

AN INVESTIGATION OF DIGITAL FORENSIC CONCEPTS IN AN
INTERNATIONAL ENVIRONMENT: THE U.S., SOUTH AFRICA, AND NAMIBIA

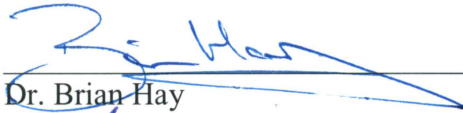
By

Amelia Phillips

RECOMMENDED:



Dr. Uma Bhatt



Dr. Brian Hay



Dr. Jon Genetti



Dr. David Blurton



Dr. Kara Nance, Advisory Committee Chair

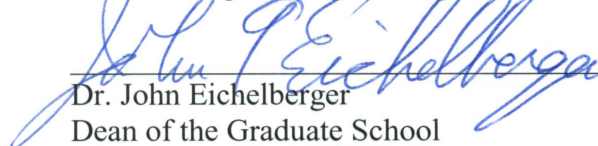


Dr. Jon Genetti, Chair
Department of Computer Science

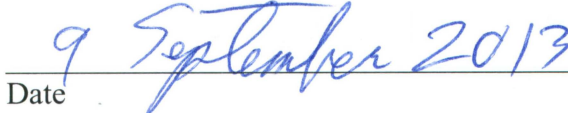
APPROVED:



Dr. Douglas Goering
Dean, College of Engineering and Mines



Dr. John Eichelberger
Dean of the Graduate School



Date

AN INVESTIGATION OF DIGITAL FORENSIC CONCEPTS IN AN
INTERNATIONAL ENVIRONMENT: THE U.S., SOUTH AFRICA, AND NAMIBIA

A
Dissertation

Presented to the Faculty
of the University of Alaska Fairbanks

in Partial Fulfillment of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

by

Amelia Phillips, B.S., MBA-TM

Fairbanks, Alaska

August 2013

ABSTRACT

Digital forensic investigations are growing in number not only in the United States but in nations around the world. The activities of multinational corporations and cybercrime cross jurisdictional boundaries on a daily basis. This investigation sets out to perform a qualitative analysis of the requirements needed for acceptance of digital evidence in multiple jurisdictions and the qualifications of digital forensic examiners by focusing on three case studies. The countries chosen are the United States, South Africa and Namibia. The research lays the foundation by examining existing international laws and treaties, and then uses the three case studies to address constitutional issues, civil and criminal law as they pertain to digital evidence. By ascertaining where the similarities and differences lie, a grounded theory approach is used to provide digital forensic examiners, legal staff and investigators a basis that can be used to approach digital cases that come from or must be presented in foreign jurisdictions. As more countries struggle to establish their digital laws regarding investigations, the resulting approach will serve as a guide and reference.

Keywords: digital evidence, multijurisdictional, cybercrime, computer forensics, digital forensics, digital law, computer investigations, digital investigations

TABLE OF CONTENTS

	Page
Signature Page	i
Title Page	iii
Abstract	v
Table of Contents	vii
List of Figures	xi
List of Tables	xiii
List of Appendices	xv
List of Acronyms	xvii
Acknowledgements	xxi
Dedication	xxiii
Chapter One	1
Background	2
Purpose of the Current Study	7
Case Studies	9
Approach and Focus of the Investigation	12
Importance of the Study	14

Summary	14
Chapter Two – Literature Review	17
Literature Related to International/National Digital Evidence, Processes, Rules, and Training	18
International Digital Evidence Sources	19
United States Literature Search.....	30
Rules, Statutes and Legal History..	30
Training and Licensing of Experts.....	45
South African Related Literature	56
Rules, Statutes and Legal History..	56
Namibian Related Literature	65
Rules, Statutes and Legal History.	65
Email Issues on the International and National Scenes	70
Case Law.....	73
U.S. Case Law.....	74
Case Law in South Africa and Namibia.....	81
Extradition Law	87
Literature Related to Qualitative Analysis, Case Studies, and Grounded Theory	88
Summary	93

Chapter Three – Comparison of Case Law	95
U.S. Case law	95
South African Case Law	107
Namibian Case Law	111
Summary	112
Chapter Four - Hypotheses and Comparisons	115
Examination of Commonalities	117
Examination of Variances	129
Forensic Investigators and the Judiciary	131
International Cooperation	135
Summary	137
Chapter Five - Expert Opinions	141
Expert One	142
Expert Two	143
Expert Three.....	145
Expert Four	148
Expert Five.....	149
Expert Six.....	150
Expert Seven.....	153

Expert Eight	154
Expert Nine	156
Summary	159
Chapter Six - Conclusions and Next Steps	161
Conclusions and Resulting Grounded Theory	161
Challenges	172
Implications and the Way Forward	174
REFERENCES.....	179
Appendices.....	193

