified police personnel to process it, has resulted in severe backlogs in the criminal justice system (James & Gladyshev, 2015; Goodison et al., 2015; Gogolin, 2010). Gogolin (2010) found these backlogs are approaching two years. Similarly, Hitchcock et al. (2016) found that there were significant delays in police departments between the time the investigators submit evidence for analysis and the completion of that analysis, which left investigators bereft of information that could lead to the identification or prosecution of offenders. Cunha et al. (2016) found that a lack of clearly defined roles resulted in digital forensics experts attending the crime scene and replicating the work already done by first responders. This unnecessary drain on these specialized resources also contributed to delays in digital evidence processing (Cunha et al., 2016; Horsman, 2017).

In Canada, the Charter of Rights and Freedoms, Section 11(b) outlines the right of a person charged with a crime to be tried within a reasonable time. Court rulings, such as R. v.

Jordan (2016) have interpreted this time period to be 18 months. Since that ruling, nearly 800 court cases in Canada have been dismissed due to delays (Russel, 2019), but it is unclear as to how many of those dropped cases experienced delays in the processing of digital evidence. The public hears of these delays and looks to place blame at all levels of the Canadian criminal justice system – including the police services (Hitchcock et al., 2016). Public trust in the police is essential to the police being able to exercise their duties (Koksal, 2009).

1.1.7 Summary

At the present time, policing, like many other areas of society, finds that the pace of digital technology change threatens to outpace the skills of its current workforce. Cobb (2016) reports that the need for more cyber-skilled employees across all sectors is a global issue. At the same time, digital crime is increasingly impacting the lives of citizens and organizations, and there is pressure to upskill quickly and efficiently. The ubiquity of digital devices, tools, and technologies being used by private business, public sector services, and members of the general public, along with the increasing data in all its forms, has resulted in their being a digital element to every crime (Calam, 2017; Herrod, 2018; Horsman, 2017). Canadian police organizations face a number of challenges as they are expected to operate in an evolving crime landscape while concurrently adapting to organizational changes brought about by the adoption, implementation and use of these same technologies by police services. The technology skills of police officers haven been identified as being of paramount importance to the future of law enforcement (Bossler & Holt, 2012).

Until recently, the prevention and response to the digital elements of law enforcement have been the purview of specialist police officers, as encountering a digital crime was a rare occurrence for a frontline officer (Harkin et al., 2018). As citizens, organizations, and public services increasingly turn to ICT devices and data, the volume, variety, and velocity of digital crime has increased. Frontline police officers are likely to encounter digital evidence on any given call for service.

Not only is it important for police officers to have the skills to respond to cybercrimes and digital evidence, they also need to be able to function with competence in the online world. The internet, social media, and other network technologies have created a forum where traditional crimes can now occur in the virtual environment. This environment has also enabled the creation of new crime types that would not be possible in the physical space. In short, public safety requires police personnel at all levels to possess ICT skills and literacies in order to fulfill their role as the defenders of society's safety (Tanner & Meyer, 2015). To date there has been little research measuring the competencies required of frontline police officers as they relate to digital literacy and technology use.

Police education and training are at the core of the development of skills and competencies, and similarly, digital competencies. Police training in Canada falls into two broad categories: recruit training and in-service training. Basic recruit training is the last formal education step before a police recruit becomes a police officer (Jewell, 2013). Recruit training is designed to provide the incumbent officer with the skills, knowledge, and competencies required for their first day on the job, while in-service training is intended to update that knowledge and those skills to align with current police practices.

This study examines the perceptions of training officers at police training academies across Canada. The participants' roles as police trainers position them as individuals who are uniquely suited to discuss the ways that prospective police officers are being trained to provide police services to their communities.

1.2 Roadmap

This study employs a theoretical framework that comprises of the Unified Theory of

Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis & Davis, 2003) combined with a grounded theory approach. This theoretical model considers the role of digital literacy in technology adoption and use in a policing context. The theoretical framework is outlined in detail in Chapter 2, the literature review. In Chapter 2, the academic literature relevant to this study is synthesized and findings are reported using a thematic analysis. Chapter 2 also lists the primary and secondary research questions that guide this study.

Chapter 3 is the methodology chapter which outlines key research decisions, processes, and theories, including sections on participant selection, data collection tools, research procedures, and consent. Chapter 4 outlines the five high-level themes that emerged from the analysis of the qualitative interview data. These data indicate that academies face many challenges to the incorporation of digital technologies into the basic recruit training of police officers. Chapter 5 is the discussion and conclusion chapter which examines the findings of both the literature review and the qualitative interviews with respect to their ability to answer the research questions. The theoretical framework is revisited in light of the findings. Implications of the findings are also discussed, along with limitations of the study and recommendations for future research in the topic areas.

Chapter 2: Literature Review

2.0 Overview

The importance of training in police practice cannot be overstated (Stanislas, 2014). In Canada, police training requirements are determined by each individual province. Training standards vary from province to province (Wyatt & Bell, 2014). A police officer in one province is not automatically recognized as an officer in another province (Interprovincial Policing Act, 2009). The same is true for police officer hiring practices, where some provinces have standardized pre-employment training and others train post-hire (Wyatt & Bell, 2014, p. 74). Similarly, some provinces conduct post-hire training at a provincially-mandated facility, whereas other provinces do not. While this approach to police training allows for flexibility and customization to the unique needs of each province, it presents challenges in establishing minimum training outcomes and competencies (Wyatt & Bell, 2014), reflecting a centuries old model of provincial training standards (Marquis, 1994).

Police organizations around the globe are facing a virtual uphill battle to meet the pace and depth of changes required to train officers for a digital era. The literature review identifies a number of gaps and problem areas that emerge when examining the role of digital technologies in training and practices. Prominent themes in the literature include the identification and persistence of a global cyber-skills gap; the growing problems of cybercrime and cyber terrorism especially in relation to police organizations’ abilities to prevent and respond to these crime types; the resulting erosion of public trust in the police; police handling of digital evidence; technology adoption rates of officers; aligning current police training with the evolution of frontline police officers’ responsibilities; the need for digital literacy skills and competencies among police officers; training challenges posed by a new generation of police recruits; and the use of emerging technologies by both the police and criminals.

2.1 Policing the Digital Society

"Technology, more than any other phenomena, has been the driving force behind change and advancement in policing" (White & Escobar, 2008, p.128). The link between technological advancement and police practice has a long history. For example, the invention of the automobile forced police services to move to adopt vehicles and embrace mobile response – a model that persists to this day (Koper et al., 2009). The realization that a person's fingerprints and DNA were unique changed the way police processed crime scenes – paving the way for the adoption of new forensic tools. Multiple authors have expressed the strong link between technology and law enforcement (Calam, 2017; Faith & Bekir, 2015; Nuth, 2008; Wall et al., 2015; White & Escobar, 2008). Other authors have similarly identified a strong link between technology advancements and crime (Custers, 2012; Savona & Mignone, 2004; Wexler, 2012), with Nuth (2008) claiming that the evolution of digital technology has forced police into a "crime technology race" (p.443) where criminals and police both seek the technology to thwart the other side.

Silberglitt et al. (2015) present the theory that the police, society, and technology advance together and in response to each other, creating a cyclical relationship, where society presents demand that technology evolves to meet, which drives changes in police practice. Faith and Bekir (2015) found that technological developments improved police productivity. An example of a society-driven technological development can be found in the terrorist attacks on the United States in September, 2001 (Goodman, 2015). This societal event fundamentally changed policing by adding responsibilities to frontline officers (Wolf, 2013).

The theme of transformational change in policing brought on by digital technology is prevalent in the literature, with some authors, such as Council of Canadian Academies (2014) calling for police to undergo a transformational change that is urgently needed. Wexler (2012) points out that a fundamental transformation of policing has already begun. Goodison et al. (2015) address the dynamic relationship between policing and technology by stating that "[l]aw enforcement must not only *be* up to date, it must *stay* up to date" (p.7). Wydra and Hartle (2015) state that emerging new technologies such as IoT, the proliferation of smart devices, and surveillance systems have "forced policing into the 21st century" (p.224). Their use of the word "force" implies a lack of choice in terms of police adaptation to technology.

The relationship between policing and technology is complicated and controversial (Heal at al., 2006). Faith and Bekir (2015) state, "Traditionally, law enforcement agencies have had an unfriendly relationship with technology" (p.294). Grabosky and Smith (2017) state that criminals are quicker to take advantage of new advancements in technology than the police, who are more restricted in their ability to adapt to technology changes. Blandford (2014) reports that police leaders play a critical role in law enforcement's ability to adopt and adapt to new technologies. Calam (2017) concurs, stating that regardless of the challenges involved, police must keep pace with changes in society.

2.1.1 Public Expectations of Police

The literature reports an issue with the public's trust of police, in part due to the crisis of confidence that arises from the public's expectations for law enforcement's response to cyber-enabled crime (Holt, 2018; Sturgeon, 2015). Wall et al. (2015) express concern that the fear of cybercrime is so high that expectations of police response and involvement in cybercrime are not realistic and are difficult to meet.

The expectations of the public for their police services are changing rapidly (HMIC, 2016), with the public placing increasing demands on police services to address digital crime. One such expectation is for the police to be competent using digital technologies (Blandford, 2014; Faith & Bekir, 2015; HMIC, 2016; Koksal, 2009; Silberglitt et al., 2015). Another was that the police respond appropriately to cyber-enabled crime (Cockcroft et al., 2018; Faith & Bekir, 2015; Holt, 2018; Horsman, 2017; Koksal, 2009). The public expects police to provide the same level of service in dealing with online crime as they do with real world crime (Calam, 2017; Choo, 2011; HMIC, 2015). Calam (2017) finds that smaller agencies are expected to provide the same level of response to cybercrime as larger cities despite having fewer resources.

Koper et al., (2009) found that police services who effectively respond to technology-based crimes experience improved citizen satisfaction, a finding supported by Koksal (2009). HMIC (2016) drew parallels between the level of confidence the public had in the police to the amount of crime being reported to police – specifically with respect to digital crime. Calam (2017) reports that public trust, satisfaction, and confidence in police agencies increases as their digital experiences improve. However, the UK House of Commons (2018) found that "Policing is struggling to cope in the face of changing and rising crimes…Without significant reform and investment, communities will be increasingly let down" (p.6).

2.1.2 Police Budgets

One such challenge was that of police funding and budgets. A lack of funding and resources was mentioned prominently in the literature reviewed. In general, police budgets have not kept up with demands for policing in a digital society (Brown, 2015; Cockcroft et al., 2018; Goodison et al., 2015; Harkin et al., 2018). This underfunding has risen at a time when the cost of policing is rising (Council of Canadian Academies, 2014), resulting in an environment where police are expected to maintain increasing service levels despite decreasing resources (Custers, 2012; Hitchcock et al., 2016; Wexler, 2012). The budget and resources allocated to fighting digital crime are on the decline despite the rising number of cyber-enabled crime (Brown, 2015; Cockcroft et al., 2018; Heal et al., 2015; UK House of Commons, 2018; Nuth, 2008).

In some nations, such as the United Kingdom, police funding saw a dramatic drop, declining by nearly 20% between 2011 and 2016 (HMIC, 2016). Smaller police services are especially vulnerable to budget cuts (Craiger et al, 2005; Harkin et al., 2018). Many services are responding to these cuts by reducing personnel or services (Hitchcock et al., 2016; Holt, 2018). Interestingly, police spending on IT has increased (Hollywood, Boon, Silberglitt, Chow & Jackson, 2015). The emphasis on IT spending is representative of a shift in priorities from traditional policing to policing using digital technology (Lum, Koper & Willis, 2017).

2.2 Police Training in Canada

Current police training is not designed or prepared to meet the needs of a digital society (Mugford, Corey & Bennell, 2013; Timpf, 2014). Cockcroft et al. (2018) found that the most prevalent theme of need across their needs assessment was the issue of training and knowledge – specifically, the theme of training in digital technologies. Many authors (Cockcroft et al., 2018; Hitchcock et al., 2017; Koksal, 2009) find that technological competencies are not recognized in police training. White and Escobar (2008) found that police agencies need to enhance current training curriculum in order to ensure that officers have the skills and knowledge to use digital technologies effectively. A recent study by HMIC took the position that ICT and new technology skills need to be core to police training and day-to-day work (HMIC, 2016).

2.2.1 Traditional Training Models persist

Despite a growing body of literature calling for police to embrace technology training, many police services continue to train officers in traditional ways, relying on practical skills and craft-based curriculum (Roberts, Herrington, Jones, White & Day, 2016; Timpf, 2014). Police services have been organized for an older reality (Council of Canadian Academies, 2014), utilizing an “acquisition and transfer” approach that is the standard paradigm in police training (Cockcroft et al., 2018). “Often, police training expends significant time and effort to teach disciplines and techniques, such as physical skills, that are seldom encountered or used” (Timpf, 2014, p. 9). Enea (2010) and Stokes (2010) had similar findings, indicating police training over-emphasizes traditional skills and a behaviorist approach that is modeled after a 40-year-old paradigm where officers are blank vessel waiting to receive knowledge.

The theme of the behaviorist model as the dominant training approach was prominent in the literature. Enea (2010), Schafer and Boyd, (2007) and Timpf (2014) found that policing continues to use traditional behaviorist methods to train police officers, and that this model was consistent with military training. Several authors (Deverge, 2016; Schafer & Boyd, 2007; Timpf, 2014) found that the paramilitary model persists in most police training academies. The authors state that police still focus too much on the technical and mechanical aspects of policing, where training emphasis is on the trainee’s effort and compliance to rules. This model emphasizes punishment for undesired outcomes and praise for positive results, and is a contradiction to current police trends (Timpf, 2014).

Timpf (2014) indicates that a paramilitary training approach does not prepare officers to function in a partnership with the community and can actually create conflict between the police and the public they serve. Schafer and Boyd (2007) found that behaviorist training creates a paradox whereby police are trained to follow orders and procedures in a punitive and paramilitary environment, yet are expected to be creative and innovative problem solvers on the street. Timpf (2014) expands on these findings, reporting that current police training “does not encourage spontaneity or unscripted outcomes in the training environment” (Timpf, 2014, p. 9), and that “the present prevailing philosophy of training is not conducive to advanced modern police thought on crime prevention and intervention” (Timpf, 2014, p. 20). Willis (2010) identifies the risk that current traditional training approaches produce “cookie cutter” police officers.

Twelve years ago, Schafer and Boyd (2007) predicted a shift in pedagogy was coming in policing training. The authors predicted by the year 2020 police training would be learner-centered, less militaristic, and focused on critical thinking and problem solving. To date, police training practices in Canada and the U.S. has not realized that vision. Academies continue to use a passive training model relying on the traditional, instructor-centered approach to deliver the content in a lecture-based format (Timpf, 2014). There has been some departure from this approach, for example with non-digital simulations, but there remains a heavy dependence on the lecture format with "a strong reliance on objective examination as the preferred mode of assessment" (Schafer & Boyd, 2007, p. 383). However, multiple authors (Mugford et al., 2013; Schafer & Boyd, 2007; Timpf, 2014) have found that training instructors are forced to use lecture-based teaching due to the volume of content to cover and limited training time.

The issue is not ignorance on behalf of the instructors, as Mugford et al. (2013) found that police trainers are "generally aware of adult learning principles" but are not provided with specific training strategies which support the adult learning paradigm (p. 314). Similarly, Enea (2010) reports that training instructors have little latitude for modifying existing curriculum. In the vein of instructor knowledge and qualifications, several authors found that training officers were generally selected based on their practical experience and not on their teaching skills or the possession of teaching certifications (Etter & Griffin, 2011; Ramshaw & Soppitt, 2018; Schafer & Boyd, 2007). Despite the emerging interest in adult learning principles among police trainers, instructors continue to "teach as they were taught" (Schafer & Boyd, 2007, p. 399).

2.2.2 E-Learning, Andragogy, and Problem-Based Learning

There is evidence of the kind of growth Schafer and Boyd (2007) predicted, specifically in the areas of e-learning, andragogy, and problem-based learning. E-learning has become a common way of delivering courses to police officers (Mugford et al., 2013, Schafer & Boyd, 2007), especially with respect to computer-based in-service training (Council of Canadian

Academies, 2014; Mugford et al., 2013). However, e-learning has been criticized as being underdeveloped (Monett & Elkina, 2015), ineffective, and unpopular among officers (Cockcroft et al., 2018), and involves considerable expense (Giovengo, 2017). Cockcroft et al. (2018) suggested that e-learning should not stand alone as a teaching method, but rather would be better used to impart pre-course knowledge or refresher training. The preferred police education models appear to be the ones that are interactive, learner-centered, and problem based.

Andragogy is a theory of adult learning proposed by Malcolm Knowles in 1990 (Knowles, Holton & Swanson, 2005) that emphasized six learning characteristics of adults, among them, the need to root content in the learner's past experience, to make the content directly relevant to the learner, that adults need to be respected as learners, and that adults are self-directed and internally motivated. This is a diversion from traditional police training pedagogy (Etter & Griffin, 2011; Sturgeon, 2015). Andragogy is being used in some Canadian police academies (Deverge, 2016). Timpf (2014) identified the need to "consider the life experiences that officers bring to training and how those experiences can benefit their learning and the learning of other students" (p. 9), and that adult learning theory lends itself to the complex police training environment. Mugford et al. (2013) believe training initiatives must be consistent with adult learning theory as the learner-centered approach allows for many different learning styles to be accommodated in the training environment. Similarly, Timpf (2014) states that adult learning theory is ideal for police education in that it is collaborative and participatory. Schafer and Boyd (2007) recognize andragogy as an ideal approach to teaching officers as it allows recruits to be dynamic actors in the learning process.

Problem-based learning (PBL) is an approach to police education that has been gaining traction of late (Lettic, 2015), as police officers are increasingly being asked to be problem solvers in the field (Gresham, 2016; King Stargel, 2010; Lettic, 2015; Mugford et al., 2013).

Multiple authors identify that frontline officers are expected to analyze problems and propose solutions (King Stargel, 2010; Lettic, 2015). Timpf (2014) found that officers cannot perform adequately unless their training is rooted in authentic problems and context, and that PBL needs to be incorporated into police training at all levels in order to “prepare officers for the complex job requirements of modern policing” (p.1). Mugford et al. (2013) directly linked PBL with the development of higher order thinking skills.

2.3 Police Training vs Police Education

The literature discussed the need to delineate between training and education. Despite being distinctly different, both are identified as complimentary processes to police learning (Schafer & Boyd, 2007), but are often used as synonymous concepts (Roberts et al., 2016). Training is defined as the systematic building of particular skills, knowledge, and abilities that transfer directly to the worksite (Schafer & Boyd, 2007). Giovengo (2017) identifies these skills as primarily “shooting, driving, and handcuffing” and other “technical expertise” (p. 7). Training focuses on gaining the skills needed to accomplish the immediate tasks and goals of police operations, compared to education’s role in developing the ability to “conceptualize and expand the theoretical and analytical learning process” (Roberts et al., 2016, p. 29). Deverge (2016) and Roberts et al. (2016) found that the primary purpose of police education must be to deliver learning and thinking skills as opposed to focusing on technical expertise.

Police education is defined in the literature as emphasizing the cognitive abilities of the officer, specifically creativity, problem solving, analysis, and evaluation (Mugford et al., 2013; Willis, 2010). Consideration of Bloom’s Taxonomy of educational objectives is crucial when developing police training programs – frontline officers are expected to perform at the highest levels of Bloom’s taxonomy (Mugford et al., 2013). Timpf (2014) concurs in his research, which identified that critical thinking and higher order thinking skills are a requirement for frontline officers, who are increasingly being asked to act autonomously. Taylor, Fritsch & Liederbach (2014) likewise found the critical need for officers to be able to analyze and understand problems. Schafer and Boyd (2007) recognized the role of higher order thinking given the emphasis on outcomes-based policing insofar as officers needing to know how to solve problems in a way that maximizes benefit and minimizes risk.

Policing involves problem solving, analysis, research, and critical thinking, and that officers are expected to be innovative and creative (Enea, 2010; Timpf, 2014). It has also been argued that education is more transferable than job-specific technical training (Timpf, 2014) Education and training fill different roles in police practice (Schafer & Boyd, 2007), and that training objectives are more easily measured and therefore more likely to receive recognition (Roberts et al., 2016). Learning and thinking skills must be recognized, valued, and rewarded by police leaders (Roberts et al., 2016), yet police agencies generally do not actively encourage education – specifically formal post-secondary education – once an employee is hired (Paoline, Terrill & Rossler, 2019; Schafer & Boyd, 2007).

2.3.1 Role of Higher Education in Policing

Deverge (2016) found that higher education adds value to police training as it reinforces the development of critical thinking skills, finding that recruits who entered the academy having already completed a college or university program performed better in cognitively oriented courses. Other authors (Carter, 2014; Paterson, 2011; Rydberg & Terrill, 2010) have linked higher education with reduced use-of-force incidents and police misconduct, and shootings. However, most police agencies do not require post-secondary certifications prior to employment (Carter, 2014; Paoline et al., 2015), many police organizations require degrees in order to be considered for promotion or police leadership roles (Carter, 2014; Hilal, Densley & Zhao, 2013; Rydberg & Terrill, 2010). Multiple authors (Paoline et al., 2015, Schafer & Boyd, 2007) found that most officers who possess degrees earned them prior to employment as a police officer.

Despite the growing body of research, the specific role and impact of higher education in policing remains unclear (Carter, 2014; Paoline et al., 2015, Paterson, 2011; Rydberg & Terrill, 2010). Some authors (Cockcroft et al., 2018; Sturgeon, 2015) linked higher education with officers who were more successful using digital technologies and tools, however Craiger et al. (2005) found that college and university education was not common among cyber-specialist staff. Stokes (2010) expands on that theme, stating that specialist training should be offered by universities in the form of highly targeted graduate programs. In terms of cybercrime and digital policing, Hitchcock et al. (2017) believes universities should offer online digital crime courses, and that the UK College of Policing is considering the creation of their own digital academy. Universities are cautioned, however, to avoid becoming “degree mills” in order to meet these growing areas of need for police education (Schafer & Boyd, 2007, p. 394).

2.3.2 Need for cyber training

The development of digital skills needs to be a critical priority for law enforcement (Custers, 2012; Sturgeon, 2015). There are many examples in the literature of the presence of a cyber-skills gap both internally and between departments at all levels of law enforcement (Koper et al., 2009). Wolf (2013) found that there were even gaps in the competency levels of officers performing similar duties. Other authors (Koksal, 2009; Sanders & Hannem, 2012) found that there was little consistency in officers’ levels of technology competence. Harkin et al. (2018) found that cyber expertise was hard to acquire, and that the skills from other specialized units were less transferable to the cyber realm, which may account for the disparity in competency levels even within specialized cyber units. This contradicted a finding by Stokes (2010) who indicated that prior technical skill was not an important indicator of digital training. The levels of cyber knowledge, skills, and abilities within policing may differ, yet there was consensus in the literature reviewed that all officers, regardless of rank or experience, needed cyber training at some level.

Cockcroft et al. (2018) state there is a "need for a generic level of cyber knowledge to be distributed throughout all roles within the [police] organization" (p. 17). This sentiment was prevalent in the literature as multiple authors (Cunha et al., 2016; Holt & Bossler, 2012a; Hitchcock et al., 2017) state the need for all officers and police staff to have the rudimentary skills to use operational technology. Specific groups identified as being in need of cyber training included administrators and police leaders (Harkin et al., 2018; Holt & Bossler, 2012a), prosecutors and court officials (Holt & Bossler, 2012a), and frontline officers (Holt & Bossler, 2012b). Given that officers are dispatched to calls based on availability, there is a pressing need for baseline cyber knowledge common to all first responders (Hold & Bossler, 2012b).

The need for cyber training was not limited to existing personnel, as several authors indicated the importance of digital training being present both at the academy and post-hire (Flory, 2016; Cunha et al., 2016; Deverge, 2016; HMIC, 2015). Flory (2016) found that in many US departments digital crime is not covered with any initial or in-service training. A theme that emerged was the need for both initial cyber training at the academy followed by regular, more advanced training being offered to as in-service training – especially given the short lifespan of cyber expertise and the rate of technology change (Harkin et al., 2018; HMIC, 2015).