LIST OF FIGURES

	Page
Figure 1 - Areas of Study (Nance & Ryan, 2011).....	7
Figure 2 Republic of South Africa (citation in footnote).....	57
Figure 3 - Namibian Regions Post-Independence (citation in footnote)	66
Figure 4 - Use of Case Studies with Grounded Theory	93
Figure 5 - Mobile Device Warrant Decision Flow	100
Figure A1 - Conceptual Drawing.....	194
Figure A2 -Entity-Relationship Diagram.....	196
Figure A3 - Database Navigation Menu	207
Figure A4 - Federal or Country Rules Form.....	208
Figure A5 - State-Province Form.....	209
Figure A6 - Case Law Form.....	210
Figure A7 - QBE Grid.....	211
Figure A8 - Resulting Report.....	213

LIST OF TABLES

	Page
Table 1 - Comparison of the Laws of the Three Countries	94
Table 2 - Development of Common Search Criteria	112
Table 3 - FRCrP Rule 41 and Relevant Sections	119
Table 4 - Chapter 2 of CPA Act 51	120
Table 5 - Namibian Act 25 of 2004	121
Table 6 - Applicable Rules of the FRE	123
Table 7 - Comparison of Criminal Laws	165
Table A1 - Country Table	197
Table A2 - Country Table Data	197
Table A3 - Federal or Country Rules	198
Table A4 - Rule Type	198
Table A5 - Populated Rule Type Table	199
Table A6 - Key Terms	200
Table A7 - Populated Key Terms Table	200
Table A8 - Populated Federal or Country Rule Table	201
Table A9 - State-Province Table	202
Table A10 - Populated State-Province Table	203
Table A11 - State Rules Table	204
Table A12 - Populated State Rules Table	204
Table A13 - Federal Rules Subsections	205

	Page
Table A14 - Populated Federal Rules Subsections	205
Table A15 - Case Law Table	206
Table A16 - Populated Case Law Table	206
Table A17 - Query Results	212
Table B1 - Country Table	215
Table B2 - State-Province Table	216
Table B3 - Federal or Country Rules	223
Table B4 - Federal Rule Sections or Subsections	226
Table B5 - State Rules.....	227
Table B6 - Case Law	237
Table B7 - Rule Type	249
Table B8 - Common Search Criteria.....	250

List of Appendices

	Page
Appendix A – Database Design	193
Appendix B – Populated Tables	215
Appendix C – Copyright Permissions.....	251

LIST OF ACRONYMS

ACLU – American Civil Liberties Union

ACT 57 – South African Computer Evidence Act 57 of 1983

ABA – American Bar Association

ADA – Americans with Disabilities Act

BTK – Bind, Torture, Kill serial killer

CEO – Chief Executive Officer

CERT – Community Emergency Response Team

CESPAM – Center of Specialization for Public Administration and Management

CFAA – Computer Fraud and Abuse Act

CIA - United States Central Intelligence Agency

CNIL – The French Data Protection Agency

COECC – Council of Europe’s Convention on CyberCrime

CPA – Criminal Procedures Act

DEFER – Digital Evidence First Responder

DFCB – Digital Forensic Certification Board

DOJ – Department of Justice

ECPA – Electronic Communications Privacy Act

ECT 25 – the South African Electronic Communications and Transaction Act 25
of 2002

EDI – Electronic Data Interchange

EDMS – Electronic Document Management Systems

EDRM – Electronic Discovery Reference Model

EEDI – End-to-End Digital Investigation

EEOC – Equal Employment Opportunity Commission

ENFSI – European Networks of Forensic Science Institutes

ESI – Electronically Stored Information

ETA – Australian Electronic Travel Authority

EU – European Union

EULA – End User License Agreements

FBI – Federal Bureau of Investigation

FISA – Foreign Intelligence Surveillance Act

FRCP – the U.S. Federal Rules of Civil Procedure which are applied to federal cases regarding civil torts

FRCrP – the U.S. Federal Rules of Criminal Procedure which are applied to federal cases regarding criminal law

FRE – the U.S. Federal Rules of Evidence which apply in both civil and criminal proceedings.

GPS – Global Positioning System

HIPAA – Health Insurance Portability and Accountability Act

IACIS – International Association of Computer Investigative Specialists

IGRM – Information Governance Reference Model

ICT – Information and Communications Technology

IOCE – International Organization on Computer Evidence

ISP – Internet Service Provider

IT – Information Technology

NamLex – Index to the Laws of Namibia

NIST – National Institute of Standards and Testing

NSA – National Security Agency

OCGPA – Online Communications and Geolocation Privacy Act

PI – Private Investigator

S.A. – South Africa

SADC- Southern African Development Community (namely sub-Saharan Africa)

SANS – System Administration, Networking and Security Institute

SCA – Stored Communications Act

SEC – Securities and Exchange Commission

UBS – Union Bank of Switzerland

UCT – University of Cape Town

UECA – Canadian Uniform Electronic Commerce Act

UETA – U.S. Uniform Electronic Transactions Act

U.K. – United Kingdom

U.N. – United Nations

UNCITRAL – United Nations Commission on International Trade Law

UNECE – United Nations Economic Commission for Europe

UPL – Unauthorized Practice of Law

U.S. – United States

ACKNOWLEDGEMENTS

My sincere thanks go to my advisor and supervisor, Dr. Kara Nance for her support throughout this process. Also thanks to my entire dissertation committee for their guidance.