Goodison et al. (2015) found that digital evidence handling and preservation at the academy level would result in more appropriate initial response by frontline officers. Deverge (2016) found that pre-employment education in the cyber realm can help address the expanding police role, and that post-hire models where academy training is a recruit's first contact with digital crime is at a disadvantage due to the short time allotted for recruit training and the heavy cognitive load that academies place on students (Mugford et al., 2013). In-service approaches to cyber training are more popular with most departments, however these offerings tend to focus heavily on the transmission of new information, such as changes in legislation and skills-renewal exercises (Schafer & Boyd, 2007). The literature also presented several examples of the types of cyber skills that needed to be developed in police learners.

Of all cyber skills mentioned, digital evidence was particularly prevalent in the literature, with multiple authors reporting a need for training on digital evidence recognition, handling, and preservation being critical to both police recruit training and in-service offerings (Cockcroft et al., 2018; Cunha et al., 2016; Flory, 2016; Goodison et al., 2015; HMIC, 2015). In particular, digital devices such as smartphones and personal electronic devices were identified as a source of evidence that is often missed or damaged by the untrained first responder (Cunha et al., 2016; Hitchcock et al., 2016, HMIC, 2015). Digital evidence collection is such a pertinent issue to first responders that the National Institute of Justice (NIJ) created a guide entitled "*Electronic Crime Scene Investigation: A Guide for First Responders*" (NIJ, 2008). Officers also needed increased training on which crimes are likely to have a digital element, as well as how to appropriately respond to victims of cybercrimes (Bossler & Holt, 2012; Stokes, 2010). Other topics identified in the literature included the need for social media training (Koper et al., 2014; Wexler, 2012) and training on video surveillance (Strom, 2017). The need for cyber training was evident, but less clear was the level to which officers needed to be cyber competent, which introduced the topic of specialization and specialized cybercrime units.

2.3.3 The Specialization Debate

The topic of specialized cybercrime units, including their role, their training, their value, and their challenges, was prominent in the literature. Specialized cybercrime units are the current, prevailing model in policing, and are becoming increasingly common (Harkin et al., 2018). Some authors argued against frontline officers having any role in responding to cybercrime (Council of Canadian Academies, 2014; Stokes, 2010), in favor of handling crime scenes, interviewing witnesses and other first responder duties. Other authors valued the specialized units but believed they needed to be part of a tiered response to cybercrime (Cockcroft et al., 2018; Hitchcock et al., 2016; Sturgeon, 2015). There is a need "for upskilling officer outside of the specialist cyber-crime squad and recognizing that technology-enabled crime is a police-wide problem" (Harkin et al., 2018, p. 529).

A tiered response would lighten the load on currently understaffed and overworked cyber units (Hitchcock et al., 2016; Stokes, 2010). Stokes (2010) posits that specialization saves police organizations millions in redundant training costs, delivers higher expertise, and allows skilled personnel to develop and follow individualized career paths. Stokes fails to account for the body of literature that specialized cyber units are underfunded (Bossler & Holt, 2012; Hitchcock et al., 2016; Hunton, 2011; Goodison et al., 2015) too expensive for smaller services to maintain (Craiger et al., 2005; Koksal, 2009), that there is a lack of skilled or trained workforce to fill the required number of positions (Cunha et al., 2016; Hitchcock et al., 2016; Harkin et al., 2018; Goodison et al., 2015), have not been proven to impact crime clearance rates (Koksal, 2009), and often result in duplication of investigations (Cunha et al., 2016).

Harkin et al. (2018) found that cybercrime units were a low institutional priority, while Schafer and Boyd (2007) report that cybercrime units result in differential police response in areas that had no such units. When examined through the lens of training, Cunha et al. (2016) found that organizations who trained officers to be cyber specialist were more successful than organization who trained specialists to be police officers, and that non-police specialists lacked the context required to understand their role in the criminal justice process. HMIC (2015) state that cybercrime should not be the exclusive purview of specialized units, stating, "It is no longer appropriate, if it ever were, for police services to consider the investigation of digital crime to be the preserve of those with specialist knowledge" (p. 8).

Multiple authors cited the issue of a lack of training standards or certifications for cyber units (Craiger et al., 2005; Sturgeon 2015). With Stokes (2010) advocating that cyber specialist should not be required to attend police academy and be forced to complete traditional police training, which includes "the numerous hours normally dedicated to physical fitness, defensive tactics and firearms" (p. 4). One of the reasons that traditional training models persist, and that police training is slow to change, might lie in the lingering police value which places emphasis on traditional police practices such as reactive policing.

2.4.4 Reactive Policing

A theme in the literature was how current training practices reinforce reactive approaches to policing (Cunha et al. 2016; HMIC, 2016; Schafer & Boyd, 2007; Timpf, 2014), which contradicts most police force's mandates to prevent crime. Timpf (2014) indicates that policing is no longer reactive and requires the individual officer to be a thinking professional (p. 18), and that only a small portion of an officer's time is spent on traditional policing such as arrests and using force (Timpf, 2014). Timpf (2014) argues that 90% of current training time is devoted to preparing officers for less than 10% of their actual duties. As indicated previously in this review, the technologies police use supports their existing paradigm of response-centered policing rather than supporting new ways of working (HMIC, 2016).

In the context of a digital society, traditional policing approaches are ineffective in addressing the evolving crime landscape (Cunha et al., 2016). A digital society requires officer who have both the technologies and the skills to meet digital demand (Custers, 2012; Hitchcock et al., 2017), yet digital skills are not included in standard police training (Bossler & Holt, 2012; Harkin et al., 2018; Sturgeon, 2015) leaving officers to develop digital skills on their own (Sanders & Hannem, 2012; Schafer & Boyd, 2007). Current methods of training have failed to adequately prepare officers for digital crime fighting (Wexler, 2012; Wolf, 2013). Koper et al. (2009) report an onus on police agencies to ensure that personnel are properly trained to use and understand digital technology. Bossler & Holt (2012) contend that "(l)ocal law enforcement agencies, including their line officers, must increase their capability to respond to cybercrime" (p. 166). Other studies found that police officers are being asked to be more effective first responders to digital crime but have little training for or experience with computer crime cases (Craiger et al., 2005; Holt & Bossler, 2012a,b).

2.4 Increasing Demands on Frontline Officers

The changing paradigm of policing was most reflected in the literature insofar as the digital society's impact on frontline police officers and first responders. Technology advancements have increased the employment responsibilities of police officers (Bossler & Holt, 2012; Timpf, 2014; Wolf, 2013). Holt and Bossler (2012b) report that the increased workload is felt most at the local level, stating that local law enforcement must respond to an increasing number of crime types regardless of the nature of the event. The theme of the increasing demands and expectations of frontline officers arose frequently, with two factors being mentioned repeatedly – the emergence of cybercrime and the role of frontline officers in responding to terrorism. Cybercrime was attributed as having the greatest impact on the increase in frontline duties. Bossler and Holt (2012) state "(p)atrol officers will have to play a larger role in cybercrime investigations because of their proven contributions in solving traditional crimes" (p. 168).

The events of September 11, 2001 fundamentally changed local policing (Wolf, 2013) resulting in a need for frontline officers to play an active role in counter-terrorism, intelligence gathering, surveillance, and risk threat assessments at the local level (Goodman, 2015; Schafer & Boyd, 2007; Wolf, 2013). Schafer & Boyd (2007) mention homeland security responsibilities have been added to police role, including disaster response, terrorism awareness, national security. Goodman (2015) has linked cybercrime and terrorism in a way that explains how these two phenomena have impacted frontline policing.

2.4.1 Frontline Officer Responsibilities

The literature indicates that the way frontline officers respond to digital calls for service is an issue. Officers are challenged to identify crimes as having a digital element, to identify the presence of digital evidence, and to elicit victim's confidence in the police service's response (Cunha et al, 2016; Cockcroft et al., 2018; Goodison et al., 2015; Holt & Bossler, 2012a; Horsman, 2017). These authors point to a lack of training as the cause of this issue. Cockcroft et al. (2018) state that frontline staff may not be sufficiently trained, or confident, to deal with digital crime, and that local responses to cybercrime are underdeveloped. Officers lack the ICT-related knowledge, expertise, and training to identify and handle digital crime, evidence or devices (Cunha et al., 2016; Holt & Bossler, 2012a; Horsman, 2017).

The role of the frontline police officer is changing. They are expected to be more autonomous decision makers (Timpf, 2014), conduct research and information seeking (Guclu, 2018; Guclu & Can, 2015; Timpf, 2014), and respond to a dynamic and growing crime landscape (Calam, 2017; Schreuders, Cockcroft, Butterfield, Elliot & Soobhany, 2018; Stratton et al., 2017). In particular, the theme of frontline police officers' role and ability to respond to crimes with a cyber-element was abundant in the literature. Digital crime fighting has to start with a trained frontline officer (HMIC, 2015), and frontline officers should possess the necessary technical skills and training to be better educated on cybercrime (Harkin et al., 2018; Sturgeon, 2015). Many frontline officers are unable to manipulate basic computer systems, write reports, or contribute valuable data (Bossler & Holt, 2012; Sanders & Hannem, 2012). HMIC (2016) report that working digitally is necessary for efficient and effective policing, yet very few forces are developing their officers’ digital skills. Other authors (Koper et al., 2009; Montgomery, 2017; Quinn, 2018) found that the unsafe computing practices of untrained officers pose a significant information security risk to their police services, who are increasingly being targeted by malicious cyber actors.

HMIC (2015) takes a strong view on the issue of frontline officer responsibilities, stating that “(t)he public has the right to demand swift action and good quality advice about how best to deal with those who commit digital crime from every officer with whom they come into contact” (p. 8), and that victims of any crime, including cybercrimes have a right to the level of help and support they would normally receive from the police. Bossler and Holt (2012) and Holt and Bossler (2012a) similarly found that frontline officers should play the same role in computer crimes as they do in traditional cases. Of particular note was the expectation for officers to be effective first responders in the handling of digital evidence (Cunha et al., 2016; Goodison et al., 2015; Hitchcock et al., 2016; Holt & Bossler 2012a, 2012b).

The literature presented some dissenting views that argued against frontline officers handling of digital evidence, stating that cybercrimes should be the responsibility of federal (as opposed to local) law enforcement agencies (Holt & Bossler, 2012a), and that frontline officers were not interested in computer and cyber training (Bossler & Holt, 2012). A theme emerged relating to the expectation that frontline officers would upskill themselves – often on personal time and at personal expense (Hitchcock et al., 2017; Ramshaw & Soppitt, 2018; Roberts et al., 2016; Schreuders et al., 2018). The theme of the education and skill levels officers attained on their own arose when examining the way police services recognize prior learning.

2.4.2 Police Fail to Capitalize on Existing Skills

A noted theme in the literature was the rigid adherence by police organizations to traditional norms. Regardless of skills upon entry, all sworn police personnel must train and start as frontline officers as there is only one point of entry into policing (Roberts et al., 2018). This requirement is demonstrative of police organizations' belief that recruits are empty vessels waiting to be filled (Enea, 2010). There is a need for police organizations to consider the existing skills and knowledge in their recruits (Bossler & Holt, 2013; Cockcroft et al., 2018; HMIC, 2016; Stokes, 2010). There is a need to recruit officers with pre-existing cyber skills, and to consider appointing officers by direct commission as opposed to traditional channels (Stokes, 2010).

2.5 Digital Literacy: The Missing Link?

Today's digital society is enabled and characterized "ubiquitous connectivity and mobility, people-centered and development-oriented digital infrastructure, widespread data literacy and social media, and new tools for capturing data and sharing information" (Hanna, 2016, p. 4). Digital literacy is necessary to make effective use of data and digital technologies (Hanna, 2016). The theme of the need for digital literacy was powerfully and abundantly represented in the literature despite varying definitions and purposes. This section of the literature review synthesizes the historical context, definitions, role, and application of digital literacy in law enforcement. Also discussed are relevant literature discussing the link between digital literacy and age, generation differences, and training methods.

2.5.1 History and Definitions of Digital Literacy

Xiong (2016) traces the origin of digital literacy back to the 1974 when Paul Zurkowski proposed the concept of information capacity. Other authors point to Paul Gilster's book entitled "Digital Literacy", published in 1997, as coining the term "digital literacy". Gilster proposed the link between the evolution of computing technology and the Internet, the impact of computers on information, and the use of computers by humans (Spante, Hashemi, Lundin & Algers, 2018). Gilster believed that digital literacy was skills-based and related to how humans use computers and the functional use of technology and skills adaptation (Spante et al., 2018). More recently, digital literacy has been updated as including more than simply skills and actions, but also cognitive competencies (Spante et al., 2018), and includes the functional access, skills, and practices necessary to become a confident, agile adopter of a range of technologies for personal, academic and professional use (Spante et al., 2018).

Digital literacy has proven to be challenging to define, however authors working for UNESCO (Law, Woo, de la Torre & Wong, 2018) proposed the following definition:

> "*Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy*. (p. 6)

This definition identifies digital literacy as the merger of multiple other new literacies (Kilic, 2010; Schafer & Van Es, 2017). Previous authors (Al Daihani & Rehman, 2007; Kilic, 2010) attempted to define the differences between *computer literacy* and *information literacy*. Kilic (2010) identified that computer literacy was a subset of overall technology literacy. Davies (2011) defined the term *technology literacy* as the ability to "adopt, adapt, invent, and evaluate technology, and who can use technology as a tool for organization, communication, research, and problem solving (p. 4)." Davies proposed a scale whereby low technology literacy involved basic awareness of technology, while practical competency and practical wisdom demonstrated high technology literacy (Davies, 2011). Reedy and Goodfellow (2012) posit that digital literacy can be classified into 5 levels. The lowest level, level 0, represents a level of literacy that allows for basic access, whereas level 4 involves professional use and digital identity management (Reedy & Goodfellow, 2012). Public Safety Canada (2018) concurs that digital literacy operates on a spectrum, with basic use at the low end and complex coding and algorithms at the other.

The UNESCO definition from Law et al. (2018) also implies that digital literacy is a combination of skills and competencies (Reedy & Goodfellow, 2012; Sharma, Fantin, Prabhu, Guan & Dattakumar, 2016), and operates on a cognitive level that exceeds practical skills to incorporate higher order thinking skills including understanding, analysis, processing, and creation of information (Davies, 2011; Osterman, 2012; Xiong, 2016). Digital literacy also includes communication, collaboration and teamwork, social awareness in the digital environment, understanding of e-safety and creation of new information (Reedy & Goodfellow., 2012). Schafer and Van Es (2017) argue in favour of a recognizing multiple "new literacies" including coding literacy, network literacy, data literacy, graphical literacy, social media literacy, and algorithmic literacy. Buck (2012) and Steyn (2018) both found that digital literacy could not be universally defined because it is contextual and based on the environment and needs of the user, implying that a user could be digitally literate in some contexts but not others.

When digital literacy in the context for policing, for example, Al Daihani and Rehman (2007) studied the computer and information literacy skills of Kuwaiti police officers and found that officers struggled with databases, spreadsheets, multimedia files and file management while showing marginal skills with e-mail, word processing, and using the Windows operating system. The authors also found that officers struggled with search strategies when accessing external sources. Not only is there a lack of consensus in the literature in terms of defining digital literacy, there are also varying views on the elements that comprise a digitally literate user.

In policing, the ability to use operating systems, word processors, and e-mail were identified in the literature as being core elements of digital literacy, along with the ability to safely search the internet and navigate various social media platforms (Steyn, 2018). Other elements identified include the ability to communicate complex IT concepts and data output into plain language narrative (Schafer & Van Es, 2017), and the ability define what information is needed, for what purpose, collected by which methods, from which location, and in what format (Xiong, 2016). Xiong (2016) also identified a key element of digital literacy was critically evaluating the veracity and credibility of the information. Weston, Bennett-Moses & Sanders, (2019) summarize the literature in stating “understanding data goes beyond technical abilities and requires an ability to understand how data fit together… not only is data literacy a required competency, but one that cannot necessarily be taught (and therefore needs to be recruited for)” (p. 8-9).

2.5.2 Importance of Digital Literacy

Damodaran and Burrows (2017) found that despite living in a digital society, “significant numbers are challenged by the demands and specificities of information and communications technologies (ICTs)” (p. 5). Several authors discuss the need for digital literacy both in general terms, and in terms of the policing context. Kilic (2010) states that digital literacy skills are vital for individuals working in government organizations. Choo (2011) links digital literacy with cybersecurity, stating that low digital literacy places people and organizations at increased risk of cyber victimization. Osterman (2012) indicates that employers need to bridge the digital divide that exists between home and the workplace. Weston et al. (2019) found that data literacy and technical skills are increasingly important despite arguments that software is becoming more intuitive, implying a lessening importance of digital literacy. The literature presented multiple points of view concerning the need to measure and maintain digital literacy levels (Hitchcock et al., 2017).

Law et al. (2018) state that UNESCO aims to define a minimum level of proficiency in digital literacy skills. Sharma et al. (2016) found that defining digital literacy levels is challenging as there are no standardized tests to measure digital literacy. This lack of standards is no surprise given the lack of a consensus definition of digital literacy. Digital literacy levels cannot be inferred or assumed based on age or occupation (Seawright, 2012), which means that in policing, there is a need to evaluate and re-evaluate the digital literacy skills of officers (Bossler & Holt, 2012). Other authors contend that digital literacy assessment and training need to be part of the basic police academy curriculum and written into policy (Al Daihani & Rehman, 2006; Sharma et al., 2016).

2.5.3 Digital Literacy in Police Training and Practice

The following statement by Wydra and Hartle (2015) poignantly summarizes many of the themes in the literature that relate to digital literacy in policing. They state:

> The technical evolution of police work coupled with the datafication of evidence is creating a need for technology officers who can investigate complex technical cyber-crimes, forensically examine digital evidence, maintain and deploy field robots and drones, operate and maintain predictive policing hardware and software, maintain and operate wearable cameras and devices, utilize social media tools, code apps, and maintain the various disparate data sources and data bases, to name a few. (p. 225)

The digital society needs a digital police officer who possesses a new set of skills from traditional police practice (HMIC, 2016). HMIC (2016) further state that “working digitally is necessary for efficient and effective policing” (p. 36), Digital skills have become highly relevant and are increasingly important to frontline police work (HMIC, 2016). As White and Escobar (2008) state, “basic computer skills are now essential for police officers” (p. 128). Bossler and Holt (2012) concur in their research, stating that “basic computer literacy is necessary for patrol officers” (p. 168). This sentiment is echoed by Seawright (2012) who states, “The role of technology and computers in police work cannot be overstated. Officers need a specific set of technology literacy in order to work effectively and efficiently." (p. 61). Seawright also identifies that digital literacy is important to proactive policing.

The core function of police is computerized and data driven (Chander, 2015), and frontline officers need "general digital awareness" (Cockcroft et al., 2018). Law enforcement is a dynamic profession, in which [officers] must be able to take information from a variety of sources and integrate it into knowledge that has practical application" (Stephens, 2015, p. 109). Kilic (2010) finds that most police tasks require certain levels of information literacy as police officers must deal with continuous information flow in every aspect of their job, which makes it imperative that officers be confident and competent in interacting with information. This theme of confident and competent arose several times in the literature (Damodaran & Burrows, 2017). Policing is a data-driven job, only possible if police must have adequate computing and information seeking skills. Police officers need to be efficient in using information systems and sources in order to excel in their jobs (Al Daihani & Rehman, 2006).

Despite the calls for digitally literate officers (Ministry of Justice, 2012; Ramshaw & Soppitt, 2018), multiple authors report that police personnel do not possess adequate digital skills (Cunha et al., 2016; McCoy, 2006; Olawoyin, Esse & Madukoma, 2017; Seawright, 2012). Weston et al. (2019) found that some of the most technical roles in policing are not filled by digitally literate personnel, and that digital literacy is not common in law enforcement (McCoy, 2006). Seawright (2012) found that many police officers lack basic literacy – language and writing skills - yet literacy is not developed either at the academy or via in-service training. Cunha et al. (2016) found that officers "have a total lack of technical insight concerning high-tech crimes" (p. 183). In their study, Al Daihani and Rehman (2006) found that police officers had weak computing and information capabilities, and generally poor searching skills, and that these skills needed to be developed internally. McCoy (2006) argues in favour of academy and in-service training that focuses on basic keyboarding, operating systems, software use, ethical use, and information security practices. HMIC (2016) points to a failure on behalf of police organizations to identify and measure pre-existing digital skills, stating, “very few forces are developing digital skills in their workforce, and none is taking full advantage of the skills that police staff…can bring to forces” (HMIC, 2016, p. 36).

Ramshaw and Soppitt (2018) call for a “new breed of police officer” (p. 247) who can deal with the current and future technologies and threats (Choo, 2011), and use social media and mobile technologies (Chander, 2015). Police need digital literacy to advance with the times, focusing on ways and means of training student the information ability to explore and apply information (Xiong, 2016, p. 331). Computer-based report writing was identified as an essential law enforcement skill that is as important to an officer as shooting skills (Seawright, 2012). Olawoyin et al. (2017) found a positive relationship between effective information use and quality of service. The literature had many positive notes relating to digital literacy in policing, as Weston et al. (2019) found that digital literacy among officers is gradually increasing, and Damodaran and Borrows (2017) reporting that basic digital literacy is sufficient for most roles – digital mastery is rarely required. However, Seawright (2012) cautions against underestimating or assuming basic levels of digital literacy, stating, “It cannot be assumed that because officers live in a technological society that they automatically gain the computer and technology literacies they need on the job” (p. 61).

Several authors advocate the need for continuous evaluation of digital literacy, finding that digital skills deteriorate over time (Damodaran & Burrows, 2017; Sharma et al., 2016) and have a short life span (Harkin et al., 2018, Horsman, 2017). One method of developing digital literacies that was prevalent in the literature was through game-based learning, including computer-based simulations. Damodaran and Burrows (2017) found that positive digital experiences promote deeper digital literacy learning. Wall and Williams (2007) report a dual benefit to virtual reality training insofar as the officer not only learns about technology but also familiarizes themselves with virtual environments. The authors suggest that virtual spaces constitute very real communities, that virtual space is connected to physical life, and that crime can and does occur in these communities. While the role of police in digital communities is not currently clear, virtual policing will become a reality (Wall & Williams, 2007). Werth and Werth (2011) point to the example of the US army's game-based learning, whereby games were used to recruit and train soldiers. The authors found that "the potential recruiting base is huge if gamers are reached" (p. 15). The theme of combining digital literacy with recruiting practices of police organizations was particularly prominent in the literature.

2.5.4 Digital Literacy in Police Recruiting

Policing begins with the critical first step of recruiting the right people (Hitchcock et al., 2016), yet recruiting is the one area of policing that is being ignored by both academia and police leaders (Wydra & Hartle, 2015, p. 224). The literature suggests that one option to addressing the lack of digital literacy skills among police personnel is to update the recruiting process (Silberglitt et al., 2015). Wydra and Hartle (2015) recommend a strategy to recruiting that emphasizes the shift from traditional policing. Schafer and Boyd (2007) recommend a concerted effort to move away from the military approach, finding that it is a turnoff for bright, educated applicants who do not want to be treated and trained like soldiers.

In particular, there is a need to target and hire applicants with pre-existing technology skills (Choo, 2011; Koper et al., 2009; Silberglitt et al., 2015; Stokes, 2010). HMIC (2016) found that most police recruiters are unaware of the need for digital skills in new recruits. Police organizations need to do more to recruit a technologically literate workforce (Cockcroft et al., 2018), and should look to hire, train, develop, and retain cybersecurity skills officers (Newhouse, Keith, Scribner & Witte, 2016). Wydra and Hartle (2015) suggest that police leaders need to focus as much recruiting emphasis and effort on recruiting technologically skilled officers as they do on recruiting women and visible minorities.

Finding cyber talent is a challenge (Sturgeon, 2015), and there is steep competition from the private sector for cyber-savvy applicants (Hitchcock et al., 2017) as well as from other government organizations who are all trying to recruit the same applicants (Harkin et al., 2018). literature suggest several different strategies to solve the recruiting dilemma. White and Escobar (2008) recommend hiring college educated officers. Wydra and Hartle (2015) recommend police agencies target students in IT programs as opposed to the traditional graduates from Criminal Justice programs, as current criminal justice programs have not matured to meet the needs of modern police agencies. Similarly, Silberglitt et al., identified the need to recruit candidates who are comfortable with network-centric environments (p. 29). Silberglitt et al. (2015) also recommend police agencies actively promote the cyber aspects of policing as doing so will attract younger applicants.

The theme of recognizing the different needs of younger applicants was prevalent in the literature. Hitchcock et al. (2017) suggest identifying the generation differences, values, and preferences of the younger generation. Werth and Werth (2011) identify gamers as an untapped demographic of potential applicants. Newhouse at al. (2016) and Hitchcock et al. (2017) describe the effectiveness of police-sponsored cyber security competitions – also called Hackathons – as a proven strategy for identifying and recruiting digital talent. Hanna (2016) suggests police agencies look beyond digital literacy to include digitally literate leaders, as these are the future administrators who will navigate police organizations through times of technological change. The focus on recruiting the younger generation might be explained when examining the literature on the relationship between age and digital literacy.

2.5.5 Age as a factor in Digital Literacy

The mean age of officers continues to increase, according to Etter and Griffin (2011), who state, “the thin blue line is graying” (p. 233). An ageing workforce is a fact of modern policing (Etter & Griffin, 2011). Several authors have identified the age of officers as having an impact on their levels of digital literacy computer skills, and technology adoption (Damodaran & Burrows, 2012; Demircioglu, 2010; Etter & Griffin, 2011; Seawright, 2012). Choo (2011) refers to the “digital generation” as “the young and internet aware” (p. 719). Horsman (2017) linked digital skills with exposure to computers at a young age, which aligns with HMIC’s (2015) finding that today’s policing applicants grew up spending significant amount of time online in their teenage years.

When examining the information seeking practices of younger officers, Demircioglu (2010) found that younger officers prefer digital sources of information as opposed to reaching out to more senior officers, whereas senior officers preferred to rely on their own knowledge and experience rather than use digital information sources. Olawoyin et al. (2017) concur, in their findings that age impacts how police officers use information. However, Bossler and Holt (2012) caution police leaders against assuming a level of digital literacy based solely on the age of the officer. Werth and Werth (2011) identify an issue with generational needs of police personnel, stating “There is a digital divide between millennial students and their older counterparts” (p. 18). The theme of the impact of the *millennial generation* was prominent in the literature.

In the next decade, nearly half of the almost 700,000 active-duty, sworn law enforcement officers in the United States will be eligible to retire (Stephens 2015, p. 1). This exodus of retiring officers will result in a generational shift is occurring in the workplace (Werth & Werth, 2011). Stephens (2015) finds that Millennials will be the dominant generational cohort in the workforce during the next decade. Horsman (2017) states “An increasing younger populous of computer-savvy individuals are replacing an older, more computer-illiterate generation” (p. 449). Stephens (2015) and Werth and Werth (2011) identify four generations in the police workforce: Traditionals, Baby Boomers, Gen X, and Millennials. Traditionals accounted for such a small percentage that they were not considered in Stephens’ study.

Millennials are defined by their age and the tech they grew up with (Gresham, 2016). The literature presented some variance in terms of the age range of the millennial generation; however, the general findings were that Millennials are born between the years 1980 and 2000 (Giovengo, 2016, Gresham, 2016; Stephens, 2015; Werth & Werth, 2011). Etter and Griffin (2011) found that most police recruits are millennials. Millennials are entering law enforcement in greater numbers, by 2020 accounting for the majority of officers (Gresham, 2016).

There were distinct generational trends among officers in different age brackets (Gresham, 2016). For example, millennial officers were found to have unique needs and skills and need to be trained differently (Giovengo, 2016, Gresham, 2016). They are attracted to technology and are looking to work with the latest technologies (Koper et al., 2009). Millennials are a generation that identifies, values, and trusts technology, and are also savvy multitaskers (Giovengo, 2016). Generational differences between instructor and learner are a challenge in police training (Stephens 2015). Millennial officers will not respond well to traditional police training methods such as passive lectures (Werth & Werth, 2011).

Using terminology coined by Marc Prensky (2001), Gresham (2016) refers to millennials as “digital natives” (p. 3) who grew up with ready access to digital technologies. Keeping with Prensky’s terminology, Giovengo (2016) refers to Baby Boomers as a generation who did not grow up with technology and called them “digital immigrants” (p. 207). Giovengo (2016) and Gresham (2016) both suggest the learning styles and preferences of digital natives do not align with the teaching styles of digital immigrants. Due to their comfort and competence with technology, digital natives have a “competitive advantage” over immigrants in the workforce (Sharma et al., 2016, p. 636). Due to their predisposition to adopt and natively understand technology, millennial officers are well-positioned to address both the current and future crime landscape.

2.6 Impact of Future Technologies on Policing

According to Strom (2017) the two digital technologies that have had the greatest impact on police practice to date are digitized records management systems and computer-assisted dispatching. The literature was rich with predications on the emerging technologies that would similarly change the face of law enforcement. IP video surveillance, video analytics (such as automated license plate recognition), police body-worn cameras (BWC), real-time wireless live streaming video feeds, and in-cruiser audio and video recording were frequently mentioned (Goodman, 2015; Hitchcock et al., 2017; Rowe, 2018; Strom, 2017; Wexler, 2012). Predictive policing, while not a new concept, continues to evolve and mature in the form of increasingly sophisticated data mining and analysis for crime prevention (Custers, 2012; Joh, 2018; Wydra & Hartle, 2015), including crime mapping using GIS (Chander, 2015; Koper et al., 2009, Strom, 2017).

The role of data in police cannot be overstated. Multiple authors indicate that policing is an information-centric service that is crucially dependent on data and data analysis (Al Daihani & Rehman, 2006; Kilic, 2010; McCoy, 2006; Weston et al., 2019). This dependence on data places police departments at an increased risk of cyber-attack (Francescani, 2016; Koper, 2009; Quinn, 2018). The recent trend towards Next Generation 9-1-1 call-taking and real-time monitoring centers also demonstrate law enforcement’s transformation to support the digital society (Hirsh, 2016; Hollywood, Vermeer, Woods, Goodison & Jackson, 2018; Koper et al, 2009; Strom, 2017). The use of ever-increasing quantity and quality of data has also led to the increased adoption of Intelligence-based policing (Cotter, 2017; Ramshaw & Soppitt, 2018; Ratcliffe, 2016).

Also prevalent in the literature was law enforcement's increasing use of social media tools, applications, and analysis for recruiting, community outreach, public notifications, and investigation (Horsman, 2017; Joh, 2018; Silberglitt et al., 2015; Trottier, 2015). Accordingly, online privacy, encryption, and other data obfuscation methods are evolving and will continue to challenge law enforcement in the coming years (Craiger et al., 2005; Custers, 2012; Horsman, 2017; Wydra & Hartle, 2015).

Other technologies mentioned in the literature as having an impact on policing include biometric identification (primarily via facial recognition) (HMIC, 2018; Rossler, 2019), and the emergence of robotics, drones, and autonomous vehicles as all having both promise and problems for law enforcement (Chander, 2015; Hitchcock et al., 2017, Joh, 2018; Koper et al., 2009). The increasing prominence of augmented and virtual reality in the form of virtual worlds, online gaming, and police training was a budding theme in the literature (Enea, 2010; Koper et al., 2009; Schafer & Boyd, 2007), with theft of virtual, intangible property representing one example of this evolving crime landscape. Schafer and Boyd (2007) indicate virtual environments will increasingly play a role in police training as they become more realistic, interactive, and end-user driven.

When considering future technologies, the last theme of note in the literature was the abundance, ubiquity, and increasing prevalence of digital devices. In the context of smart cities, for example, multiple authors mention the Internet of Things (IoT) as previously non-digital devices are replaced by connected sensors (Chander, 2015; Rathore et al., 2018; Wydra & Hartle, 2015). As noted by Horsman (2017), these digital devices are constantly changing and are all very different which makes standardizing investigative procedures nearly impossible. To illustrate, the author contrasts the techniques of digital evidence collection from devices with the established process of collecting physical evidence such as blood splatter – a process which hasn't changed in 150 years (Horsman, 2017).

Digital devices will continue to re-shape to duties and responsibilities of the frontline officer, as police gradually increase their use of smartphones, mobile apps, roadside biometrics, DNA-based identification, in-field digital forensics, and body-worn cameras (Choo, 2011; Joh, 2018; Rathore et al., 2018; Stensland, 2018; Strom, 2012). As Seawright (2012) states, "Technological devices are used for almost every facet of a police officer's daily duties" (p. 59).

2.7 Theoretical Framework: UTAUT and Grounded Theory

As identified earlier in this review, digital technology is now at the core of police practice. Accordingly, several studies have examined the role of technology acceptance, albeit none have done so in the context of policing or police training. The UTAUT model (Venkatesh et al., 2003) proposes a number of factors and modifiers that impact technology acceptance and use. However, UTAUT alone was not directly applicable to this research context, and does not consider the role of digital literacy. Therefore, this study considers the UTAUT model as a potential foundation for a new theory of technology adoption in policing. Therefore, the combination of UTAUT and grounded theory form the theoretical framework for this study.

2.7.1 Technology Acceptance in a Digital Society

This review of the literature has established that technological change is a persistent force in policing (Koper, Lum & Willis, 2014). Tanner and Meyer (2015) state, "There has been an ongoing technological revolution in police work" (p.388). The authors conclude that this technological revolution is resulting in a deep transformation and a frantic acceleration taking place (Tanner & Meyer, 2015). Rossler (2019) states "The nexus between policing and technology is so close" (p.210). It stands to reason, therefore, that technology adoption by police is a must in today's digital society (Damodaran & Burrows, 2017).

Police are not alone in their struggle to adopt new technologies. Viswanath Venkatesh, one of the foremost theorists on technology adoption, believes that as information technology becomes increasingly central to all organizations, technology acceptance also becomes increasingly important (Venkatesh & Bala, 2008). Technology supports the overall goals of policing and is commonly used by law enforcement agencies at all levels (Tanner & Meyer, 2015). This should imply that technology adoption is not an issue with the police, however the literature suggests otherwise. In the interest of context, a brief summary of the technology adoption theory (TAM) in its various forms is provided.

2.7.2 History of Technology Adoption Model

The concept of TAM was initially proposed by Fred Davis in 1989 (Davis, 1989). Davis was interested in understanding how external variables such as perceived usefulness (PU) and perceived ease of use (PEOU) impacted behavior intention in the context of computer use. PU involves the participant's belief that the technology will enhance their job performance, while PEOU relates to the participant's belief that the technology is too hard to use and that the performance benefits of usage are outweighed by the effort of using the application (Davis, 1989). Davis's theory was initially developed for businesses who were introducing computers in the workplace (Lindsay, Jackson & Cook, 2014). Despite the growth and evolution of adoption models that accounted for other variables – both internal and external to the participant – Yalcinkaya (2007) found that PU and PEOU remain the two most significant determinants of technology adoption, with PU having a greater impact than PEOU among police officers (Yalcinkaya, 2007).

In 2000, a time when technology was advancing, Venkatesh and Davis collaborated to advance the TAM theory, creating TAM2, in response to challenges that the initial TAM was not effective in predicting adoption and the problem of under-utilized system persisted (Venkatesh & Davis, 2000). TAM2 included new variables: social influence process (subjective norms, voluntariness, and image) and cognitive instrumental process (job relevance, output quality, result demonstrability, and experience) (Venkatesh and Davis, 2000). TAM2 also placed less focus on TRA and participant attitude (Yalcinkaya, 2007). Eight years later, Venkatesh and Bala (2008) proposed TAM3, a model that placed greater emphasis on the context of the technology use environment – specifically on the role of the manager in technology adoption. TAM3 recognized the known factors that affect TAM, but sought to understand how managers can influence those factors (Venkatesh & Bala, 2008). TAM3 provides interventions to boost PU and PEOU, but the focus of this model remained on the individual and not in the wider implementation context (Lindsay, Jackson & Cooke, 2011).

Lindsay et al. (2011) examined how previous TAM models could be applied in an increasingly mobile technology context, and expanded on current TAM theory to propose a mobile-TAM (M-TAM) theory. M-TAM was designed specifically to examine police officers' adoption and use of laptops in police cruisers, also called mobile data terminals. Lindsay et al. (2011) recognized that policing was a unique context and incorporated factors relating to implementation and social interactions when considering technology adoption. The authors identified four categories of acceptance of mobile technology: performance, security and reliability, management style, cognitive acceptance (Lindsay et al, 2011). Lindsay's later work to include other mobile devices used by police (Lindsay et al., 2014), Tanner and Meyer (2015) identified the most prominent mobile technologies in policing are smartphones and body-worn cameras (BWC). Body worn cameras are perhaps the most discussed new technology in policing (Rossler, 2019). Other technologies being considered for adoption include aerial surveillance IP video, social media, GIS Crime mapping and crime prediction analytics, and less lethal force technology (Rossler, 2019).

2.7.3 Technology Adoption and the Police

The adoption and use of digital technologies are vital to policing, yet the literature suggests that police are behind the technological curve and are actively chasing technological progress (Tanner & Meyer, 2015). Understanding the role of technology adoption by police is essential to solving the technology paradox police often encounter, where failure to adopt technology is not an option, but technology adoption is fraught with challenges and often results in failure (Tanner & Meyer, 2015). Technological advancements do not always produce obvious or easy improvements in police practices (Koper et al., 2014). Lum et al. (2017) concur, and report being less sure of the role of technology in policing insofar as the link between technology and effective policing is still not clear. While some research has shown that technologies make policing processes faster and easier, contrasting research shows that technology reduces efficiency and adds to officer workloads (Lum et al., 2017; Williams & Aasheim, 2005). When viewed from the perspectives of police officers and citizens, both groups strongly believe that technology can enhance policing (Koper et al., 2014), is essential to the success of police organizations (Lindsay et al., 2014), and is recognized as a critical tool for preventing and fighting crimes (Straus, Bikson, Balkovich & Pane, 2010).

2.7.4 Citizen Trust and Technology Adoption by Police

A theme emerged in the literature that linked citizen trust and faith in their police service and the level of technology used by that service (Damodaran & Burrows, 2017; Koper et al., 2014; Lum et al., 2017; Rossler, 2019). Damodaran and Burrows (2017) found that slow adopters of technology are socially and digitally excluded. Lum et al. (2017) indicated that a lack of evidence linking police use of technology to crime reduction erodes public trust, confidence, and satisfaction with police (p.2). A lack of adequate technology in policing "poses a major risk for losing face when confronting citizens" (Tanner & Meyer, 2015, p.393). Multiple authors (Koper et al, 2014; Rossler, 2019) found that technology use by police in the form of communications technologies increase their legitimacy and strengthens police-citizen relationships. When viewed through a lens of technology adoption, Rossler (2019) found that citizens' interpretation of police technology use impacts adoption. For example, police are reluctant to adopt technologies that the citizens feel violate their privacy (Rossler, 2019). The pubic expects the police to not only protect people and property, but also to safeguard the data relating to citizens; describing police as being in the "intelligence sector" (Yalcinkaya, 2007, p.20).

The link between policing and digital technology is complicated and unclear despite technology use being linked to many aspects of policing (Lum et al., 2017). The adoption of technology by police is also complicated, with the literature suggested a myriad of factors that directly and indirectly impact technology adoption. External and internal, social, operational, technical, organizational, and cultural, factors each emerged in the literature.

2.7.5 Factors Influencing Technology Adoption

Social factors such as subjective norms (Lin, Hu & Chen, 2004) emerged, where the influence of peers was a common factor. Lindsay et al. (2014) attributed the influence of peers to the nature of police work, where officers work together in intense situations which forms close bonds and high levels of trust. Similarly, Rui-Hsin and Lin (2018) found that peer acceptance contributed to technology adoption, and that adoption was more likely if important people in the user's social group view the technology as important. Rowe (2018) linked low levels of adoption and motivation to negative past experiences using technology, and Damodaran and Burrows (2017) found that officers who had up-skilled were more likely to help those who are slower to adopt technology. Conversely, Yalcinkaya (2007) described the influence of peers as having only a moderate effect on technology adoption, claiming that the paramilitary nature of policing impacted voluntary use of technology. A fact that Lindsay et al. (2014) found to be advantageous in gauging adoption.

There are also a number of **operational factors** identified in the literature. Task fit was another theme that emerged as having a positive impact on technology use, with multiple authors (Lum et al., 2017; Koper et al, 2016) finding that adoption and use were higher if linked to traditional policing activities – such as reactive response – and daily tasks. Technology must interact/integrate into the officer's existing daily routines without adding work (Koper et al., 2014; Tanner & Meyer, 2015). "From the point of view of patrol officers, a good [technology] is one that best fits with, or even enhances, established work practices (Tanner & Meyer, 2015, p.390). Officers were more likely to adopt technology when they can see its application to their daily duties and specific roles in policing (Straus et al., 2010; Tanner & Meyer, 2015). Rui-Hsin and Lin (2018) identified job relevance as having a positive effect on PU. Straus et al., 2010 found that technologies that support the collaboration needs of police were more likely to be adopted. In short, technology fit to roles and tasks were highly influential factors (Lindsay et al, 2014; Lum et al., 2017).

There was also a link between adoption and operational outcomes – specifically those that produced and facilitated outcomes that aligned with traditional reaction and response models of policing (Lindsay et al, 2014; Lum et al., 2017; Koper et al, 2016). Adoption increases if officers hear of system leading to arrests and charges (Bossler & Holt, 2012). Yalcinkaya (2007) describes police officers as being very pragmatic and needing to see tangible results before buying in to new technologies. Adoption and motivation are higher if technical efficiencies are evident (Lum et al., 2017; Straus et al., 2010). Adoption was low when officers question the value of the technology's contribution to street police work, according to Tanner and Meyer (2015), who also noted low use levels if the cost-benefit equation doesn't balance. For example, if the technology costs time and energy but doesn't yield measurable results, adoption is less likely (Tanner & Meyer, 2015). Control over the technology arose as a relevant factor, with officers reporting higher adoption levels if they felt they had control over the technology (Rui-Hsin & Lin, 2018; Yalcinkaya, 2007). Perception of control was higher if the tool was perceived to be easy to use.

Age surfaced as a relevant factor in technology adoption, with older officers reporting being less likely to use technology due to decreased vision, dexterity and memory (Damodaran & Burrows, 2017), and younger officers were found to be more open to adopting technologies. Younger officers perceived their services as having low levels of technology adoption (Tanner & Meyer, 2015), while older officers generally believed that technology adoption by the service was high – a fact that was attributed to older officers having witnessed more technology-related changes in the department (Tanner & Meyer, 2015). Despite the fact that mastery of the technology or tool did not appear to impact adoption (Damodaran & Burrows, 2017), younger officers who showed greater competence with digital technology. This divide in digital competence levels has resulted in a "reversal of learning" (Tanner & Meyer, 2015, p.391) whereby the knowledge and experience of more experienced officers is less valued than the technology skills of the younger officers, which inclines the more experienced officers to resist the technology (Tanner & Meyer, 2015).

A number of **technical factors** and challenges were noted as having an impact on technology use, including difficult or cumbersome user interfaces, slow response times by technical support, technical problems with software or tools that go unaddressed by administration, and the requirement for officers to learn new processes and remember new codes

(Koper et al, 2014; Straus et al, 2010). Other technical issues related to the IT infrastructure, including low bandwidth and network latency, scalability of the technology, reliability of the technology, cybersecurity concerns resulted in security measures that impacted ease of use (Straus et al., 2010); Williams & Aasheim, 2005). Lastly, both system quality and service quality were shown to positively impact both PU and PEOU (Rui-Hsin & Lin, 2018).

Some challenges to adoption were related to the **organizational factors**, with low adoption being linked to a lack of clarification or policy relating to devices or software leaves officers feeling unsure of consequences and therefore reluctant to use (Straus et al., 2010; Tanner & Meyer, 2015). In the absence of department issued technology, frontline officers feel obligated to purchase and use their own personal devices, such as smartphones and body worn cameras, for ‘legal survival’. Administrators are aware of this but do not discipline officers for doing so (Tanner & Meyer, 2015). In fact, police organizations reap several benefits from officers’ use of personal devices insofar as these devices come at no cost to the department, the department is not responsible to provide training and is therefore not liable for an officer’s use of misuse of the technology (Tanner & Meyer, 2015). The role of administrators in technology selection, deployment, and adoption was prevalent in the literature.

It is the police leaders’ job to acquire technology, and acquisition and deployment decisions are high priority topics for police leaders (Koper et al., 2014). Lindsay et al. (2014) state, “Without buy-in from senior management, it is unlikely that new technology projects will proceed” (p.433). In procurement, many police leaders neglect to include their own IT staff – failing to recognize the role of IT in technology adoption (Williams & Aasheim, 2005). Along with acquisition decisions, police administrators must consider adoption challenges and implementation strategies. According to Koper et al. (2014) Police leaders often fail to strategically deploy technologies, resulting in low adoption and poor outcomes. Police leaders play a powerful role in technology adoption (Lindsay et al., 2014; Straus et al., 2010; Venkatesh & Bala, 2008), as do the policies they create. Straus et al. (2010) found that internal policies play a key role in technology adoption, and that technology use should be linked to documented policing outcomes. Managing technological change involves adjusting the frames of police officers – similar to organizational reform (Lum et al., 2017). Managers need to develop and implement effective interventions in order to maximize employees' IT adoption and use (Venkatesh & Bala, 2008).

The literature generally showed a divide between the technology decisions of administrators and the officers' technology use (Tanner & Meyer, 2015), with police leaders being unaware of the impact the technology may have on operations. There is a disconnect between police leaders' opinions of technology use and that of frontline officers. Police Leaders believe technology facilitates many aspects of policing, whereas frontline officers, detectives, and supervisors do not (Lum et al., 2017). Police administrators are inclined to choose technologies that limits the opportunities for officers to think creatively to solve problems, preferring to use technology to control operational decisions (Koper et al, 2014). Tanner and Meyer (2015) found that officers perceive a lack of managerial support as an invitation to creatively solve their own technical challenges. The authors also found that police administrators can be inconsistent in their attitudes toward technology whereby they promote technology use as helpful to policing, but reprimand officers "for always having their heads turned toward the screen" (p.391). The relationship between police leaders and frontline officers is particularly prevalent when looking at technology adoption through the lens of organizational culture.

The literature identified several **cultural factors** impacting technology adoption, including organizational culture, subcultures, and cultural barriers (Lindsay et al, 2014; Straus et al., 2010). Technology use and interpretation is shaped by policing cultures and subcultures (Koper et al, 2014; Lum et al., 2017). There is cultural resistance in policing to the incorporation of new forms of knowledge into police roles (Cockcroft et al, 2018). Koper et al. (2014) found that “Cultural resistance to change is a common impediment to innovation in policing” (p.215). User resistance can undermine technology adoption (Sanders & Hannem, 2012; Williams & Aasheim, 2005). Police culture can distort or impede the adoption, use, and outcomes of technology (Lum et al., 2017), and officers resist technologies that impact their autonomy and discretion, facilitate surveillance/micromanagement by supervisors (Koper et al, 2014; Lum et al., 2017; Rowe, 2018), and are seen as a means of increasing accountability while restricting discretion of frontline officers (Rossler, 2019).

Police culture values autonomy in police work and will resist technologies that negatively impact that autonomy (Tanner & Meyer, 2015). For example, officers will often elect to use personal devices in their daily duties as a means of escaping the scrutiny of administrators and to bridge the technology gap between their service and the criminals (Tanner & Meyer, 2015). Technology is resisted when it is perceived that technology use drains time from other culturally valued activities, such as coaching, mentoring, and guiding patrol officers (Koper et al, 2014). Lastly, the police culture values risk avoidance, making officers unlikely to adopt technologies or changes that add risk (Yalcinkaya, 2007). One proposed solution to cultural barriers is to be strategic when implementing of new technologies.

Police agencies and organizations often struggle to implement technology in a way that maximizes adoption (Koper et al, 2014; Tanner & Meyer, 2015). Venkatesh and Bala (2008) report that **implementation factors**, such as poorly planned deployment of technology can lead to huge financial losses, while Lindsay et al. (2014) found that implementation of technology was often rushed. Despite the challenges, a review of the literature revealed several suggestions to strategic technology deployment by police. Koper et al. (2014) emphasized that technologies were more likely to be adopted if frontline officers are allowed input into the procurement and deployment processes, and are provided evidence that their input was considered. The role that frontline officers play in the implementation stage was prevalent in the literature, with Koper et al. (2014) reporting that frontline officers are the most challenging group to adopt new technologies and are the most impacted by new technologies. The dissemination of information was a key factor to successful implementation (Tanner & Meyer, 2015) as the more information frontline officers receive the better they can understand and optimize new technologies.

2.7.6 Impact of Training on Technology Adoption

The relationship between technology training – both pre and post deployment – and technology adoption was frequently found in the literature, specifically the availability, quality, and quantity of training. Training has been suggested as one of the most important post-implementation interventions that leads to greater user acceptance and system success (Venkatesh & Bala, 2008). Technology adoption rose when officers believed the system was easy to learn, which, in turn caused them to regard the technology as an effective and useful service (Rui-Hsin & Lin, 2018). “Proper levels of training are essential, especially for the most difficult technological changes” (Koper et al., 2014, p.218). In the absence of formal training, officers are often left to learn on their own, resulting in inconsistent use of the technology and inconsistent output (Sanders & Hannem, 2012). The lack of technology education in basic recruit training, for example, demonstrates a disconnect between recruit training and police practice (Tanner & Meyer, 2015).

The quantity of technology-based training was found to impact technology adoption and use. Koper et al. (2014) found that officers receive little in the way of consistent training or direction on ways to optimize technology use in their daily work and deployment habits training on new technologies. Less training or no training resulted in low perceived usefulness (Lindsay et al, 2014; Sanders & Hannem, 2012). Koper et al. (2014) indicated that technology training and education need to be offered at both basic recruit and in-service training, while Williams and Aasheim (2005) found that training and re-training were critical to change management initiatives.

Quality of technology training was another theme that emerged. Police training on technology emphasizes the basics of operating the technology (skills-based), and there is less emphasis on how the technology and information gathered are used by the organization to support the overall goals of policing (Koper et al, 2014; Lindsay et al, 2014; Sanders & Hannem, 2012; Williams & Aasheim, 2005). Training must focus on the proactive value of the technologies (Koper et al, 2014), and should include information about how the output of the technology is used by police leaders, lawyers, and court officials (Koper et al, 2014; Williams & Aasheim, 2005), as well as the tips and tricks found by other officers in similar contexts. Training that was customized to the policing role of the trainee (learner-centered) resulted in high levels of adoption (Lindsay et al., 2014). Interestingly, Venkatesh and Bala (2008) found that game-based training was more effective than traditional training to enhance user acceptance of a new system.

2.8 Criticisms of Technology Adoption by Police

The presence, quality, and quantity of training were linked to technology adoption and/or use. However, there remain a number of criticisms of technology use that impact adoption. The theme of technology as a distraction was prominent in the literature as was the over-dependence on technology (Straus et al., 2010; Tanner & Meyer, 2015). Officers perceive that technology use negatively impacts the development and use of traditional policing skills such as observation, deduction, fieldwork, and interpersonal contact was established (Tanner & Meyer, 2015). Lum et al. (2017) found that the adoption of technologies can reduce agency efficiency and produce unintended and negative consequences, such as officers spending more time writing reports, inputting data, and correcting input errors – thus negating the time savings of electronic reporting over paper-based. The authors also found that technology often takes the officer off the street which limits potential for citizen interaction and community policing.

Other relevant themes included how technology use created frustration and stress among officers (Lindsay et al., 2014; Tanner & Meyer, 2015; Williams & Aasheim, 2005), has no impact on job satisfaction, and was not linked to crime reduction outcomes such as lower clearance rates (Koper et al., 2014). Officers with low levels of adoption found ways to neutralize, circumvent, or work around, the technology (Sanders & Hannem, 2012; Tanner & Meyer, 2015; Williams & Aasheim, 2005). Lastly, while the factors that affect technology adoption are known, there is a lack of research into the ways police organizations and leaders can influence, or change, these variables (Venkatesh & Bala, 2008).

2.9 Summary

This review of the literature identified a number of key themes when examining the nexus of the digital society, police training and practice, technology adoption, and digital literacy. These themes were synthesized and organized in the context of the current police environment.

Chapter 3: Methodology

3.0 Overview

The purpose of this research was to examine the ways in which police recruit training responded to the needs of a digital society. The demographic best suited to answer the research questions are the people who are responsible for creating and providing police basic recruit training.

3.1 The Topic

This research concerns the convergence of policing and digital technologies. There is little existing research that directly links the digital literacy levels of police officers with the training offered to recruits and the requirements of frontline police officers in a digital society, nor was there any literature that linked the digital literacy levels of police officers with the levels of technology adoption and training. The recent rise in cybercrime, the ubiquity of digital evidence, and the growing public sentiment that police officers may be challenged to practice their craft in this new crime landscape make this topic one worth researching. The need to discuss the levels to which police officers in Canada are being prepared to prevent and respond to crime in an increasingly digital of society is both timely and relevant.

It is especially relevant when considering the continued development and evolution of digital technologies and devices used by both the public and the police, the increasing dependence on data and computers by police, the challenges faced by police agencies to remain relevant in the crime race, and the emerging need to develop digital literacy levels of law enforcement personnel. An initial review of the literature in these areas (Chapter 2) reveals a lack of research linking police recruiting, initial training, recurring training, on-the-job experiences, and technology adoption with digital literacy competencies. This chapter describes the research plan and the methodology used to collect, analyze, and synthesize the data, as well as the constraints of the research methods used in this study.

3.2 The Research Plan

The type of research study undertaken is dependent on the kinds of questions the author seeks to answer (Del Balso & Lewis, 2012). The literature review identified several gaps. There were gaps connecting the needs of a digital society and the training of new police officers. There were also gaps between the expectations of the public and the observed practices of frontline police officers. There were gaps in the literature with respect to levels of technology adoption among police officers, trainers, and administrators. Finally, the literature did not identify the digital literacy requirements of police officers in the field compared to those requested by police recruiters.

Based on these identified gaps, the researcher sought answers to the following research questions:

1. In what ways do current police recruit training academies in Canada recognize the digital society?
2. What are the attitudes of police trainers regarding the adoption and teaching digital literacy skills?
3. What is the role of digital literacy in police training and practice?

   Through the process of refining the research questions, a number of secondary research questions arose:

4. How do trainers describe the relationship between actual police activities and academy training?
5. Which changes do police trainers identify as necessary to improve the current police training curriculum?

6. What is the perceived future of police education in Canada and what are the challenges impacting these changes?

Given the research questions above and the body of literature synthesized in chapter 2, an exploratory research study was appropriate. Del Balso and Lewis (2012) identify that an exploratory study is undertaken when the author seeks to determine what the reality is in situations where there is a lack of firm information. They state that, "[A]n exploratory study is designed to seek out as much information as possible from whatever sources are available about the subject" (p. 35).

According to Del Balso and Lewis (2012) an exploratory research study can utilize either quantitative, qualitative, or a combination of both types of data. Qualitative research is exploratory, detailed, descriptive, and interpretive, and can involve interviews where the data must be interpreted by the researcher using an inductive method of data analysis (Del Balso & Lewis, 2012). Qualitative research uses open-ended interviews to collect participants' statements, ideas, perceptions and opinions on a topic or question, and is characterized by verbal or literary presentation of data (p. 39). Qualitative research asks questions about experiences and subjective meaning of social situations while exploring subcultures, norms of peer groups, and reactions to institutional changes (Del Balso & Lewis, 2012).

According to these parameters, this study is exploratory, as it utilizes qualitative research data to deliberately and systematically connect new research to previous research in order to derive results that are presented in such a way so as to promote subsequent research. This research design uses semi-structured interviews (Creswell, 2014) with an emphasis on collecting qualitative data.

There are several reasons supporting this study's emphasis on qualitative data. The purpose of this study was to add information to the literature on the gap in digital literacy and technology skills among police recruits from the perspective of police educators. Accordingly, the research design is qualitative in order to fully explore the views of these educators on digital policing within the contexts of their workplaces. The data in this study were collected through semi-structured interviews.

According to Rao and Perry (2006), qualitative methodology using interviews is used to answer the research questions about a field of research that has not yet been developed. Merriam and Tisdell (2016) states that qualitative researchers have an interest in understanding how other people experience and construct their world views, and give meaning to their experiences. Creswell (2014) agrees that qualitative research helps to explore and understand how groups attribute meaning to a social problem. Qualitative research, according to Creswell, typically involves collecting data in the participant's setting or workplace (Creswell, 2014). The research outlined in this chapter investigated police trainers' views through interviews that took place in their work setting. Quantitative methods would be less appropriate given that quantitative data studies tend to be large experimental studies that confirm a hypothesis (Merriam & Tisdell, 2016). The precise ways in which police services in Canada are using or teaching about digital technologies is unknown at this time. Also, the level to which police trainers perceive a need for police recruits to be more proficient with digital tools and the means through which they see how digital literacy skills could be developed are also under-researched in Canada.

This research was qualitative because it aims to allow the answers to the research questions to emerge from the data. Since the answers have not been predetermined, participants cannot be asked if they agree or disagree using a Likert scale. Qualitative research allows the researcher to ask open-ended questions designed to encourage participants to reflect on their experiences and philosophies to generate a range of answers to the research questions (Merriam

& Tisdell, 2016). Additionally, quantitative methods such as short answers may have restricted responses and failed to capture the level of depth and detail that is required to answer the research questions.

3.3 Philosophical Worldview

The philosophical worldview supporting this research plan is constructivism. A constructivist philosophy seeks to understand concepts and generate meaning based on input from multiple participants (Creswell, 2014; Merriam & Tisdell, 2016). With constructivism, interview questions are broad and general to allow the participant to define, in their own words and given their own contexts, terms such as digital skills, digital literacies, technology tools, ICT, and technological competencies. The contexts for their answers are specific to their work environment, and they are answering through the lens of their professional role (Creswell, 2014). Creswell (2014) states that, “The goal of [constructivist] research is to rely as much as possible on the participant’s views of the situation being studied” (p. 8). This research relies on the participants’ views, opinions, experience, and ideas surrounding the identification and value of technology skills in police education and training. Interview questions were open-ended, broad in scope, and sufficiently general to allow the participants to infer and construct their own meanings on these topics. According to Crotty (1998), constructivist research may not begin with a theory in mind, but rather aims to inductively develop a theory based on the data collected and the themes that emerge. Accordingly, this research uses an inductive design with a constructivist worldview which Merriam and Tisdell (2016) considers a basic criterion for a qualitative study.

3.4 Qualitative Research Design: Grounded Theory

Merriam and Tisdell (2016) finds that the methodology of grounded theory merges well with a constructivist worldview. This research employs a grounded theory design for the data collection, analysis and interpretation (Glaser & Strauss, 1967). According to Merriam and Tisdell (2016), grounded theory data collection tools can include interviews, observations and documentary materials. Grounded theory applies to practical problems where there is no previous theory to guide the analysis of the responses. The literature review indicates an absence of a specific theory to study the digital skills of front-line police officers.

Strauss and Corbin (1994) state that grounded theory develops theory that is situated in data, that the data collected must be gathered and analyzed systematically, and that continuous interplay between the analysis and the data being collected results in the emergence of theories specific to the research context. This interplay between data collection and data analysis form the basis of the constant comparative method. This method is discussed in Section 3.11 – Data Analysis. Strauss and Corbin (1994) further stress that grounded theory "[M]ust include the perspectives and voices of the people whom we study" (p. 274).

3.5 Participants

The participants for this study were police personnel directly involved in the education and training of police recruits (N=8) at multiple police training academies across Canada. Participant roles and job titles include instructors, curriculum designers, and administrators responsible for police recruit training at their respective academies. Police academy trainers and administrators are the most likely to provide current, pertinent information relative to this study as they are in a position to qualitatively report on both the students and the expectations of police leaders. This study excludes police students/recruits, as they have not worked on the street and therefore cannot know any difference between training and practice.

Police training academies in Canada offer basic police officer training to either hired officers (post-hire academies) or to students who have not yet been hired by a police service but are required to complete recruit training before they are eligible to be hired by a police service (pre-hire academies). Despite the different employment status of the students, both types of academies were included in the study as they perform the same function – to educate and train recruits with the knowledge and skills required to work as a police officer. The researcher contacted the Canadian Association of Chiefs of Police (CACP) and was provided a list of the 14 police training academies and institutions responsible for basic recruit training of police officers in Canada were invited to participate. A list of Canadian police training academies can be found in Appendix A.

Due to the desire to achieve national representation in the study, and therefore be able to generalize the results, contacting any one police training academy might not have yielded generalizable results, given that policing needs and training in Canada are reflective of the needs of the communities that each service supports. Crouch and McKenzie (2006) identify that in qualitative research using interviews, smaller sample sizes (less than 20 respondents) allow the researcher to foster close associations with the participants while allowing for more in-depth inquiry.

3.6 Context

Canada is the second-largest country in the world by land area at nearly 10 million km^2 (worldpopulationreview.com, 2019). There are 37 million Canadians, 18.4 Million are male and 18.6 million are female (worldpopulationreview.com, 2019). In her report for statistics Canada, Conor (2018) states that in 2017 there were over 69,000 sworn police officers in Canada. Of these officers, 79% are male and 21% are female. Conor (2018) also found that as of 2017, 56% of police officers are over the age of 40 nationally, with the OPP having 66% of their police force over 40 years old and the Royal Newfoundland Constabulary (RNC) having only 42% of personnel over 40 years old. Ten percent of police officers in Canada are eligible to retire but choose not to (Conor, 2018). A total of 2,917 police officers were hired and trained in Canada in

2017, with 86% of these being new recruits and 14% being transfer hires (Conor, 2018). Conor (2018) reports that Canadian police agencies spend 14.7 Billion dollars per year. “Policing in Canada is administered on 3 levels: municipal, provincial, and federal services. In 2017, at the municipal level, there were 141 stand-alone police services and 36 First Nations self-administered services” (p.6). There are three provincial services and one federal service (Conor, 2018). Municipal services employ 38,911 police officers (56%) while 27% of all police officers work for RCMP. Conor (2018) reports a total of six provinces are losing more officers than they are hiring – led by Quebec (-146) and Ontario (-115), while four provinces showed a net gain – led by Alberta (+262) and British Columbia (+255).

According to Jewell (2013), there is no standardized police training in Canada. Some police services are required to send their newly hired officers to provincial training academies, (Ontario, Saskatchewan, and British Columbia) whereas other provinces rely on pre-hire police education models, such as in Manitoba, Quebec, New Brunswick, Prince Edward Island and Nova Scotia (Jewell, 2013). Many of the western provinces do not have provincial training academies, requiring each individual police service to train their own new recruits to suit the unique needs of the communities they service. The Royal Canadian Mounted Police (RCMP) is the only federal police service in Canada and they follow a post-hire training model, where newly hired officers are trained at the RCMP Academy in Regina, Saskatchewan (Jewell, 2013).

Creswell (2014) indicates that “[I]f a concept or phenomenon needs to be explored because little research has been done on it, then it merits a qualitative approach” (p. 20). In this study, the researcher does not know all of the variables that need to be examined, which makes a qualitative approach especially useful (Creswell, 2014). Creswell further states that qualitative research is appropriate if the topic is new and existing theories do not apply to the group being studied. This study meets Creswell’s criteria in that there is a small body of research that there is limited existing research, the researcher does not know all of the variables to be considered and examined, and there are no existing theories that directly apply to the participant group and research questions.

3.7 Interview Data

This study uses guided, semi-structured interviews (Lichtman, 2012). According to Cohen and Crabtree (2008), semi-structured interviews are suitable when there is a need to provide participants the freedom to answer interview questions and provide responses in their own terms. Semi-structured interviews involve the researcher having questions prepared beforehand to generally guide the interview and collect comparative qualitative data that is reliable (Cohen & Crabtree, 2008). Interviews are an ideal data collection tool when exploring an individual's perception about a phenomenon. Further, the researcher can follow up immediately to ask probing follow-up questions to clarify responses if a participant's response to an interview question is not clear. Individual interviews scheduled in accordance with each participant's availability are more feasible than trying to synchronize several participants' work schedules. Observation was not selected due to the nature of work of the participants. Surveys were not employed because the topic under research is complex and the situational aspects are constantly changing. This study required in-depth, in-person interviews with the police trainers.

Lichtman (2012) explains that different types of questions can be included in an interview such as questions that ask about knowledge or procedure, opinion questions and questions about experience. The interview questions were developed based on the gaps shown in the literature review that identified unexplored areas. A preamble to the interview is found in Appendix C.

As seen in the script, the researcher gives the participants an opportunity to confirm what has been said. Creswell and Miller (2000) identify this strategy for validity as *member checking*.

Member checking is important as it helps to ensure the authenticity, accuracy, and validity of the responses (Birt, Scott, Cavers, Campbell & Walter, 2016). Candela (2019) further states that member checking allows participants to reflect and expand on their initial qualitative responses.

Cohen and Crabtree (2008) address rigor in qualitative research, arguing that research should be ethical, important, clear, and coherent. It should use the appropriate methodology and be honest about researcher bias. It should establish credibility (by using participants who are knowledgeable on the topic. Finally, the research should look for ways to establish that the data are reliable (Cohen & Crabtree, 2008). The data in this research study were triangulated with current understandings of the context of law enforcement in Canada, and also through a careful, systematic analysis of the transcripts of the interviews, using the participants own words. Finally, Tracy (2010) states that qualitative research should also make a meaningful contribution to the field, and this is the intent of this researcher.

3.8 Procedure

This section outlines all of the steps undertaken to the complete this research in the steps listed below:

1. Submission of an application for ethical review to the Research Ethics Board at Ontario Tech University
2. Identification of the police training academies in Canada responsible for basic recruit training of police officers
3. Contact was made with each of these academies with a request to speak with an administrator or supervisor responsible for basic recruit training. If insufficient interest was shown, the researcher would re-send the request after two weeks.
4. A formal research proposal, was sent by email, to the on-site supervisor, describing the study, including the interview questions, and requesting formal permission to undertake

research within their organization. Also, the researcher requested the names of any persons on their team whom the researcher could approach with an invitation to participate in the study.

5. Email of approach was sent to any referred individuals (email correspondence will not include the individual's supervisor or referee). If recipient expressed interest, the researcher replied with the consent form (see Appendix B) and interview questions (see Appendix C).
6. The researcher organized the time and date for the interview. A day before the interview a reminder/confirmation was sent by email.
7. The interview was recorded using a handheld audio recording device.
8. Once the interview was completed, the audio was transcribed into an encrypted, password-protected Word document and sent to the participant for validity and member checking (Lichtman, 2012). Participants were afforded two weeks to submit changes to the transcript.
9. After the participant responded confirming that the transcript is representative of their opinion, the data were collated and data analysis began.
10. At the end of the study, the researcher agreed to destroy all audio recordings (DiCicco-Boom & Crabtree, 2006), and a link to the completed thesis was sent to all police training academies regardless of their participation in the study.

3.9 Consent

Informed consent was obtained from each participant before the interview in writing. According to Lichtman (2012), participants should be informed about the nature of the study and have the option to freely choose whether or not they want to participate. They should not be coerced. A researcher has to be aware that once an organization (such as a police service) has approved a study, that individuals in that organization may feel compelled or pressured by their peers to participate (Lichtman, 2012). For this reason, the researcher chose not to identify the participants in the study but only to report how many participants were included in the study. The researcher further emphasized to all participants that their consent to participate, or not participate was confidential. Kaiser (2009) states that confidentiality in qualitative data collection is of paramount importance in the collection of rich, detailed data. She further states that participants need to feel confident that their identity will be protected before they will share openly (Kaiser, 2009). Therefore, this study places an emphasis on maintaining the confidentiality of the participants and the security of the data collected. Participants were informed that their identity would not be shared with their employer or with anyone outside the researcher (Kaiser, 2009).

Lichtman (2012) states that participants need to be fully informed of the full extent of the study and she raises the issue that a study might take a different turn and diverge in a direction where the participant might not feel comfortable. For that reason, the interview script and the consent letter both emphasized the participant's right to withdraw at any point during the study without penalty and provided all of the questions in advance. A copy of the consent letter is attached in Appendix B. Other consents also needed to be obtained because each police training academy needed to consent to the research study as well. Approval to conduct research was sought from the Research Ethics Board. This is discussed in the overview of the procedures.

Of the 14 police training academies who were approached, eight academies responded with approval to allow the researcher to approach and invite specific individuals to participate in the study (N=8). During the participant recruitment phase, the researcher presented at a national conference encouraging pan-Canadian participation from Canadian training intuitions and this may have contributed to the excellent response rate. Each academy referred one participant, based on their knowledge of their academy’s police training curriculum, teaching practices, and observations of the students. The researcher contacted potential participants individually by email, as a means of increasing response rate (Roberson & Sundstrom, 1990). This initial email of approach included a summary of the study’s purpose and methodology. Once participants agreed to proceed, a consent letter was emailed along with the interview questions.

Consent was documented by the researcher and confirmed at the outset of the audio recorded interview. Interview were conducted using an online video conferencing tool called Skype (N=1), by telephone (N=6), or in person (N=1). Sturges and Hanrahan (2004) found that, given the choice, participants may prefer telephone interviews over face-to-face due to convenience and privacy concerns. Only the audio was recorded and transcribed for analysis. After transcription, participants were sent encrypted, password-protected files of the transcription and were invited to modify the transcript to ensure that it accurately reflected the participant’s views and opinions. Analysis of the transcript began after the participants responded with their changes. It is important to note that the researcher has no known personal connection to any of the potential participants from any of the police training academies contacted for this study.

3.10 Data Collection

Transcription was done by the researcher. All research study-related files, including audio files and transcription documents, were encrypted and saved on two separate external storage devices for redundancy and security purposes. Merriam and Tisdell (2016) suggests that data need to be organized and carefully annotated because the interviews blend into themselves after time and it becomes more difficult to remember which participant made which comment. The researcher developed an organized system in order to access particular interviews and also keep track of ideas which emerged while transcribing and preparing the data for analysis.

3.11 Data Analysis

The researcher analyzed the data following recommended methods (e.g., Creswell, 2014; Merriam & Tisdell, 2016), First the researcher created an inventory of the full data set so that it was organized and labelled. The researcher then examined how the data answered each research question because the research questions were the original organizers or categories for the questions. Next the researcher used inductive and comparative analysis to determine connections among the data, looking for what Merriam and Tisdell (2016) call "recurring regularities in the data" (p. 203). The researcher constantly sorted and compared the data and progressively identified useful themes and categories. The researcher constantly compared the emergent theory with the UTAUT theoretical framework using a process of constant comparison (Glaser & Strauss, 1967) to develop a theory that was more grounded in police training.

The steps followed for the grounded theory were: 1) coding, 2) category identification, 3) connections among categories, and 4) grounded theory development (Merriam & Tisdell, 2016). To begin to identify the categories, the researcher used open coding – adding notes to the data for any topic that might be relevant later (Merriam & Tisdell, 2016). At step 2, these notes were used to link or join the codes into tentative categories. Once the researcher had a tentative scheme of categories, then all the relevant data were added into these categories. The categories sometimes changed during this process. Next, the researcher moved from coding toward theory-building, looking at how the different categories were connected to each other. The researcher looked for how the categories connected to discern a possible theory to explain what was happening.

3.12 Constraints and Restrictions

This study had some constraints and restrictions. By design, this study examined only the recruit training programs and practices in Canada. Future research could expand this scope to also investigate training opportunities curriculum provided to police officers via in-service training. Despite a high response rate, not all academies participated. This study was limited to police recruit training personnel, but could be expanded to also include input from the students/recruits themselves, their coach officers, and police recruiters – each role has relevant knowledge and experience that could further the discussions surrounding the nexus of digital literacy and police practice. A document analysis comparing recruit training curricula across all police training institutions in Canada was considered, but given the contextual nature of police training (where training is determined based on the needs of different communities and the laws of different provinces), this avenue was not pursued.

Chapter 4: Findings

4.0 Overview and Context

These findings are presented based on the themes that emerged in the interview data and the strength of these themes, relying on multiple participants raising key points – sometimes with different opinions on the same topic. Elements of this research study are unique because small descriptive details which might seem important to the reader would compromise the guarantee of anonymity that the researcher gave to the participants. For example, a police academy can be identified by factors such as the stage at which recruits enter the academy (be it pre or post hire), the length of the recruit training period, the software, systems, or technologies they use, the length of the training period, and other training practices that may be unique to that academy. Training institutions could also be identified through a combination of these factors. In the interest of guaranteeing anonymity to the eight disparate training organizations, the findings are reported with as much specificity as anonymity allows.

This chapter describes the findings from research data collected and analyzed from the eight interviews. Five high-level themes emerged while coding and comparing the data: a) the backgrounds of participants, b) digital literacy, c) recruit training, d) changing models of training, and e) technology adoption. These themes are further refined into sub-themes and are identified, reported, and supported by participants' comments. The alignment of the research questions, interview questions, and data analysis themes are outlined in Appendix D. This alignment demonstrates that the interview data further understandings of the impact of the digital society on police training in Canada. This chapter closes with a summary that leads to the final chapter, Discussion and Conclusion (Chapter 5).

4.1 Similarities and Differences among Participants

The research participants in this study were recruited by referral from the primary contact at their respective academies. The criteria for selection was that the participant needed to be involved in – and have current knowledge of – the basic recruit training program(s) offered by their respective academies. Potential roles included administrators, instructors, instructional designers, and subject matter experts. Participants come from a variety of backgrounds, experiences and roles within their organizations. Half of the participants were instructors, and two were both instructors are administrators. Six of the participants had previous teaching or training experience ranging from 1-10 years and three participants had military backgrounds. The educational backgrounds of participants varied; multiple participants had completed a master's degree. Participants were also diverse in their geographic locations, with four participants representing training academies in the western provinces of Canada, three participants from provinces in central Canada, and one participant from an eastern province.

A key topic for all participants was the design and currency of the basic recruit training curriculum. In this study, the term "recruit" describes any student enrolled in basic training at a police academy. Due to the disparity in hiring requirements across provinces, the recruit training process follows either a pre-hire or post-hire model.

4.1.1 Need to Maintain Currency of Curriculum

The first theme emerging from the interviews with participants concerned the need to ensure currency in the recruit training curriculum. The term *currency* can be described as occurring in or belonging to the present time; therefore currency of curriculum involves ensuring that what is being taught to recruits reflects the needs and expectations of today's policing environment. Every participant mentioned the need for training content to be current given the dynamic nature of policing, the expectations of officers, the rules they are expected to enforce, and the processes by which enforcement occurs. They said, "Change is a continual process", and "Currency is very important – we work very hard on that", and "We are always looking for information to keep us current…it's a work in progress and it never stops." Another participant used the analogy of content currency as a "target", stating, "You have to continually assess how close to the target you are or you end up firing all day without hitting it." Another participant explained,

> The job changes fast, so we rely heavily on those new officers [instructors] who are coming in and their opinions on what is critical to the job and what needs to be taught. There are changes to the curriculum with every single course/class. We are in this perpetual state of [curriculum] tweaking, tweaking, tweaking.

4.1.2 Sources of Change

While there was consensus that change was constant, the sources that informed those changes varied. Changes to core content that come from new legislation, case law, and government ministries are mandatory, but other sources of change also influenced curriculum. These sources differed from one academy to the next, and included feedback from multiple sources, including: recruits and graduates; coach officers and mentors; instructors; specialty units, and police administrators.

Other information sources included current events, product training manuals, coroners' inquests, recruit evaluations, and various advisory boards and committees. Cultural norms were also a source of change, such as the need to ensure inclusive language on the training slides. Some academies assigned personnel to proactively visit other police agencies to observe their actions and to interview frontline officers.

Two of the participants mentioned a trend towards relying on academic research and evidence to inform training curriculum, using the term "evidence-based policing". Evidence-based policing is generally understood to mean that decisions made by police leaders are guided by evidence, such as academic research and statistical analysis, as opposed to the intuition, opinion, hunches, or other subjective factors. While participants believe evidence-based policing is not widely used now, they suggest that it soon would be. One said,

> Everybody is talking about evidence-based policing but we still have a long way to go. There needs to be more research done to support decisions that will impact training. If we want to promote evidence based-policing from the early stages of a career, there are information literacy skills that are important to gathering and evaluating evidence.

4.1.3 Recruits' Levels of Cyber Hygiene

Cyber hygiene can be described as the methods and steps taken by computer users to protect their identity and personal information online. Participants identified that recruits' awareness of their online presence is critically important in the digital society. Three instructors saw online safety as key in cyber hygiene – they want their officers to be safe when using social media and online tools and to be aware of the risks posed by their private and public online identities. They also wanted recruits to be aware that they represent both themselves and their police service in their online activity, such as social media posts and images, who they "follow" on various social platforms, and what they "like" on Facebook. Only one participant named a specific social media platform, the rest of the participants used the general term "social media", which is understood to mean popular platforms such as Facebook, Twitter, Instagram, YouTube, and other similar applications. A lack of cyber hygiene puts the police service and the judicial process at risk.

One said about recruits,

> They don't think about that if they ever get involved in a case, those images of themselves partying or whatever is what will end up on the cover of the [newspaper] or in front of a jury while the defense attacks their character.

Another said, “Social media can also devour police when decision-making is questioned.” This participant was likely alluding to how an officer’s online activity could cause a court official to question the officer’s objectivity or decision-making, thus undermining that officer’s testimony. For example, one participant shared a story of a recruit who had “liked” the Facebook page of a known motorcycle gang member. Five instructors saw the relevance of social media but two discussed how they teach social media, online presence, digital footprint and digital permanence with their recruits. They teach recruits that once they press “send” on anything, they have lost control over it.

One training institution invited the specialized cybercrime unit to speak with new recruits. The speakers surprised the recruits when they shared unique, personal information about recruits that they located in advance using publicly available online tools. One instructor described the recruits’ lack of awareness of their digital footprint saying, “I would hope some of the services are teaching this as [in-service training] now, but I wouldn’t guarantee it.” One instructor wanted recruits to be aware of what they had online and cleanse it saying, “[A] lot of services ask officers to give up their social media profiles.” One participant was considering a formal course on cyber hygiene. For others, cyber hygiene training happens “later” after recruit training, but did not specify at what point in the recruit’s career this would occur.

4.2 Digital Literacy

Instructors expressed mixed levels of understanding of the impact of the digital society. They demonstrated an overall awareness of the digital society, but there was a lack of consensus as to whether or not recruit training should include digital literacy skills.

4.2.1 The Role of Digital Literacy in Basic Training

Participants defined digital literacy differently. Two participants claimed that digital literacy focuses on technology use and comfort, while another defined digital literacy as requiring higher order thinking skills such as understanding, critical thinking, and creativity. One stated, "Digital literacy is more about critical thinking and collaboration. Our students, police officers, [and] the public need critical thinking skills to be able to validate information." Similarly, another participant raised the topic of information seeking and critical literacy, stating:

> Digital literacy means being able to use technology and technology tools like social media, communication tools, and networks to find what you need, to use information to create information… [it] is a skillset that is required to determine what information is accurate and identifying misinformation.

Every participant saw digital literacy training as important but there was a lack of consensus on teaching digital literacy at the basic recruit level. Most felt digital literacy was learned after graduating from the academy while others thought it was not required due to the age of recruits. Others still felt that there was no need to teach digital literacy skills to recruits because there were no identified core competencies related to digital skills. One stated, "One of the things we have to remember is that our program is *basic* training," while another stated, "We don't have a requirement or a framework for any digital competence so we don't teach that." Another explained,

> [Police graduates are] basically the initial call takers and first responders and they are putting out fires for the most part. Actually understanding how something works is not as critical to the employer as them being able to perform a specific function and get the job done….I believe recruits typically will be end users and not expected to understand the operative capabilities of cloud storage, retrieving data from cellular devices, and the like until later in their careers.

Still another stated,

> Right now, the recruits need to spend their time on the fundamentals. Learning

> the elements of the offence, and their authority. These are the core things…they won't be deploying the drone. They will be securing the scene and protecting the people and evidence, containing the scene.

Another participant commented that trainees would learn the technology while on active duty because they would be "forced to use it."

In comparison, some participants advocated strongly for the inclusion of digital literacy skills in recruit training, saying that recruits needed "this stuff" now and at a basic level. They argued that recruits need tech skills saying, "As technology keeps changing policing, we might have to find some way to do that...they need to be strong with technology." Still another said, "Technology is not a tool of the job – it is intrinsic to doing your job." For this reason, the instructor felt that recruits need an introduction to digital concepts in class so that it is not "alien to them the first time they see it on the street."

Other instructors saw it differently, stating,

> We do teach them about the use of the digital technologies in our environment that we use to deliver the program…I see our next major evolution of the [recruit] training program being the incorporation of technology-enhanced learning. We want recruits to look at scenarios through the lens of technology.

Another stated,

> I think that new officers need to understand and become proficient with the digital workflow of their agency. That is not something we can teach. They need to know how to get into the phone, they need to do some video surveillance, and they need to know how to work equipment…more and more of the technical aspect of their job.

The participants who were in favor of teaching digital literacy skills to recruits identified that this need arose from a general change to the duties of frontline officers. One summarized this saying, “The knowledge and theory on technology are important. I think they need a general idea about things like digital identity as a police officer meaning that they would be able to use any technology they need for their work.” In sum, participants’ views about whether or not police recruit training should include digital literacy skills were divided.

4.2.2 The Age of the Recruits

Instructors spoke of generational differences in policing and saw two generations: older officers, and “Millennials”. One explained, “They [new recruits] have grown up with a computer in their hand from day one and I grew up with a Tonka truck in my hand.” Another identified himself as an “Oregon Trail Millennial”, a term the participant used to describe people who had an analog childhood and digital adolescence. Participants said that Millennials have different skills and different challenges: they are gifted end users and consumers of digital technologies with which they are familiar, but they are not as familiar with the implications of the technology. One explained, “[T]hey are connected, they all use it…they are switched on. None of them come in here without a cellphone. This is an age group who don’t have to memorize anything – it’s at their fingertips, they just Google it.”

Four participants related technology comfort level to recruit age. Younger recruits are more familiar and proficient with technology. One said, “Last year we had an older group and they really struggled with [the Learning Management System (LMS)] and records management.” Another explained that,

> The standards are different for the younger generations like millennials. Sometimes experienced officers want to think about the arrest and the chase and they forget about how much the technology helps them. They think that humans come first and technology after…Younger recruits are happy with their

> cellphones but they have issues with desktop computers. They can tap the screen on the phone but are challenged to use computers effectively.

Each participant connected recruits' digital literacy levels to their age, but also said that being a "digital native" did not guarantee that they had "baseline digital skills."

4.2.3 Digital Literacy Levels of Recruits

The instructors recognized that recruits have digital skills that do not match workplace technologies. One instructor explained that academies spend more time placing restrictions on the recruits' use of technology ("using the reins") as opposed to pushing them to use technology ("using the spurs"). One participant described the recruits' levels of digital literacy in this way,

> Their ability is incredible. …. we start by telling them how to get to the document and halfway through the instructions …they are already there – they've already found it. I'm blown away with the literacy and how fast they can navigate the waters of an unknown web-based site. They can just go onto it and intuitively find their way through it, where I have to try several different paths.

Interviewees distinguished among digital skills finding that, for example, the recruits can touch, tap, and swipe, but not keyboard. Instructors cite different skill deficits – typing, formatting a page, using bullets, inserting tables and other functions. One said, "The adoption and the interest is there, but the skills aren't. They know what they need to know at a surface level but don't get anything beyond basic end users." Another found that recruits struggle with the differences between texting and emailing and between internal and external communications. One said that the rules needed to be taught while another said the rules held them back, saying,

> They are not limited by the technology or by their ability, but by our rules on how they can use it. …with our rules we risk stifling that creativity, but it's for their safety. In the end we want to help them use their technological powers for

> awesome and not evil.

They also said that the recruits tend to be more digitally literate than the instructors. One instructor said, “If it can be done, they already know how to do it.” Another said, “Recruits are very comfortable with using social media, such as Facebook, Instagram, Twitter and they all have cell phones.” One instructor described their skills this way,

> They are so quick with computers. They can set things up and navigate things, where I’m calling the helpdesk... There is nothing we throw up that they [the recruits] can’t pick up... They are very receptive to learning about anything digital.

Some negative aspects of recruits as “the smartphone generation” were mentioned. One participant said that many of the recruits do not realize that they are addicted to their phones. This instructor wanted to teach recruits how to deal with crime from their phones, saying that they “get the tech but not the consequences” and they can be “clueless as to the implications.”

4.2.4 Recruiting and Digital Literacy

The participants identified that their biggest challenge was finding qualified applicants. Some have challenges attracting recruits who are digitally literate. One stated, “We are competing with the private companies for these employees and the private companies will cater to those expectations and usually for more money.” This apparent contradiction in the digital literacy levels of recruits can be attributed to the different ways participants defined digital literacy. Participants said that digital literacy has not been recognized as a formal requirement for policing and is not part of the hiring process. Asking applicants about their digital skills is up to the discretion of the recruiter. Participants suggested that baseline skills such as keyboarding and word processing should be part of the recruiting process. Recruits should have “some basic understanding of how to use the computer” and decent typing skills.

They should be able to navigate a cellphone and a tablet. One said that recruiters could look at the “pre-existing knowledge, skills and education that a recruit brings to the table” in order to determine if an applicant could be directly posted to a specialized unit and bypass basic recruit training.

The most popular view, however, was that digital literacy skills are inherent in the young recruits. One said, “We often expect these young folks to be the ‘digital natives’. Most young people had access to technology in high school and grew up with it.” Another participant stated,

> I don’t believe that they need [digital literacy courses] given the level of knowledge that they come in with. That would be lost on the majority of the audience that the police service is trying to attract. It’s like giving the birds and the bees talk to a group of 30-year-olds. If we need to teach [that] to recruits, then it’s a big problem and means we missed the mark on recruiting. If we are teaching about basic digital literacy at this stage…in the game then we have a problem with who we’ve hired.

In short, participants saw that competition from the private sector, a lack of recognized recruitment requirements for digital competencies, and the presumption of pre-existing digital skills all impacted the digital literacy levels of recruits.

4.3 Recruit Training

Participants shared their opinions on what should be taught to recruits in basic training. This opinion was influenced by two primary factors: the coaching and field training stage and the changing role of frontline officers. These factors, along with the need to provide specialized cybercrime training to recruits is also discussed in the following subsections.

4.3.1 Coaching and Field Training

Coaching and mentoring in policing were seen as critical for recruit learning. After academy graduation, most police services pair up the recruit with an experienced frontline officer (called “coach officers” or “patrol training officers” (PTO)). This field training with the PTO is designed to familiarize recruits with the unique operations and expectations of their respective police services and is designed to provide context for their academy learning. Multiple participants see that there is a lack of standardization of this stage, as each police service is unique in its approach to policing, the needs of the community they police, and the computer systems and digital technologies they use. One participant said that if a standardized model was to be achieved, then the recruit trainers needed to “own” the coaching phase. There was general agreement of the need for more linkages between the coaching stage and the recruit training stage. This is significant as most participants view the field training as the stage where recruits are exposed to digital technologies. One stated, “That is all going to be taught by their coach officer when they get to their respective service... a lot of that [technology learning] is going to be on-the-job.”

These job-specific technologies include specific software for records management, evidence handling, note-taking tools, and mobile apps (specific names of software tools are omitted to protect the anonymity of participating academies). One participant said, “When recruits do go out into the second phase when they are out with their police training officer, then they are going to get more experience with the programs that they use on the daily basis.” There is variation of radio systems, interview recording equipment, officer equipment such as BWC, and roadside tools. This is reported as a training challenge. One participant said, “[T]echnical skills are so specific to each organization that they will teach those skills there.”

In sum, participants saw a need for standardization of the coach officer stage of recruit training, but this remains challenging given the unique needs and expectations of each service.

4.3.2 Changing Role of Frontline Officers

Most participants reported that the role of the frontline police officer is changing due to the need to be able to identify and preserve digital evidence and, the need to appropriately respond to "volume cybercrime" – a term meaning that cybercrimes have drastically risen in volume and present a greater number of calls for service. Some debated if frontline officers should receive specialized cybercrime training. One participant stated,

> Early on we do an introduction to cybercrime, but to be honest that's a sector of policing that I think we are probably the most under the gun and behind in…Its probably one of the most nebulous and misunderstood sectors of policing…more and more commonly our investigations are going online or going from the physical world into the digital world and many, including myself find it hard to navigate back and forth between those worlds…we do not have the capacity to adequately train officers to do that at this point.

Another said that they would need to cope with volume cybercrime, explaining,

> All of our volume crime teams in policing are set up to deal with physical issues such as shoplifting, thefts, common assaults, domestic assaults…They are not set up for cyber…We need to come up with some way of dealing with all of the traditional stuff (such as abuse) but now being done online….We need to be able to deal with those ransom demands. The criminals are so sophisticated and they research their targets now. They use open source data to create profiles of their victims and they exploit people's weaknesses and extort money from them. I hope that we will be teaching this stuff in the next few years.

When discussing cybercrime, four participants thought that frontline officers should not be expected to possess a specialist level of knowledge to deal with digital evidence. The consensus among participants was that the frontline officer would identify and preserve digital evidence before handing the call over to specialized units who received in-service training above and beyond that of basic recruits. One disagreed and said front line officers needed the training to respond to calls that involved “bullying and criminal behavior posted to social media.” This participant said that recruits needed to know how to analyze the social media content to identify risks and identities because “specialized investigation units may not always be available.” Similarly, another participant said that specialization may no longer be appropriate for today’s crime landscape, stating “In the next five years I think we will see the de-[specialization] of positions [where] we shy away from the uber-specialized positions and employing police officers in those capacities.” This participant continued, “We cannot be efficient as a police service if officers are limited by specialization…We are entering an era where we need to change our structure to provide tiers to these specialty functions.” This participant did not clarify if they meant only specialized cyber units or specialized units in general.

Another participant felt that specialization units would remain, but would no longer be comprised of sworn police officers, stating “We are looking at civilianization to solve this problem...to fill that skills gap.” *Civilianization* is a term used to describe the hiring of non-sworn police personnel to complete tasks previously reserved for sworn police personnel. This same participant was not certain of this position, stating, “There is a whole other set of competencies you develop when you are that frontline officer, which sometimes makes stepping into specialized roles go more smoothly.” One participant said that “Even officers in specialized units sometimes find course content to be "well beyond their level of digital literacy." In summary, most agree that the role of the frontline officer is changing because of cybercrime and the prominence of digital evidence, but there was no consensus among participants as to if specialized cyber skills should be included in recruit training or to which level these skills should be taught.

4.4 Changing Models of Training

Participants were asked to identify possible changes they would like to see to their recruit training. Many responded by explaining their current pedagogical practices. These are summarized in the following subsections: learning theories, training models, and training challenges.

4.4.1 Pedagogy in Police Training

Each participant discussed the pedagogical approaches used in their recruit training. These included: adult learning principles (andragogy), flipped classrooms and blended learning, the need for more experiential learning, and concerns with cognitive overload felt by recruits. Five participants mentioned adult learning approaches. They reported using flexible classrooms with movable furniture and they recognized that adults learn differently. Some academies use blended learning, and some blend online learning with face-to-face instruction through third-party providers. Multiple participants use the *flipped classroom* approach, where recruits learn content on their own time and then analyze and synthesize that material in class. One stated, "[T]hey study everything before they arrive [for class] to learn the theory and information they need to read through [our LMS]". Another said that the flipped classroom allows recruits to "…ask the teacher the hard questions."

Experiential learning opportunities are seen as important, including the need for high fidelity training environments (usually simulations) and the need for the learners to situate the training content in their experience. The participants saw the lack of context for learning as a challenge. Each academy worked to create or simulate that context for the learner. "They need context for what they are learning." said one participant, who reported that recruits accompany an active officer for one shift to observe the officer, but found that it is not sufficient, stating,

> Most of our recruits have never seen live policing so we are giving them knowledge in a vacuum because they don’t know what this job looks like. I think we need to give them a snapshot to help them ground that training in experience.

Another said, “We bring crown prosecutors and judges in to talk to the recruits about testifying – like a mock court trial...We like to add life to these concepts so that the recruits don’t have to imagine the context – they experience it.” Live simulation exercises were prominent in all academies, where scenarios included a variety of common police calls for service, such as responding to retail store robberies and domestic disputes. One participant said they use hired actors, (usually off-duty officers) who come in on their own time to act in the scenarios. Participants identified that live simulation exercises used a lot of physical space and injuries are common. Another said, “The recruits love the live simulation exercises, but they are very expensive and I have to prove the ROI (return on investment) [to our leaders and decision-makers].” In comparison, some participants found that simulators lack the fidelity to simulate the real environment. One said, “It’s just not real enough”. Another said, “The simulations need to be interactive and reflect the reality of their work, and right now our simulators are very good but they don’t quite do that.” Several saw that virtual reality would assist. One stated,

> It [virtual reality] allows for so many more scenarios than live actors; it’s more immersive, more consistent training, uses less space, is easier to record, can be used more often at all hours, can be interactive and responsive to the student’s decisions, and has less training injuries. It’s a totally different way to do scenarios which are so important to their training.

Another stated,

> Virtual reality is a technology I would love to add… I would love to see where we can bring on more technology. Maybe better simulators and virtual reality and

> fidelity to the simulations. The simulations need to be interactive and reflect the reality of their work, and right now our simulators are very good but they don't quite do that.

Another participant summarized the discussion on virtual reality, stating, "[W]e are trying to make sure that the training environments in certain situations are as real to life as we can make it...We are going to have to keep up with whatever technology supports that training goal."

Cognitive overload is an issue that impacts how much technology can be introduced. One said, "I'll say it this way, they're drinking from a firehose… I think they retain only a percentage of what they learn from us at the academy. They are so overwhelmed… it's like brain overload." Another said, "[T]he fire hose is overwhelming. There is so much information, skills, tactics, strategy, law, policy…They don't have time to think about what they aren't learning nor do they have the capacity to take on more." Another stated:

> They are so overwhelmed with their stuff they are not asking to study something else. There is so much that they are trying to learn and remember…We are always trying to make sure that we don't give them cognitive overload but we have to teach them as much as we can because for a lot of them this is the last training they get before they go on their first shift.

Possibly because of the volume of curriculum and the cognitive overload, the instructors use both formal and informal learning to teach recruits about digital technology, and they reported that there are no formal courses on digital literacy. One training group offers a course on internet use that focuses on, "building awareness of their online social presence, their digital footprint and things they should be aware of as new police officers in a world of social media." Other academies offer recruits some formal training on the use of records management systems.

Informal methods are used to teach skills such as email etiquette as technology skills "are being taught as a bit of a sidebar." Another participant stated, "Recruits may learn some digital skills through their use of the LMS, videos, and other software in the classroom, but there are no formal literacy courses offered." Another said that, "[W]e hope that by making students use technology they will also learn about technology and why technology is important and why they need to be strong with technology." One said, "That stuff is discussed anecdotally in class but is not part of the formal curriculum. We tell the students about things like kill switches on power systems that can be used to destroy evidence using electromagnets."

Participants recognize that digital technology skills are important, but the volume of traditional training content limits opportunities to include digital content at academies where training time is short. Longer training periods were identified as having more opportunity to include training courses beyond those that focused on officer survival. One participant stated, "We only have [a few] weeks with these recruits, to add digital literacy means something else would have to go." Another said, "We can't. There just isn't room or time for that kind of training in our program right now… but we just don't have the time." Another said, "Sometimes they [graduates of the recruit training] suggest changes and I ask them, ok, 'What would you take out in order to add that?' … Training is too short. I would continue it on longer." One stated, "We get these recruits for [x] months, but it seems like I could keep them twice as long. The amount of information that we have to convey is almost endless…"

According to one participant "There is a lot of disparity in Canada when it comes to the length of officer training.", and that recruit training programs in Canada range from two to six months in duration. This prompted one participant to state, "You can't produce a good officer in [a few] weeks – that's the 'Don't Die' program." The cognitive overload, the amount of curriculum coverage, and the time allocated to training appeared to impact both what was taught and the teaching models used.

4.4.2 Traditional Models Persist

Six participants identified the teaching approach at their academies as “lecture-based” and involves “passive learning.” One stated, “The program is basically the same since I've been here”, and “We still use passive learning model where they pick one or two officers to go through the scenarios and everyone else watches. It’s very scripted.” When discussing lecture-based classroom, one participant said, “[R]ight now we are very PowerPoint driven." One described their training as “[e]xtremely paper-based with rows of desks facing the front” which “did not promote communication and collaboration.”

Multiple participants pointed to the paramilitary nature of policing in connection with the use of traditional approaches. One said, “If I see [a cellphone] out then we are going to be doing pushups.” Participants recognize this can limits students’ opportunities to express views on digital technologies. One said, “[T]here is that military mentality where students will do whatever the instructor requires of them and don’t usually challenge or ask questions.” Another stated, “[T]he culture internally is such that [recruits] use the programs because they are told to, not because they want to.” Participants’ views of the paramilitary approach varied. One explained that, [T]he military does this very well.”

In sum, there were a number of training issues affecting digital literacy. The next section offers more participant views on technology-related aspects of technology adoption.

4.5 Technology Adoption

Technology adoption was an important topic for every participant. This finding supports the use of the UTAUT model as part of the theoretical framework for this study. The UTAUT model considers several factors such as gender, age, experience, and voluntariness of use as having the ability to influence and modify the four key constructs of technology acceptance: 1) performance expectancy, 2) effort expectancy, 3) social influence, and 4) facilitating conditions. The UTAUT model posits that these are the factors that most affect a user's intention to use technology. While gender did not arise in the data for this study, age, experience, and voluntariness of use were frequently discussed. These and other factors are discussed below.

4.5.1 The Experience of the Participants

Participants said that they had varying levels of digital literacy. Two describe themselves as highly digitally literate. Another is "pretty good" at technology, while another said, "I'm a geek. I love it." Others report being less digitally literate, describing themselves as "the least technologically advanced person" or having minimal skills or a "techno-peasant." Despite this range, each is aware of the digital society and the rapid rise of technology in policing as "the crime landscape now." Another said, "I know there are more and more technologies being used by society, but I'm not sure which will be used by police." One commented that "Technology doesn't stand still; it will keep changing." One recognized changes in data saying, "There is an increasing demand for technical literacy… if we don't understand how that information is produced, created, stored, accessed, then how do you become authentic, evidence-based police leaders without those literacy skills?" Another said, "We are at a point in society where that digital literacy is at a level where it is not a big deal to introduce [technology] in the workplace."

Most participants report that their instructors are current, serving police officers seconded to work at the academy based on their subject matter expertise and experience. Nearly all participants see the instructor as the "deliverer" of a curriculum designed by others such as the curriculum designer who creates the teaching points. Another stated, "[T]his model ensures consistency of delivery – it's not subjective to the instructor's beliefs or which part they deem worthy of transmission." Some saw that instructors have some flexibility in the method of delivery. One participant knew that technology can be used to substitute a traditional method such as using a PowerPoint instead of writing on the wall. In general, they viewed the instructors as having low levels of digital literacy with one saying, that, “As far as digital literacy there is definitely something to be desired there.” Another explained, “Some instructors are subject matter experts but are not very comfortable with technology …We have instructors for whom technology is a middle level issue…Both in comfort and ability.” Still another said, “I think most struggle with the tools and technologies. While some of them have smartphones and laptops of their own but…not many of them incorporate these into their subject areas.” The technology adoption of instructors is a key issue. One stated,

> As for the instructors, I think as a collective they are probably very used to or comfortable with what they know, but as soon as it’s something that they don’t have to do very often, or if it’s something that they recognize has a significant amount of consequence if not done correctly, people do back off pretty quickly. There are not very many who are going to take the time to figure it out… it’s 100% a comfort level issue.

Another stated,

> [The instructors] feel technology is time consuming and they are not properly well-versed themselves in its use. They are intimidated by what they don’t know or what is expected of them if they use technology. They aren’t tech support and don’t want to look bad in front of the recruits. Technology adoption is definitely low here especially among faculty.

4.5.2 The Impact of Age on Technology Adoption

The age of the instructors is seen as a factor in technology adoption. One said, “People who are a few years on the job are really being forced into using it in a way that they don’t really like.” Another said, “We get a little bit of resistance from experienced officers but less and less as time goes on because the age group is getting younger." In comparison, one participant saw instructors as "fluent" in digital literacy. Some thought that increasing the instructors' levels of digital literacy would improve the overall learning experience. One participant stated, "Instructors needed certain skill sets to be able to leverage them in the training…I don't think they are scared of it. I just don't think that they understand it…they don't know how to get there." These comments indicated that instructor familiarity with technology presented a barrier.

4.5.3 Technology in Training

Despite early statements on traditional pedagogy, participants identified that digital technologies were being used in their academies; however, the volume and types of digital technologies varied across academies. One said "[W]e do not introduce much technology to the recruit program." The majority of participants, however, indicated that a variety of digital technologies were used to teach and train such as: body-worn cameras, digital/electronic note-taking, IP video and audio recording, Chromebooks, iPads/tablets, online polling software, smartphones, laptops, computer simulators for driving and firearms training, and in-vehicle technologies such as automated license plate recognition cameras.

Multiple academies use an LMS and mentioned LMS use for e-learning. One said, "[Our academy] has a learning management platform and I use that extensively. All my stuff is posted online." Another said, "[A]ll lesson content is accessible to them. Some students like to read ahead to figure out why they are learning something and where the instructor is going with this." Five participants state that their academies employ videos as part of their teaching. They create their own videos for instructional purposes. One said, "I develop videos and post them on YouTube and share the links" while others engaged third-party vendors such as the Canadian Police Knowledge Network to provide instructional training videos. They reported using video recordings of simulations "for feedback and self-reflection." One said,

> Each of the defensive tactics moves now has a video so that students can practice and perfect technique. Same as firearms training. This also helps [ensure consistency in] what we are teaching their officers. Lastly, the videos help the recruits articulate what move they were performing [and why].

Body-worn cameras, smartphones, and laptops are used in some training. Mobile devices create videos. IPads were often mentioned for “recording, instructor feedback and self-evaluation.” They are also used for record keeping and assessment.”

Smartphones were the most polarizing topic. One participant said, “We know that cellphones are becoming a common tool used by police and the research is showing that most organizations are pushing for mobile technologies.” That service was seeking an LMS that was mobile-friendly. Half of participants identified that recruits are not allowed to have cellphones in training and that the use of mobile devices in the classroom is rare. One said, “I’m probably the only one who regularly uses those kinds of technologies and devices for training purposes… our policy is that cellphones are not even permitted in the building during training.” Participants reported that recruits were “addicted” to their smartphones. One said, “You can almost see them sit there and twitch. They just need to connect.” Another stated,

> They are so connected that we actually have to break their addictions to their phones. They are so used to walking around with their faces in their phones, but if they do that with a gun on their hip, they are going to get in trouble… [M]any of them don’t even realize that they are addicted to their phones.

One participant identified that cybercrime training was offered to recruits. Multiple participants indicated that cybercrimes are discussed anecdotally. One said, “We don’t have any courses specifically on technology, like teaching cybercrime.” Another said, “I tried to once… and the feedback I got from the recruits was that this was above their level of what they felt they needed as a basic recruit so I stopped offering it.” Cybercrime training was offered at multiple academies but was reserved for experienced officers. One stated, “If you look at cybercrime, for example, I think rudimentary online or cyber involved investigations will, probably sooner than later, become a ‘common dog’ part of policing that will work its way into recruit training.”

4.5.4 Barriers to Technology Adoption

As one participant astutely identifies, “There are two things that police officers hate, and that is the way things are, and change.” Technology challenges are substantial barriers to the adoption of technology in recruit training. Issues include: unreliable technology, lack of user-friendly software, and a lack of software specifically designed for police training environments. Access to “test environments with sample data” was in demand but unavailable, and training with “live” data was prohibited. Trainers reported that they resort to “tabletop exercises” that restrict recruits from engaging with digital technology. A third stated,

> Sometimes technology fails, has bugs and glitches, which is normal, but instructors who are already not interested in technology get very frustrated when it doesn’t work. Their opinion against technology is biased and their use of technology is affected…some instructors think that it’s extra work and are not 100% on board with the technology.

In addition to these issues, the majority of participants saw disconnects between training needs and decisions made by the IT department. Most frequently mentioned was the conflict between IT’s need to maintain operational security of information and the trainers’ needs for open and accessible software and systems. Data created by police departments is highly confidential. Access to materials for training conflicts with security needs. Recruits cannot collaborate openly online because of the sensitivity of the information. An LMS behind a firewall creates a barrier.

Another issue raised was connection speed. This caused developers to have to embed video rather than letting the recruits search. One training service reported that they "finally" have a Wi-Fi system that supports "the use of a mobile device of some sort." One issue that was raised as a barrier was that instructors find that technology is more work and they question its value.

Cost is another barrier. One participant stated, "I suspect that the reason some of the other police services haven't adopted these technologies is the costs. Storage, servers, and technical support are all expensive." Another said, "Another challenge is ability to procure software that aligns with the requirements of all of our partners" such as bilingual software.

4.5.5 Budgets, Resources and Admin Support

The cost of technology is another barrier, or in the words of one participant, "Cost is a big thing." They would like to have more technology but it requires a bigger budget. This is especially a challenge for smaller academies. One instructor explained that recruits expect a lot, and said that unfulfilled expectations of recruits may lead them away from technology:

> We have people who grew up playing Halo and other video games that companies spend hundreds of millions of dollars to create and make billions of dollars selling, and that becomes the [recruits'] expectations for a simulated environment. They are familiar with an incredibly high-fidelity virtual environment. We don't have that budget or ability to meet the standard set by those companies.

Half of the participants articulate that the administration needs to be persuaded to adopt technology. One said, "We are hoping to show the administration the value of a technology-centric approach to learning and prove that this next big change is a worthwhile investment because we can't make major changes like that without funding." Another stated, "[H]opefully once we can get some better support, then we can start to bring in more interactive things into the classroom." Another participant identified a "tug-of-war" for management in that there was pressure from the trainers to increase the length of training which conflicts with the organization's need to put officers on the street, stating, "[E]very time we add to the training time there is the potential for pushback." A third participant linked a lack of support from police leaders to their age, stating "I think the older police leaders need to think technology first, and until they do, the training is not going to change [to include] digital technologies."

4.5.6 The Impact of Emerging Technologies on Adoption

Six of the eight participants see that emerging digital technologies will impact police training and practice. "We cannot avoid these technologies" said one participant. Another identified that the technology was advancing so quickly that their training academy was challenged to keep pace and had been looking at industry partnerships to maintain technological currency, such as moving towards more app-based learning methods. While multiple participants mentioned mobile apps, a number of other prominent, emergent technologies were mentioned such as: the use of drones; mixed and augmented realities; activity trackers; augmented reality (such as Microsoft's HoloLens); facial recognition; data mining; video recording technologies for police vehicles; automatic license plate recognition; navigation systems and incident management.

Multiple participants mentioned the growing adoption of police body worn cameras, but voiced challenges to adoption that included privacy concerns, officer discretion, and infrastructure costs to support. One participant stated, "I am not sure where we are going to take body cameras… Privacy is a battleground – look no further than number plate recognition cameras. There is a point at which society won't put up with being surveilled." These discussions aligned with comments made about the digital society.

4.6 Summary of Findings

This chapter identifies a number of primary and secondary themes that emerged in the analysis of the interview data. More than 40 themes were identified and collapsed to form five overarching themes. These findings and themes are summarized in the table 4-1: Summary of Findings. The next chapter examines these findings through the lens of the themes identified in the literature review, and makes recommendations for future research in this area.

Chapter 5: Discussion and Conclusion

5.0 Overview

The purpose of this research study on digital technology and police training was to identify how police recruit training in Canada is impacted and influenced by an increasingly digitally-dependent society. The secondary purpose of this study was to add to the current body of literature surrounding the nexus of police training, digital literacy, digital technologies, and technology adoption. To accomplish these research goals, this study took a qualitative research approach that utilized exploratory interviews with eight participants who work at recognized police recruit training academies in Canada. The data from these interviews was summarized in Chapter 4 and reported based on the strength of the themes in the data. Those themes were grouped and coded based on their ability to answer the research questions that have guided this study. This chapter employs a similar organizational approach, as the research questions provide a discussion framework.

This chapter analyzes the interview data themes through the lens of the themes pulled from the review of the literature (See Chapter 2). There were a number of themes that were common to both the Literature Review and the Findings, while some were present only in one or the other. Additionally, this chapter examines the study's data through the lens of the theoretical framework of technology acceptance (the UTAUT model) (Venkatesh et al., 2003). This chapter closes with a section on the limitations of this study and makes recommendations for future research in this area.

5.1 Question #1: Impact of the Digital Society on Police Training

The primary research question was "In what ways do current police recruit training academies in Canada recognize the digital society?" Chapter 1 discussed how the literature supports the position that society is increasingly dependent on digital technologies. In Chapter 4, participants repeatedly discussed the ways in which society's penchant toward digital technologies are impacting policing and police training, referring to what they call "the new crime landscape".

One finding was the need for recruits to understand the ramifications of their online presence. For example, encouraging recruits to be aware of the ramifications of their social media posts and other online activities with respect to impacting an officer's credibility in court. One participant stated, "Social media can also devour police when decision-making is questioned." However, the emphasis on the need for recruits to be taught the possible consequences of their online activities was less prominent in the literature. The need for officers to be aware of social networking sites as powerful investigative tools was prominent in both the literature and the interview data.

Both data sources included the substantial rise of cybercrime (Cockcroft et al., 2018) and the exponentially increasing number of calls involving digital evidence (Hitchcock, 2016) as key phenomena affecting policing. The literature strongly suggested the inclusion of these factors in recruit training, however the participants in the study were divided as to when recruits should be taught cybercrime and digital evidence skills (before, during, or after basic training). There was consensus from both data sources that policing has become increasingly digital with respect to the tools of the trade and the dependence on information. There was consensus from both data sources that the role of the frontline police officer is changing as a result of these phenomena (Bossler & Holt, 2012). The literature posits that a lack of digital skills among officers could result in the mishandling of cyber-related calls for service (Goodison et al., 2015) is an issue requiring immediate attention. The participants however did not mention this issue.

The combination of these findings supports an overall need to recognize that cybercrime, the increasing use of digital tools by police, and the increasing prevalence of digital evidence from multiple digital sources requires a paradigmatic shift in the way police officers execute their duties. The role of the frontline officer is being redefined and currently, the digital skills of frontline requires the same redefinition. Officers need to recognize that every person they encounter is part of a digital community. As such, officers need to view citizens as having both digital and physical identities, activities, and lives, and need to consider the opportunities for evidence and crime in digital form. This recognition needs to come early in training or sooner than it appears to be happening.

5.2 Question #2: The Adoption and Teaching of Digital Literacy Skills

The data from both the literature and the participants consistently mentions numerous issues surrounding technology adoption in police training and practice. Participants raised challenges with technology adoption, including a lack of instructor comfort with technology, issues with reliability, bandwidth and other issues with technology including administrative support for increased technology use. The literature cites similar factors impacting technology acceptance and use by police, and further linked technology acceptance to citizen trust, police efficiency, and a lack of technology-based training (Lindsay et al., 2014).

Both data sources identify the impact of age, past experience, and "voluntariness of use" (the level to which the user sees their technology use as voluntary or as forced upon them), technology adoption, as well as the critical role police leaders play in supporting technology-based tools and training. Participants reported that younger recruits and instructors demonstrated higher levels of technology adoption, which was consistent with the literature. Similar congruence was found surrounding the negative impact of *forced use* on technology adoption, with multiple participants discussing the negative impact of forcing technology use on instructors and recruits, which resulted in a lack of interest in using a specific digital tool.

The possibility needs to be raised that low levels of technology adoption in recruit trainers may be negatively impacting the abilities of new officers to police a digital society. Greater adoption of digital technologies in the recruit training environment would better prepare officers to police the new crime landscape. Increasing technology adoption can be accomplished through various methods, from new models that involve low and high adopters working together to partnering newer officers with cybercrime specialists. Low levels of technology adoption among instructors and police leaders could be mitigated by encouraging them to experience technology-assisted learning environments as students. Although this may seem contradictory to the present reporting structure, it would allow them to see the benefits of newer methods. Increasing technology use at the recruit training level will encourage officers to view technology as central to police training and practice, rather than optional.

5.3 Question #3: The Role of Digital Literacy in Police Training

The topic of digital literacy featured prominently in the interviews and the literature. Both sources identified challenges with defining this term, but there was consensus from the participants that digital literacy implies the ability to both use digital tools and to understand the implications of that use. Both data sources defined digital literacy as being more than basic use of digital technology and placed emphasis on the overall awareness of how digital technologies work and are integrated into other primary functions of policing.

Both the literature and the participants reported that age is a key indicator of digital skills and comfort using digital technologies (Seawright, 2012), but participants believed that age alone did not guarantee the possession of “baseline digital skills”. Participants felt that the digital skills of younger recruits were generally high, which contrasted with the literature finding that digital skills among police officers were lacking. This lack of congruence could be attributed to age, as the literature did not specify if it was younger or older officers who struggled with digital literacy. The need for police officers to possess baseline digital skills was prominent in the literature but less so in the interview data, where participants were divided as to whether digital skills should be the exclusive purview of specialized cybercrime units. The topic of specialized units is further discussed in the next section of this chapter.

The literature identified that there was an issue with police agencies identifying pre-existing digital skills – either among current officers or new recruits (Stokes, 2010). This finding was supported by participants, who believed that police recruiters should seek pre-existing digital skills among applicants. One participant stated, "If we are teaching about basic digital literacy at this stage in the game then we have a problem with who we've hired." However, both the literature and the participants identified multiple challenges with recruiting cyber-talent (Sturgeon, 2015), citing competition from the private sector and the paramilitary nature of policing as deterrents to recruiting. The issue of low digital literacy levels among instructors responsible for recruit training was strongly represented in the participant data but not in the literature. The role if the instructor is further discussed in section 5.5 of this chapter.

In response to the research question, there is consensus that digital literacy is a must in policing and police training with multiple options for training digitally literate officers from recruiting candidates with pre-existing digital skills to developing digital skills in either recruit or in-service training. Police leaders cannot assume that digital skills are present due to age or proficiency with handheld devices, but instead should look to establish the core competencies related to digital literacy and then design training to those objectives. There should be a clearer continuum of digital skills development in police education that measures digital competency before or at recruitment and throughout every officer's career.

5.4 Question #4: Relationship between Police Activities and Academy Training

Both data sources report that recruit training generally reflected actual police practice, with some notable exceptions. Half of the participants indicated that recruits were not permitted to use their smartphones during class time, whereas the literature indicates that the use of smartphones is common police practice. Multiple participants indicated that recruit training was designed to prepare officers for their first day on the job, and was therefore focused on those skills that related to officer survival such as driving, shooting, use of force, and other physical skills, however the literature indicates that these tasks represent a small percentage of officer activities (Giovengo, 2017), finding instead that officers spend more time solving problems, thinking critically, and fostering relationships with the community (Deverge, 2016).

There was also a lack of consensus on the inclusion of cyber-skills in recruit training. Whereas the literature strongly favors the need for recruits to learn these skills (Cunha et al, 2016; Hitchcock et al, 2017), several participants believed that cyber skills should be developed later in the officer's career, for example if the officer chose to enroll in a specialized cybercrime unit. The topic of specialized cybercrime units emerged in both the literature review and the comments of participants. Both indicated a lack of consensus as to the merits of relying exclusively on specialized cybercrime units (Harkin et al., 2018) as opposed to a tiered approach which involves providing baseline cybercrime training to all officers.

There was also consensus between the data sources on the importance of the time recruits spend with their coach officer after graduating from the academy (Koper et al., 2014). While both data sources identified the value of the coaching stage as the bridge between recruit training and police practice, three participants indicated that this stage is of such importance that it should fall under the oversight of the training academies and not the respective police agency. This view was not reflected in the literature.

The findings indicate that the use of digital devices in the field, such as smartphones, video cameras, and other roadside tools are increasingly used in police practice, yet few academies offer training on mastering these tools – in fact, some of these devices are prohibited by recruit trainers. A greater emphasis on the problem solving, analysis, and critical thinking skills for recruits would better reflect the realities and challenges of their impending duties. The finding that the role of specialized cyber units is unclear may indicate a need for a tiered approach to cyber-related calls for service and a need to clearly define the first responding officer. Finally, there is a need to bring more consistency or standardize the coach officer phase of recruit training.

5.5 Question #5: Updating Recruit Training Curriculum

Participants all identified that an up-to-date curriculum was a top priority, as one participant states, “We are in this perpetual state of [curriculum] tweaking tweaking tweaking”. Several participants provided examples of recent curriculum changes prompted by recent developments in case law, stakeholder feedback, and current events that were relevant to the essential skills and knowledge required of new police officers. However, the emphasis on the need for currency in the curriculum was not found in the literature reviewed.

Both data sources emphasized the pedagogical approaches to recruit training, and agreed that traditional, lecture-based models of police training persist despite attempts to shift to different pedagogical approaches (Timpf, 2014). Concepts such as flipped classrooms, the use of online learning management systems, and the adoption of adult learning principles were discussed in both the literature and by the participants. The importance of simulation-based training and other experiential learning opportunities was expressed by both participants and the literature. These are further discussed in Section 5.6 of this chapter.

The role of the instructor was a prominent theme in both data sources, but particularly so in the interview data. Both data sources contend that instructors are selected based on their experience in the subject matter rather than their teaching abilities, and that the role of the instructor is to “deliver” the content (Timpf, 2014). Participants describe the role of instructional designers as the creators of content and selectors of instructional methods. The literature does not mention instructional designers. This lack of congruence between the participants' views that instructional designers are critical to the instructional process and the absence of this role in the literature suggests that the role of the instructional designer in the curriculum process has not been researched. Any discussion on the need for change in police recruit training curriculum should include the role of, and input from, the instructional designers.

Finally, the data sources were consistent in their finding that the amount of time allotted for recruit training was a key challenge in the proper training of police recruits. Participants cited short training time and high volume of content resulted in the requirement to rely on lecture-based instruction. Participants further identify that the emphasis on covering content – often in a condensed time period – resulted in cognitive overload for recruits. This finding is supported in the literature (Mugford et al., 2013).

These findings indicate that police trainers are invested in ensuring that the recruit training curriculum accurately represents the expectations of the current policing environment. More consistency and currency could be provided by initiating a formalized feedback loop that occurs more often and involves other sources, such as members of the public, coach officers, and members of academies including academics. The velocity of cybercrime development necessitates a faster and more agile curriculum response.

As the debate rages with respect to when digital literacies should be incorporated into the development of an officer, discussions surrounding in-service training curriculum become relevant. Police agencies should consider mandatory online digital literacy courses – similar to the requirement to certify an officer on their use of force or firearms training. Post-secondary institutions could be engaged to offer digital literacy courses to officers who possess varying levels of proficiency.

There is a need for training academies to shift from traditional, lecture-based instructional methods towards more experiential, high fidelity learning activities such as virtual reality simulations and game-based learning. Simulation-based training was the consensus "best option" but was a challenge due to high costs and a lack of fidelity in some simulations. As augmented and virtual reality technologies mature, the associated costs will decrease and both quality and options will increase.

Instructors are currently being chosen largely based on their subject matter expertise, which in the past, allowed them to provide context for the training content through storytelling. Instructors could increase their classroom contributions if they worked collaboratively with instructional designers and were offered courses to develop their teaching skills.

Lastly, the findings indicate that time allotted for training is a significant issue that forces some academies to narrow their scope the most basic, practical skills officers need. There is room for consideration of alternative training options for recruits. These might include taking steps to establish a professional body for police officers that establishes national standards and more consistent training lengths, requiring officers to complete post-secondary programs, or requiring the first five years of an officer's education to fall under the supervision of a recognized training academy.

5.6 Question #6: Impact of Future Technologies on Recruit Training

Every participant discussed emerging technologies and their potential impact on police training and practice. Participants see technologies such as body-worn cameras, data and video analytics, drones, and biometrics as technologies that will re-shape police practice. With respect to the training environment, the use of computer-based simulations using virtual reality was the most oft-mentioned technology (Enea, 2010). Participants also believed that smartphones and mobile apps will play a larger role in recruit training (Rathore et al., 2018). The literature identified many of the same technologies, and included crime mapping and the growth of smart cities as technologies that stand to impact policing. The literature also identified wearable devices – such as activity trackers – and the increased use of digital devices by police officers in the field, however these technologies did not feature prominently in participants' responses.

The reasons for the disconnects between the emerging digital technologies in the literature and those discussed by participants are not clear. It may be a lack of awareness or a lack of recognition of their impact on policing. Participants' exclusion of emerging technologies appears to contradict their stance on the need for curriculum currency. Given the velocity of technological change and development of products, software, and services, no mechanism exists to alert trainers across provinces of these innovation. This poses a paradox for those responsible for recruit curriculum decisions: they cannot incorporate every emerging technology, but have no mechanism for predicting the next mainstream device, tool, software, or system. A "wait and see" approach could result in recruits leaving the academy unaware of technologies they may encounter in the field.

5.7 Limitations of This Study

This study provides answers to each of the research questions but has limitations. This study did not include any document analysis. An analysis of the codified curriculum at each academy might shed further light on connections between digital literacy and training. Not all academies who were invited chose to participate; those that did not participate may have added new findings. The interviews were limited to police academies in Canada. An international research study would provide comparative analysis, as there is a chance that police agencies in other countries may have encountered similar issues and have successfully addressed them through collaborative mechanisms.

There were also challenges with respect to guarding anonymity for participants and their agencies. As a result, some data could not be reported verbatim or with descriptors. Despite assurances of anonymity from the researcher, there is a chance that participants may have felt a loyalty to their academy's current practices and this may have influenced their comments.

Another challenge was that the participant selection process relied on a referral from a supervisor. Some were referred based on their digital skills, which may have impacted the findings, as those possessing digital skills may be more inclined to support technology skills development. Another limitation could be sample size. There was participation from eight out of a possible 14 academies, and one participant per academy was interviewed. It is possible that the opinion of one participant may not reflect the prevailing views of the rest of their academy, however qualitative research is not intended to produce generalizable results, but focuses instead on the lived experiences of the participants. This study endeavored to do just that.

5.8 Recommendations for Further Research

This study contributes to the current body of literature in a number of areas, but opens opportunities for further research to help understand the impact of the digital society on police training. More research needs to examine digital literacy as a core competency for police officers. Such research would help to revise the Canadian Police Sector Council's Competency-Based Management Framework (Police Sector Council, 2013) discussed in Chapter 2. In addition, more research is needed to determine the most appropriate time to teach digital literacy skills in an officer's career. Hopefully more research is emerging on the prevalence of cybercrime calls for service to determine specific numbers of calls, types of calls, and the actions of police first responders attending those calls. This research could identify the core skills and competencies required of officers to preserve digital evidence at the scene in ways that facilitate the admissibility of that evidence.

Regarding recruits, it would be beneficial for research to be conducted into the attitudes of the recruits toward digital literacy, for example, their perceptions of their own levels of digital literacy, that of their instructors, the topics recruits would like to see added or removed from basic recruit training, and which technologies they find most interesting, or least relevant. Future research could involve participants who are coach officers and mentors of basic recruit training graduates. This research could determine which digital skills are most valued by coach officers, which skills should be taught to new recruits, and the level of preparedness of recruits immediately following their completion of recruit training.

5.9 Conclusion

The digital society has impacted police training in several ways. Many police training academies in Canada have incorporated some digital technologies in the classroom. Examples include online learning management systems, computer-based simulators, creating online instructional videos, wearing body-worn cameras, and using PowerPoint presentations. Some academies encourage recruits to use smartphones and tablets in their learning and self-assessment utilizing cloud storage. Most academies involved in this research study reported anecdotally discussing the importance of cybercrime and digital evidence with recruits, with a few academies inviting specialist cyber units to come and speak with the recruits. Despite the significant rise in cybercrime calls for service, the increasing need to identify and preserve digital evidence, the importance of maintaining a clean social media posture, and the value of open-source online tools for basic investigations, none of the participants in this study reported that recruits received dedicated digital skills training as part of basic recruit training.

Technology acceptance and adoption was a prominent theme throughout this study, which supports the use of the UTAUT model to provide context for the data collected. Participants report a discrepancy between how much technology is used in the field versus the technology-related skills taught in recruit training. Findings from this study align with the

UTAUT model through the identification of challenges with *facilitating conditions*, such as cyber-security, bandwidth, equipment, funding, time, and a lack of police-centric training technologies. There is also alignment with UTAUT in terms of *experience*, as instructors, recruits, curriculum designers, and academy administrators bring diverse experience to the training environment. UTAUT suggests that *age* is a modifying factor, which is also supported by the findings as being a moderator of technology acceptance levels.

Training academies appear to fall into several camps regarding when recruits are formally taught digital skills. Some participants reported that digital skills do not need to be formally taught, as these skills are assumed in young recruits. Some believe that digital skills are developed at the mentoring stages after graduating from the recruit training academy. Some participants believe that digital skills need only be taught to officers who elect to join specialized cybercrime units. While participants differed on this topic, the literature strongly suggests the need for digital skills to be introduced at the recruit training stage, and refreshed at regular intervals throughout every officer’s career.

Data from both the participant interviews and the literature review indicate that digital literacy is not a recognized core competency for police officers despite their role to serve and protect a society that is increasingly dependent on digital tools, technologies, options, and systems. Both the literature and the interview data suggest the critical role of recruiting in the development of digital literacy skills. There is a need for recruiters to identify candidates with digital skills and articulate the opportunities in policing. Policing needs to be seen as a destination of choice for cyber-skilled personnel, and must find ways to compete with other agencies and the private sector.

Curriculum currency is a top priority for academies, and the data from this study suggest that, despite the emerging interest in alternative pedagogy, traditional lecture-based instruction represents the dominant teaching style in police recruit training. The reasons for this are a) the high volume of content combined with short training periods make the lecture format the preferred option, b) the need for consistency, accountability, and transparency in recruit training limits opportunities for learner-centered instruction, c) the emphasis on instructors to provide context via experiential narrative and storytelling, and d) slow adoption of digital tools and technologies that could create powerful learning experiences.

In a digital society, technology is constantly changing. As one participant stated, “I know there are more and more technologies being used by society, but I’m not sure which will be used by police.” Police leaders face a perpetual challenge in determining if a new technology should be adopted and used in practice. This valuation process and subsequent strategic implementation results in police being generally behind society when implementing new technologies. Moves toward more digitally-literate police agencies are needed to keep pace with changes in society.

Police recruit training academies are the first stage in a citizen moving from being a civilian to a sworn police officer, and therefore these academies play a crucial role in establishing the baseline skills, competencies, and expectations of frontline police officers. The topic of police recruit training is a complicated issue. This study raises important issues and contributes to the discussion surrounding the need for police officers to be digitally literate, possess baseline digital skills, and understand the many ways that digital technology impacts policing and public safety in the 21st century.

References

Al-Daihani, S. M., & ur Rehman, S. (2007). A study of the information literacy capabilities of the Kuwaiti police officers. *The Electronic Library*, *25*(5), 613-626. doi:10.1108/02640470710829587

Bilodeau, H., Lari, M., & Uhrbach, M. (2019). *Cyber security and cybercrime challenges of Canadian businesses, 2017*. Retrieved from Canadian Centre for Justice Statistics website: https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802-1811. doi:10.1177/1049732316654870

Blandford, S. (2014). *Hired with Competence: An Examination of Police Hiring Standards in Canada*. (Doctoral dissertation). Columbian Southern University, Orange Beach, AL.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management*, *35*(1), 165-181. doi:10.1108/13639511211215504

Bossler, A. M., & Holt, T. J. (2013). Assessing officer perceptions and support for online community policing. *Security Journal*, *26*(4), 349-366. doi:10.1057/sj.2013.23

Brown, C. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55-119. doi: 10.5281/zenodo.22387

Buck, A. (2012). Examining digital literacy practices on social network sites. *Research in the Teaching of English*, *47*(1), 9-38. Retrieved from: https://www.jstor.org/stable/41583603

Calam, M. (2017). *Policing – a vision for 2025*. Retrieved from McKinsey & Company website: https://www.mckinsey.com/industries/public-sector/our-insights/policing-a-vision-for-2025

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report*, *24*(3), 619-628. Retrieved from https://nsuworks.nova.edu/tqr/vol24/iss3/14/

Carter, B. B. (2014). *A Case Study on Law Enforcement Perceptions of the Effects of Education on Policing* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3680630)

Chander, M. (2015). Guidelines and Challenges for Policing a Smart City. *Defence and Security Alert* 6(9), 27-29. Retrieved from: https://www.academia.edu/13258613/Guidelines_and_Challenges_for_Policing_a_Smart_City

Chaouchi, H., & Bourgeau, T. (2018). Internet of things: building the new digital society. *IOT 2018 1*(1), 1-4 doi: 10.3390

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731. doi:10.1016/j.cose.2011.08.004

Cobb, S. (2016). Mind this gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. *Proceedings of the Virus Bulletin Conference*. Denver, CO. Retrieved from: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2018). Police cybercrime training: Perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice, 12*(4) 1-19 doi:10.1093/police/pay078

Cohen, D. & Crabtree, B. (2008). *Qualitative Research Guidelines Project*. Retrieved from Robert Wood Johnson Foundation website: http://www.qualres.org/HomeSemi-3629.html

Conor, P. (2018). *Police resources in Canada, 2017* Canadian Centre for Justice Statistics. Retrieved from Statistics Canada website: https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54912-eng.htm

Cotter, R. S. (2017). Police intelligence: Connecting-the-dots in a network society. *Policing and Society, 27*(2), 173-187. doi:10.1080/10439463.2015.1040794

Council of Canadian Academies (2014). *Policing Canada in the 21st century: new policing for new challenges*. Ottawa (ON): The Expert Panel on the Future of Canadian Policing Models, Council of Canadian Academies.

Craiger, J. P., Pollitt, M., & Swauger, J. (2005). Law enforcement and digital evidence. In H. Bidgoli (Ed), *Handbook of information security 2nd edition* (pp. 739-777). Hoboken, NJ: Wiley

Creswell, J. W. (2014). *Research Design* (4th ed.). Thousand Oaks, CA: Sage Publications.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice, 39*(3), 124-130. doi:10.1207/s15430421tip3903_2

Crouch, M., & McKenzie, H. (2006). The logic of small samples in interview-based qualitative research. *Social Science Information, 45*(4), 483-499. doi:10.1177/0539018406069584

Cunha, I. K., Patel, A., Moura dos Santos, A., & Celestino, J. (2016). A proposal of educating Brazilian police officers for cybercrime investigation & prosecution. Presented at the 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC). 6-8 July 2016, Moscow. doi:10.1109/DIPDMWC.2016.7529386

Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs. *Computer law & security review, 28*(1), 62-68. doi: https://doi.org/10.1016/j.clsr.2011.11.009

Damodaran, L., & Burrows, H. (2017). *Digital skills across the lifetime: Existing provisions and future challenges*. Future of skills and lifelong learning project. UK: Government Office for Science. Retrieved from: https://dera.ioe.ac.uk//29774/

Davies, R. S. (2011). Understanding technology literacy: A framework for evaluating educational technology integration. *Techtrends, 55*(5), 45-52. doi:10.1007/s11528-011-0527-3

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. doi:10.2307/249008

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in Psychology 9*(744). doi:10.3389/fpsyg.2018.00744

Del Balso, M., & Lewis, A. D. (2012). *First steps: A guide to social research,* (5th ed.). Toronto: Nelson.

Demircioglu, M. (2010). *Information-seeking behavior of crime scene investigators in the Turkish national police (*Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3417745)

Deverge, C. A. (2016). *Police education and training: A comparative analysis of law enforcement preparation in the United States and Canada* (Master's Thesis). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 10241713)

Domo.com. (2019). Data Never Sleeps 7.0. Retrieved from: https://www.domo.com/learn/data-never-sleeps-7

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education, 40*(4), 314-321. doi: 10.1111/j.1365-2929.2006.02418.x

Enea, P. (2010). Field training for the 21st century: Workforce models for today and tomorrow. *Journal of California Law Enforcement*, *44*(3), 12-17. Retrieved from: http://search.proquest.com.uproxy.library.dc-uoit.ca/docview/818558326?accountid=14694

Etter, G.W., & Griffin, R (2011). In-service training of older law enforcement officers: An andragogical argument, *Policing: An International Journal of Police Strategies & Management, 34*(2), 233–245. doi: http://dx.doi.org.uproxy.library.dc-uoit.ca/10.1108/13639511111148861

Evans, K., and Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. Center for Strategic & International Studies. Retrieved from: https://www.csis.org/analysis/human-capital-crisis-cybersecurity

Faith, T and Bekir, C. (2015). Police use of technology to fight against crime. *European Scientific Journal*, *11*(10), 286-296. Retrieved from: https://www.eujournal.org/index.php/esj/article/view/5426

Flory, T. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law*, *11*(1), 7. doi:10.15394/jdfsl.2016.1374

Francescani, C. (2016). Ransomware Hackers Blackmail U.S. Police Departments. *CNBC News*. Retrieved from: https://www.cnbc.com/2016/04/26/ransomware-hackers-blackmail-us-police-departments.html

Garcia, N. (2018). *The use of criminal profiling in cybercrime investigations* (Master's Thesis). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 10839020)

Giovengo, R. (2017). *Training law enforcement officers*. Boca Raton, FL: CRC Press.

Glaser, B. G. & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. London, UK: Wiedenfeld and Nicholson.

Gilster, P. (1997). *Digital literacy*. New York: Wiley

Gogolin, G. (2010). The digital crime tsunami. *Digital Investigation, 7*(1), 3-8. doi:10.1016/j.diin.2010.07.001

Public Safety Canada. (2018). *National cyber security strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Ottawa, ON: Her Majesty the Queen in Right of Canada, 2018

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence. *Priority Criminal Justice Needs Initiative.* Santa Monica, CA: Rand Corporation.

Goodman, M. (2015). *Future crimes: Inside the digital underground and the battle for our connected world*. New York, NY: Random House.

Grabosky, P., & Smith, R. (2017). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. New York, NY: Routledge.

Gresham, J. (2016). *Rise of the millennial officer: Multigenerational learning and field training programs* [White paper]. Retrieved from Sam Houston State University website: https://shsu-ir.tdl.org/bitstream/handle/20.500.11875/2068/1656.pdf?sequence=1

Guclu, I. (2018). Understanding information-seeking behavior for conducting tasks: An exploratory study. *International Information & Library Review, 50*(4), 265-275. doi:10.1080/10572317.2017.1399776

Guclu, I., & Can, A. (2015). The effect of socio-demographic characteristics on the information-seeking behaviors of police officers. *Policing: An International Journal of Police Strategies & Management, 38*(2), 350-365. doi:10.1108/PIJPSM-12-2014-0132

Hanna, N. K. (2016). Introduction and overview. In E.G. Carayannis (Ed.). *Mastering digital transformation: Towards a smarter society, economy, city and nation* (pp. 3-14). Bingley, UK: Emerald Publishing Limited. doi: https://doi-org.uproxy.library.dc-uoit.ca/10.1108/978-1-78560-465-220151010

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519-536. doi:10.1080/15614263.2018.1507889

Hartman, S. (2017). Exploring careers in information security. *Career Planning and Adult Development Journal, 33*(1), 12-16. Retrieved from: http://search.proquest.com.uproxy.library.dcuoit.ca/docview/2018636538?accountid=14694

Heal, C. S., Cowper, T., & Olligschlaeger, A. (2006). Law enforcement technology 2015. *Futures Working Group 2*(1) 29-38. Retrieved from US Department of Justice website: https://sciences.ucf.edu/fwg/wp-content/uploads/sites/157/2016/11/FWG-Homeland_Security_2015.pdf

Herrod, C. (2018). *Exploring the educational needs of the information security community: A qualitative* *delphi study* (Doctoral Dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 10930321)

Hilal, S., Densley, J., & Zhao, R. (2013). Cops in College: Police Officers' Perceptions on Formal Education. *Journal of Criminal Justice Education, 24*(4), 461-477. doi: https://doi.org/10.1080/10511253.2013.791332

Hitchcock, B., Le-Khac, N., & Scanlon, M. (2016). Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *Digital Investigation, 16*(1), S75-S85. doi:10.1016/j.diin.2016.01.010

Hitchcock, A., Holmes, R., & Sundorph, E. (2017). *Bobbies on the net: a police workforce for the digital age*. London, UK: Reform. Retrieved from: https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/non-secure/b/o/b/bobbies-on-the-net-police-workforce-for-the-digital-age-17.pdf

Her Majesty's Inspectorate of Constabulary (HMIC). (2015). *Real lives, real crimes: A study of digital crime and policing*, London, UK: HMIC. Retrieved from: https://www.justiceinspectorates.gov.uk /hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Her Majesty's Inspectorate of Constabulary (HMIC). (2016). *PEEL: Police efficiency 2016*, London, UK: HMIC. Retrieved from: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-efficiency-2016.pdf

Hirsch, J. (2016). Predictive Policing and Civilian Oversight: What Will It Take to Get It Right? *IEEE Potentials 35*(5), 19-22. doi: 10.1109/MPOT.2016.2569723

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy, 10*(2), 33-39. doi:10.1109/MSP.2011.181

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The Annals of the American Academy of Political and Social Science, 679*(1), 140-157. doi:10.1177/0002716218783679

Holt, T. J., & Bossler, A. M. (2012a). Police perceptions of computer crimes in two Southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice*, *37*, 396-412. doi: 10.1007/s12103-011-9131-5

Holt, T. J., & Bossler, A. M. (2012b). Predictors of patrol officer interest in cybercrime training and investigation in selected united states police departments. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 464-472. doi:10.1089/cyber.2011.0625

Hollywood, J. S., Boon, J., Silberglitt, R., Chow, B & Jackson, B. (2015). *High-priority information technology needs for law enforcement*, Santa Monica, CA: Rand Corporation.

Hollywood, J. S., Vermeer, M. J., Woods, D., Goodison, S. E., & Jackson, B. A. (2018). *Using Social Media and Social Network Analysis in Law Enforcement*. Santa Monica, CA: Rand Corporation.

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science & Justice, 57*(6), 448-

454. doi: https://doi.org/10.1016/j.scijus.2017.06.001

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61-67. doi: 10.1016/j.clsr.2010.11.001

Interprovincial Policing Act. (2009). *Interprovincial Policing Act, 2009, S.O. 2009, c. 30* Retrieved from: https://www.ontario.ca/laws/statute/09i30

James, J. I., & Gladyshev, P. (2015). Automated inference of past action instances in digital investigations. *International Journal of Information Security, 14*(3), 249-261. doi:10.1007/s10207-014-0249-6

Jewell, L., (2013). *Models and structures of corrections and police training and research activities in Canadian and international jurisdictions*. Retrieved from Public Safety Canada website: https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn32144-eng.pdf

Joh, E. E. (2014). Policing by numbers: Big data and the fourth amendment. *Washington Law Review, 89*(1), 35+. Retrieved from: https://link.gale.com/apps/doc/A366728345/AONE?u=ko_acd_uoo&sid=AONE&xid=f1422c35

Kaiser, K. (2009). Protecting Respondent Confidentiality in Qualitative Research. *Qualitative Health Research, 19*(11), 1632-1641. doi: 10.1177/1049732309350879

Kemp, S. (2019, January 30). Digital 2019: Global internet use accelerates. Retrieved from: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

Kilic, O. (2010). *Information literacy skills in the workplace: a study of police officers* (Doctoral dissertation), Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3448588)

King Stargel, T. M. (2010). *The perceived value of problem-based learning at a police training academy* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3407279)

Knowles, M. S., Holton III, E. F. and Swanson, R. A. (2005). *The Adult Learner* (6th ed.). Burlington, MA: Elsevier.

Koksal, T. (2009). *The effect of police organization on computer crime* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3368227)

Koper, C. S., Lum, C., & Willis, J. J. (2014). Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and behavioural aspects of implementing police technologies. *Policing, 8*(2), 212-221. doi:10.1093/police/pau015

Koper, C. S., Taylor, B. G. and Kubu, B. E. (2009). *Law enforcement technology needs assessment: Future technologies to address the operational needs of law enforcement.* Washington, DC: Police Executive Research Forum.

Law, N. W. Y., Woo, D. J., de la Torre, J., & Wong, K. W. G. (2018). A global framework of reference on digital literacy skills for indicator 4.4. 2. Retrieved from the UNESCO Institute for Statistics website: http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

Lettic, S. (2015). *Problem based learning (PBL) in police training: An evaluation of the recruit experience* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3735149)

Lichtman, M. (2012). *Qualitative Research in Education: A User's Guide* (3rd ed). Thousand Oaks, CA: Sage Publications

Lin, C., Hu, P. J., & Chen, H. (2004). Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. *Social Science Computer Review, 22*(1), 24-36. doi:10.1177/0894439303259881

Lindsay, R., Jackson, T. W., & Cooke, L. (2014). Empirical evaluation of a technology acceptance model for mobile policing. *Police Practice and Research, 15*(5), 419-436. doi:10.1080/15614263.2013.829602

Lindsay, R., Jackson, T. W., & Cooke, L. (2011). Adapted technology acceptance model for mobile policing. *Journal of Systems and Information Technology*, *13*(4), 389-407. doi:10.1108/13287261111183988

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly, 20*(2), 135. doi:10.1177/1098611116667279

MacNeil, T. L. (2015). *Police opinions of digital evidence response handling in the state of Georgia: An examination from the viewpoint of local agencies' patrol officers* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3742823)

Marquis, G. (1994). Power from the street: The Canadian municipal police. In R. C. MacLeod & D. Schneiderman (Eds). *Police Powers in Canada: The Evolution and Practice of Authority*. Toronto: University of Toronto Press. doi:10.3138/9781442678583-005

McCoy, M. R. (2006). Cops, computers and the curriculum. *International Journal of Police Science & Management, 8*(2), 153-158. doi:10.1350/ijps.2006.8.2.153

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research: A Guide to Design and Interpretation* (4th ed.). San Francisco, CA: Jossey-Bass.

Ministry of Justice. (2012). *Swift and sure justice: The Government's plans for reform of the criminal justice system*. Retrieved from The Stationery Office Limited website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/217328/swift-and-sure-justice.pdf

Monett, D. and Elkina, M. (2015). E-Learning Adoption in a Higher Education Setting: An Empirical Study. In *Proceedings of the Multidisciplinary Academic Conference, Prague*. doi:

10.13140/RG.2.1.2492.2963

Montgomery, C. (2017). *New security for a new era: An investigation into law enforcement cybersecurity threats, obstacles, and community applications* (Master's Thesis). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 10687217)

Mugford, R., Corey, S., & Bennell, C. (2013). Improving police training from a cognitive load perspective. *Policing: An International Journal of Police Strategies & Management*, *36*(2), 312-337. doi:10.1108/13639511311329723

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2016) National initiative for cybersecurity education (NICE) cybersecurity workforce framework. Retrieved from US Department of Commerce website: https://www.schoolofcybersecurity.com/wp-content/uploads/2018/04/NIST.SP_.800-181.pdf

NIJ (2008). *Electronic crime scene investigation: A guide for first responders, second edition*. Retrieved from the Federal Bureau of Investigation website: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Nuth, M. S. (2008). Taking advantage of new technologies: For and against crime. *Computer Law and Security Review: The International Journal of Technology and Practice, 24*(5), 437-446. doi:10.1016/j.clsr.2008.07.003

Olawoyin, O. R., Esse, U. C., & Madukoma, E. (2017). Information Use and Quality Service of The Nigerian Police. *Library Philosophy and Practice.* Retrieved from: https://digitalcommons.unl.edu/libphilprac/1540

Osterman, M. D. (2012). Digital literacy: Definition, theoretical framework, and competencies. In M. S. Plakhotnik, S. M. Nielsen, & D. M. Pane (Eds.), *Proceedings of the 11th Annual College of Education & GSN Research Conference* (pp. 135-141). Miami, FL. Retrieved from: https://core.ac.uk/download/pdf/46946450.pdf

Paoline, E. A., Terrill, W., & Rossler, M. T. (2015). Higher education, college degree major, and police occupational attitudes. *Journal of Criminal Justice Education*, *26*, 49–73. doi: https://doi.org/10.1080/10511253.2014.923010

Paterson, C. (2011). Adding value? A review of the international literature on the role of higher education in police training and education. *Police Practice and Research, 12*(4), 286–297. http://dx.doi.org/10.1080/15614263.2011.563969

Police Sector Council (2013). *A Guide to Competency-Based Management in Police Services*. Retrieved from the Police Sector Council website: http://www.policecouncil.ca/wp-content/uploads/2013/03/Competency-Based-Management-Guide.pdf

Prensky, M. (2001). Digital natives, Digital Immigrants Part 1. *On the Horizon, 9*(5), 1-6. doi:10.1108/10748120110424816

Quinn, C. (December 12 2018). The emerging cyberthreat: Cybersecurity for law enforcement," *Police Chief online*. Retrieved from: https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/

Ramshaw, P., & Soppitt, S. (2018). Educating the recruited and recruiting the educated: Can the new police education qualifications framework in England and Wales succeed where others have faltered? *International Journal of Police Science & Management, 20*(4), 243-250. doi:10.1177/1461355718814850

Rao, S., & Perry, C. (2006). Convergent interviewing to build a theory in under-researched areas: Principles and an example investigation of internet usage in inter-firm relationships. *Qualitative Market Research: An International Journal, 6*(4), 236-247. doi:10.1108/13522750310495328

Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge.

Rathore, M. M., Paul, A., Hong, W., Seo, H., Awan, I., & Saeed, S. (2018). Exploiting IoT and big data analytics: Defining smart digital city using real-time urban data. *Sustainable Cities and Society, 40,* 600-610. doi:10.1016/j.scs.2017.12.022

Reedy, K., & Goodfellow, R. (2012). *Digital and information literacy framework*. Retrieved from The Open University website: http://www.open.ac.uk/libraryservices/subsites/dilframework/dilframework_view_by_skill.pdf

Roberts, K., Herrington, V., Jones, W., White, J., & Day, D. (2016). Police leadership in 2045: The value of education in developing leadership. *Policing: A Journal of Policy and Practice, 10*(1). doi:10.1093/police/pav045

Roberson, M. T., & Sundstrom, E. (1990). Questionnaire design, return rates, and response favorableness in an employee attitude questionnaire. *Journal of Applied Psychology*, *75*(3), 354-357. doi: 10.1037/0021-9010.75.3.354

Rossler, M. T. (2019). The impact of police technology adoption on social control, police accountability, and police legitimacy. In C. E. Rabe-Hemp & N. S. Lind (Eds). *Political Authority, Social Control and Public Policy* (pp. 209-224) Emerald Publishing Limited. doi:10.1108/S2053-769720190000031014

Rowe, M. (2018). *Introduction to policing* (3rd ed.). Washington, DC: Sage.

Rui-Hsin, K., & Lin, C. (2018). The usage intention of e-learning for police education and training. *Policing: An International Journal, 41*(1), 98-112. doi:10.1108/PIJPSM-10-2016-0157

Russel., A. (2019 June 10). ‘It’s a travesty’: Nearly 800 criminal cases thrown out over delays since 2016 Jordan decision. *Global News*. Retrieved from: https://globalnews.ca/news/5351012/criminal-cases-thrown-out-r-v-jordan-decision/

Rydberg, J., & Terrill, W. (2010). The effect of higher education on police behavior. *Police Quarterly*, *13*(1), 92–120. doi: 10.1177/1098611109357325

Sanders, C. B., & Hannem, S. (2012). Policing "the risky": Technology and surveillance in everyday patrol work. *Canadian Review of Sociology*, *49*(4), 389. doi: https://doi.org/10.1111/j.1755-618X.2012.01300.x

Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research, 10*(1), 3-26. doi:10.1023/B:CRIM.0000037562.42520.d7

Scanlan, D. (2011). *Digital evidence in criminal law*. Canada Law Book.

Schäfer, J. A., & Boyd, S. (2007). The future of education and training for police. In J. A. Schäfer (Ed.), *Policing 2020: Exploring the future of crime, communities, and policing* (pp. 372-413). Quantico, VA:U.S. Department of Justice, Federal Bureau of Investigation.

Schafer, M. and van Es, K. (Eds) (2017). The Datafied Society: Studying Culture Through Data. Amsterdam, NL: Amsterdam University Press.

Schreuders, Z. C., Cockcroft, T. W., Butterfield, E. M., Elliott, J. R., & Soobhany, A. R. (2018). Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. Retrieved from The Cybercrime and Security innovation Centre website: http://eprints.leedsbeckett.ac.uk/5076/1/Needs%20Assessment%20of%20Cybercrime%20and%20Digital%20Evidence%20in%20a%20UK%20Police%20Force.pdf

Seawright, Leslie 2012. *The Literacy Practices of Law Enforcement* (Doctoral dissertation). University of Arkansas, Fayetteville, AR. Retrieved from: http://scholarworks.uark.edu/etd/295

Sharma, R., Fantin, A., Prabhu, N., Guan, C., & Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. *Telecommunications Policy, 40*(7), 628-643. doi:10.1016/j.telpol.2016.05.003

Silberglitt, R., Chow, B. G., Hollywood, J. S., Woods, D., Zaydman, M., & Jackson, B. A. (2015). *Visions of Law Enforcement Technology in the Period 2024-2034*. Santa Monica, CA: Rand Corporation

Spante, M., Hashemi, S. S., Lundin, M., & Algers, A. (2018). Digital competence and digital literacy in higher education research: Systematic review of concept use. *Cogent Education, 5*(1). doi:10.1080/2331186X.2018.1519143

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime – realities and challenges. *Journal of Accounting and Management Information Systems, 16*(4), 610-632. doi:10.24818/jamis.2017.04009

Stanislas, P. (2014). The Challenges and Dilemmas Facing University-based Police Education in Britain. In P. Stanislas (ed.) *International Perspectives on Police Education and Training* (pp.57-71). London, UK: Routledge

Stensland, W. S. (2018). *Police Administrators Should Begin Preparing Their Departments for the Millennials* [White Paper]. Retrieved from The Bill Blackwood Law Enforcement Management Institute of Texas website: https://shsu-ir.tdl.org/bitstream/handle/20.500.11875/2490/1802.pdf

Stephens, G. F. (2015). *Learning styles of millennial law enforcement officers* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT

3703456)

Steyn, R. A. (2018). Changing thoughts towards digital literacy interventions for south African entrepreneurs. *Reading & Writing, 9*(1), e1-e9. doi:10.4102/rw.v9i1.172

Stokes, T. R. (2010). Gone the Renaissance Cop: Will Specialized Police Officers be the Staffing Models of the Future? *Journal of California Law Enforcement 44*(4), 12-17. Retrieved from: http://lib.post.ca.gov/lib-documents/CC/47-Stokes.pdf

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy, 6*(2), 17-33. doi:10.5204/ijcjsd.v6i2.355

Straus, S. G., Bikson, T. K., Balkovich, E., & Pane, J. F. (2010). Mobile technology and action teams: Assessing BlackBerry use in law enforcement units. *Computer Supported Cooperative Work (CSCW), 19*(1), 45-71. doi:10.1007/s10606-009-9102-2

Strauss, A., & Corbin, J. (1994). Grounded Theory Methodology. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 273-285). Thousand Oaks, CA: Sage Publications

Strom, Kevin J. (2017). *Research on the Impact of Technology on Policing Strategy in the 21st Century: Final Report*. Retrieved from Office of Justice Programs website: https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf

Sturgeon, N. A. (2015). *Web based cyber forensics training for law enforcement* (Master's Thesis). Available from ProQuest LLC. (No. 10062241)

Sturges, J. E., & Hanrahan, K. J. (2004). Comparing telephone and face-to-face qualitative interviewing: A research note. *Qualitative Research, 4*(1), 107-118. doi:10.1177/1468794104041110

Suby, M., & Dickson, F. (2015). *The 2015 (ISC)² Global Information Security Workforce Study* [White paper]. Retrieved from: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2015.ashx?la=en&hash=01D5BD45477FB7B45EF773366CF7D1D9BB6A6753

Tanner, S., & Meyer, M. (2015). Police work and new 'security devices': A tale from the beat. *Security Dialogue, 46*(4), 384-400. doi:10.1177/0967010615584256

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. New Jersey: Prentice Hall Press.

techUK. (2016 December). Digital Policing: The Future of Modern Crime Prevention. Retrieved from techUK website: https://www.techuk.org/component/techuksecurity/security/download/9856?file=Future_of_Modern_Crime_Prevention_FINAL.pdf

The world's most valuable resource is no longer oil, but data. (2017, May 06). *The Economist*. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Timpf, J. L. (2014). *Training police officers to meet the demands of public expectations* [White paper].

Retrieved from Sam Houston State University website: https://shsu-ir.tdl.org/handle/20.500.11875/1924

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. *Qualitative inquiry*, *16*(10), 837-851. doi: 10.1177/1077800410383121

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, *18*(4-5), 530-547. doi:10.1177/1367549415577396

UK House of Commons. (2018). *Policing for the future: Tenth Report of Session 2017–19*. Retrieved from the House of Commons website: https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/515.pdf

VanDerwerken, J., & Ubell, R. (2011). Training on the cyber-security frontlines: Organizations need more well-trained experts to defend against cyber threats. *T+D, 65*(6), 46-50. Retrieved from: https://link.gale.com/apps/doc/A344209939/AONE?u=ko_acd_uoo&sid=AONE&xid=117d4c0f

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273-315. doi:10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478. doi:10.2307/30036540

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice*, *7*(4), 391-415. doi:10.1177/1748895807082064

Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: Networked and social media technologies and the challenges for policing. *Policing and Society, 23*(4), 409-412. doi: 10.1080/10439463.2013.780222

Wall, D., May-Chahal, C., & Chistyakova, Y. (2015). *Policing Cybercrime: Evidence Review*. Retrieved from N8 Research Partnership website: http://library.college.police.uk/docs/N8/policing-cybercrime-evidence-review.pdf

Werth, E. P., & Werth, L. (2011). Effective training for millennial students. *Adult Learning, 22*(3), 12-19. doi:10.1177/104515951102200302

Weston, C., Bennett-Moses, L., & Sanders, C. (2019). The changing role of the law enforcement analyst: Clarifying core competencies for analysts and supervisors through empirical research. *Policing and Society*, , 1-16. doi:10.1080/10439463.2018.1564751

Wexler, C. (2012). *How are innovations in technology transforming policing*. Retrieved from Police Executive Research Forum website: https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf

White, A. (2014). Post-crisis policing and Public–Private partnerships: The case of Lincolnshire police and G4S. *British Journal of Criminology, 54*(6), 1002-1022. doi:10.1093/bjc/azu063

White, M. D., & Escobar, G. (2008). Making good cops in the twenty-first century: Emerging issues for the effective recruitment, selection and training of police in the United States and abroad. *International Review of Law, Computers & Technology, 22*(1-2), 119-134. doi:10.1080/13600860801925045

Williams, S., & Aasheim, C. (2005). Information technology in the practice of law enforcement. *Journal of Cases on Information Technology (JCIT), 7*(1), 71-91. doi:10.4018/jcit.2005010105

Willis, R. C. (2010) Improving training through bloom's taxonomy: Why police instructors should avoid a cookie-cutter approach to training new officers. Retrieved from: https://www.policeone.com/police-trainers/articles/improving-training-through-blooms-taxonomy-NCE1dBiYkw7td6ku/

Wolf, J. W. (2013). *The training curriculum at Pennsylvania municipal police academies: Perceptions of effective training* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global database. (Accession Order No. AAT 3604327)

Worldpopulationreview.com (July 2019). Canada Population 2019. Retrieved from: http://worldpopulationreview.com/countries/canada-population/

Wyatt, S. & Bell, N. (2014). Perspectives on police training and education: The Canadian experience. In P. Stanislas (ed.) *International Perspectives on Police Education and Training* (pp.72-89). London, UK: Routledge

Wydra, C., & Hartle III, F. (2015). Educating the Technology Officer of the Future: A Needs Analysis. *Issues in Information Systems*, *16*(4).

Xiong, J. (2016). Information ability evaluation based on AHP for students in police college. Proceedings of the *2016 International Seminar on Education Innovation and Economic Management (SEIEM 2016)*. Chongqing, China: Atlantis Press. doi: https://doi.org/10.2991/seiem-16.2016.84

Yalcinkaya, R. (2007). *Police officers' adoption of information technology: A case study of the Turkish POLNET system* (Doctoral dissertation). Available from University of North Texas Electronic Theses and Dissertations. (OCLC No : 192074523).

Appendix A

Police Training Academies in Canada

Atlantic Police Academy – Holland College
66 Argus Dr, Slemon Park, PE C0B 2A0.
http://www.hollandcollege.com/atlantic-police-academy/

École Nationale de Police du Québec (ENPQ)
350 Rue Marguerite d'Youville, Nicolet, QC J3T 1X4
http://www.enpq.qc.ca/en/nc.html

Ontario Police College
10716 Hacienda Rd, Aylmer, ON N5H 2R3
http://www.mcscs.jus.gov.on.ca/english/police_serv/OPC/OPC_about.html

Toronto Police College
70 Birmingham St, Toronto, ON M8V 2Z5
http://www.torontopolice.on.ca/college/.

OPP Training Facility - Huronia Regional Centre
700 Memorial Ave, Orillia, ON L3V 6H1
https://www.opp.ca/index.php?id=128

Winnipeg Police Training Academy
200 - 1821 Wellington Ave, Winnipeg, MB R3H 0G4
https://www.winnipeg.ca/police/policerecruiting/officer/training.aspx

Brandon Police Service
1020 Victoria Ave, Brandon, MB R7A 1A9
http://police.brandon.ca/new-officer/new-recruits

RCMP Academy, Depot Division
11th Ave, Regina, SK
http://www.rcmp-grc.gc.ca/depot/index-eng.htm

Saskatchewan Police College
3737 Wascana Pkwy, Regina, SK S4S 0A2
http://www.saskpolicecollege.ca/

Edmonton Police Service Training Centre
10177 97 St NW, Edmonton, AB T5J 0L4
http://www.joineps.ca/Training/NewOutofProvinceApplicants

Calgary Police Service
5111 47 St. N.E., Calgary, AB, T3J 3R2
http://www.calgary.ca/cps/Pages/home.aspx

Peel Regional Police
180 Derry Rd E, Mississauga, ON L5T 2Y5
https://www.peelpolice.ca/en/index.aspx

British Columbia - Justice Institute of BC
715 McBride Blvd, New Westminster, BC V3L 5T4
http://www.jibc.ca/programs-courses/schools-departments/school-criminal-justice-security/police-academy

Lethbridge College
3000 College Dr S, Lethbridge, AB T1K 1L6
https://lethbridgecollege.ca/

Appendix B

Consent Form

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

RESEARCH ETHICS BOARD
OFFICE OF RESEARCH SERVICES

Title of Research Study:

Examining the Impact of the Digital Society on Police Training in Canada

You are invited to participate in a research study entitled "Examining the Impact of an Increasingly Digital Society on Police Training in Canada". This study has been reviewed by the University of Ontario Institute of Technology Research Ethics Board #4386 and originally approved on [insert date].

Please read this consent form carefully, and feel free to ask the Researcher any questions that you might have about the study. If you have any questions about your rights as a participant in this study, please contact the Research Ethics Coordinator at 905 721 8668 ext. 3693 or researchethics@uoit.ca.

Researcher: James Robertson, Graduate Student, Faculty of Education, james.robertson4@uoit.net
Principal Investigator: Dr. Bill Muirhead, Faculty of Education, bill.muirhead@uoit.ca

Purpose and Procedure:
The purpose of this study is to investigate the intersection of digital technologies and police practices, specifically the ways in which police academies in Canada prepare officers to serve and protect in an increasingly digital environment. The study focuses on police training institutions, and uses a combination of document analysis and qualitative interviews as a means of collecting data. As an interviewee, you will be asked to spend about 60 minutes of your time to meet with the researcher online (using Skype or similar online meeting tool). You will be asked to answer questions about police training curriculum at your institution.

Potential Benefits:
As a participant in this study, you will be contributing to the current body of knowledge on police training. You may also help bring to light opportunities for new courses or training methods. In short, you will help ensure that the men and women charged with policing in Canada are entering this exciting career armed with knowledge and skills that are directly related to their responsibilities as police officers.

Potential Risks:
Participants in this study will be asked to offer up 40 minutes of their time to participate in an online interview. Participants will be afforded the opportunity to review the transcription of their interview, which also involves a small commitment of time on the part of the participant. Participants will be asked about their workplace – potentially a topic where a negative opinion could be expressed. However, participants have the option to decline to answer any question. Participants may review the transcript and revise their responses prior to analysis by the researcher so the participant has control over what information is recorded from the interview.

Storage of Data:
All files related to this study will be encrypted and password protected on the USB drives. Emailed files

will be compressed using standard compression tools that are also password protected; this ensures data cannot be reconstructed if stolen while in transit. The data collected for this study will be destroyed within 2 years of collection.

Confidentiality:
Participants will not be asked personal questions, such as age, gender, or rank/role within their organization. This is to protect the identity of the participant but also because that information is not relevant to the study.

Only members of the research team will know the names of the participants. Names are not included in the transcription files, where participants are identified merely as “participant”. In the data analysis, participants are assigned a random number/letter combination, with only the members of the research team having knowledge of each participant’s alias.

Participant privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data are in transit over the Internet.

Right to Withdraw:
Your participation is voluntary, and you can answer only those questions that you choose. The information that is shared will be held in strict confidence. Participants may withdraw at any time up to two weeks after their interview, and you will not be persuaded to change your decision to withdraw. You need not offer any reason for making this request. No participants will be told if another participant withdraws from the study. If you withdraw, you will receive written confirmation that all data relating to your participation in the study have been destroyed.

Conflict of Interest:
There are no real, potential or perceived conflicts of interest concerning this study.

Compensation:
There is no compensation of any form offered to participants in this study.

Dissemination of Results:
This study will be online as an MA Thesis in 2019 and will be searchable using the name of the researcher or the title of the thesis.

Participant Concerns and Reporting:
If you have any questions concerning the research study, contact the researcher, James Robertson, at james.robertson4@uoit.net. Any questions regarding your rights as a participant, complaints or adverse events may be addressed to Research Ethics Board through the Research Ethics Coordinator – researchethics@uoit.ca or 905.721.8668 x. 3693.

By consenting, you do not waive any rights to legal recourse in the event of research-related harm.

Consent to Participate:

1. I have read the consent form and understand the study being described;
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future;

3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty. A copy of this Consent Form has been made available to me.

________________________________ ______________________________

(Name of Participant) (Date)

________________________________ ______________________________

(Signature of Participant) (Signature of Researcher)

Oral Consent: (if written consent is difficult to obtain)

1. I have read the consent form to the participant they have indicated that he/she understands the study being described.
2. The participant has had an opportunity to ask questions and these questions have been answered. The participant is free to ask questions about the study in the future.
3. The participant freely consents to participate in the research study, understanding that he/she may discontinue participation at any time without penalty. A physical/digital Consent Form has been made available to him/her.

________________________________ ______________________________

(Name or identifier of Participant) (Date)

____

(Signature of Researcher)

Online Consent: (if written consent is difficult to obtain)

1. I have read the consent form and understand the study being described.
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future.
3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty. A copy of this Consent Form has been made available to me.

□ I Agree

Appendix C

Interview Script

Interview Script:

"Thank you for volunteering to participate in this research study. This interview will last for up to 60 minutes and will be audio recorded. You have read the consent form sent prior to this interview, and before we begin I want to ask you if you have any questions about the consent form, this interview process, or the research process for this study. Do you have any questions?"

(Answer all questions)

"I want to begin by assuring you that the information you provide will be kept strictly confidential and that this interview is anonymous. Your name will not be included in any written submissions – or in the transcript of this interview. I will not ask personal questions. Any responses you provide will be screened for content that could potentially be used to identify you and that content anonymized. You have the right to decline to answer a question without explanation and you can withdraw from the study at any point without challenge or penalty up until 2 weeks after you receive a transcript of the interview. When you receive this transcript, you are free to edit your responses in any way you see fit. Do you have any questions?"

(Answer all questions)

"Thank you. Have you had a chance to read the questions beforehand?

This is a semi-structured interview - not an interrogation. I am not looking for specific answers - rather, I want to hear your thoughts, opinions, experiences, and ideas. There are no right or wrong answers. The questions are open-ended and are intended to guide the discussion.

The purpose of these questions is to collect data from the people who are directly responsible for police training in Canada. Your answers will be analyzed alongside the answers of other participants to identify common themes, trends or phenomena that will help me answer my research question, which is "What is the impact of the digital society on police training in Canada?"

Lastly, as a way of showing respect for your time, I will do my best to keep this discussion to no more than 60 minutes."

1. You must be uniquely qualified or had certain types of experience to become an instructor in a policing program. Tell me a bit about your background and experience.
2. How is the curriculum at your institution determined? How often does it change?
3. During your time with your academy, which changes, if any, have you noticed about the way digital technology is incorporated into recruit training?
4. How do you define digital literacy, and how would you characterize your own level of digital literacy?
5. How would you describe the level of digital literacy of the instructors at your academy?
6. How would you describe the digital literacy levels of the recruits entering basic training?

6. Do you think police recruits need to be taught digital literacy in basic training?
7. How receptive are the recruits to learning with or about digital technologies? Do you think this has changed over time?
8. Do the recruits ask about getting trained on new technologies? (some examples might be cybercrime training, digital evidence, social media use, smart phones)
9. If you were given the authority to add more instruction on the use of digital technologies, what changes, if any, would you make and why?
10. How do you see the way we train police officers changing in the next 5-10 years?
    a. Do you foresee any emerging technologies impacting future recruit training curriculum?

“Those are all my questions. Thank you so much for your time! Is there anything else you would like to add before i stop the recording?

I will email you the written transcript of this interview within one week. The file will be a Microsoft Word document that is encrypted and password protected. The password will be____.

Upon receipt you are free to modify the transcript as you see fit. After two weeks, if I have not heard back from you, I will enter the data from this interview into the data base. At that time, after the data are merged, I may not be able to withdraw your specific comments from the data set if you choose to withdraw.

Thank you very much for your time.”

(End interview)

Appendix D

Alignment of Interview Data with Research Questions

Research Questions	Interview Questions	Findings Subheadings
Context	1. Tell me a bit about your background and experience	4.0 Overview and Context
1. In what ways do current police training academies in Canada recognize the digital society?	2. How is the curriculum at your institution determined? How often does it change? 3. Which changes, if any, have you noticed about the way digital technology is incorporated into recruit training?	4.1.Curriculum and Content 4.1.1 Need to Maintain Currency of Curriculum 4.1.2 Sources of Curriculum Change 4.1.3 Recruits' Level of Cyber hygiene
3. What is the role of digital literacy in police training and practice?	5. How would you describe the digital literacy levels of recruits at your academy? 7. In your view, which digital skills do recruits acquire as a result of their training at your academy?	4.2 Digital Literacy 4.2.1 The Role of Digital Literacy in Basic Training 4.2.2 The age of the recruits 4.2.3 Digital Literacy Levels of Recruits 4.2.4 Recruiting and Digital Literacy
4. What is the relationship between actual police activities and academy training?	6. Which digital skills, if any, do you think police recruits should be taught at police training academies?	4.3 Recruit Training 4.3.1 Coaching and Field Training 4.3.3 Changing role of Frontline Officers
5. Which changes do police trainers identify as necessary to update the current police training curriculum?	8. If you were given the authority to make changes to the recruit training curriculum, which changes would you make and why? 9. Do the recruits you train ask for more training on digital technologies?	4.4 Changing Models of Training 4.4.1 Pedagogy in Police Training 4.4.2 Traditional Models Persist

Theoretical Framework 2. What are the attitudes of police trainers regarding the adoption and teaching digital literacy skills? 6. How might future technologies impact police education in Canada?	4. How would you characterize your own level of digital literacy as well as those of the instructors at your academy? 10. How receptive are your students to learning about digital technologies? Has this changed over time? 11. How do you see either what we train or the way we train recruits changing in the next 5-10 years? 12. What is the greatest challenge to incorporating more digital skills content and courses into police training curriculum in Canada?	4.5 Technology Adoption 4.5.1 Attitudes and Dispositions of the Instructors 4.5.2 Technology Use in Training 4.5.3 Barriers to Technology Adoption 4.5.4 Budgets, Resources and Admin Support 4.5.5 The Impact of Emerging Technologies on Adoption