Special thanks go to my administration, Dr. Jack Bermingham, Jeff Wagnitz, Alice Madsen and Dr. Rolita Ezeonu who have funded and supported me as I experienced what it means to get a PhD. And a hoorah to the NMMU Harassment Group for all the great conversations about researching and writing a dissertation and all the support we got from each other. I also want to thank all my friends and family who have listened to me as I did this.

DEDICATION

This paper is dedicated to my two surviving aunts – Bernice P. McRae who turned 100 years old this year the day I got final approval and Dr. Eunice P. Grisby who has been a staunch supporter. Both of them are retired teachers and have been an inspiration to me.

CHAPTER ONE

This dissertation is a qualitative analysis of international digital law using grounded theory and case studies¹ to establish new theories. A primary outcome of this discourse is to lay groundwork for legal proceedings regarding digital evidence in a global world dealing with multinational corporations and an increasingly interconnected economy which encounters legal systems that may or may not work well together. The motivation for this study came from teaching digital forensics investigative techniques in a foreign country. When dealing with one particular topic related to the rights of employees, a student promptly stated “You can’t do that in our country.” Upon further discussion it was determined that while both individuals were from democratic nations, the nuances between them introduced just enough differences to cause concern in the methodology used in a corporate investigation.

So how does one determine the laws, treaties or rules that must be adhered to in each country that will affect how digital evidence must be treated? Digital evidence comes in many forms including email, smartphones and electronic documents. What happens when two jurisdictions are involved in a legal proceeding with digital evidence? Investigators are trained in dealing with their own jurisdiction. What else do they need to become aware of to work in this ever expanding global world?

In this chapter, the basic premise is laid to approach these questions. The chapter begins by addressing the background of digital forensics and how the definitions have grown with the technology. The second section goes into greater depth on the purpose of

¹ The Case Studies are the United States, Namibia and South Africa

this study and the approach used to generate a grounded theory. The third section gives a brief background on the case studies chosen and the reasoning behind the selection. Next a description of the focus and approach of the investigation is given along with the objects of the search. Finally, the chapter concludes by giving the importance of the study and the potential impact.

Background

To initiate the investigation, first one must define digital forensics. Ken Zatyko, the former Director of the Defense Computer Forensics Laboratory, wrote a commentary that addresses the various disciplines grouped under digital forensics including video forensics, intrusion forensics, network analysis, software analysis and a variety of other disciplines or techniques when using the term digital forensics (Zatyko, 2007). In the commentary, he compares various sources and comes down to the following definition:

The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation.

(Zatyko, 2007)

The items that he lists affect admissibility in a court of law and should be applicable in any country in regards to digital evidence. Zatyko goes on to present eight

steps needed for a scientific approach to digital forensics science. Specifically, “search authority, chain of custody, imaging/hashing² function, validated tools, analysis, repeatability, reporting and possible expert presentation (Zatyko, 2007).” While his is not the only definition available, it is a valid one from which to start.

For this research effort, the term digital forensics refers to the application of scientific methods to discover, collect and analyze digital data and metadata³. The term “e-discovery” is used to refer to data mining for use in litigation. While the focus of the research is digital forensics, e-discovery laws are more firmly in place due to multinational corporations and can have a bearing on the digital forensic aspects.

Digital forensic investigations are performed in multiple jurisdictions worldwide. Many of these investigations cross jurisdictional lines. The prevalence of laptops, tablets, cell phones and other mobile digital devices means digital evidence is used in a majority of cases that are tried in the civil and criminal courts.

With multinational corporations, mobile devices and new technologies such as the ubiquitous cloud⁴, the need for an understanding of the digital laws of various nations is crucial. The ultimate challenge is dealing with the different approaches to digital evidence – i.e., what is admissible as evidence and what is not.

The initial place to begin is at the international level. The United Nations

² Hash values are used in digital forensics to verify that a file or drive image has not changed. Alterations as minute as the deletion of a space cause a change in the hash value. The hash types include MD5, SHA 256, and SHA 512.

³ Metadata is literally “data about data”, this can information regarding the modified, accessed and creation data of a file, to whom the application is registered, IP addresses when dealing with email and other critical information.

⁴ The “cloud” is defined by the National Institute of Standards and Technology as “convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011)

Commission on International Trade Law (UNCITRAL) created the Model Law on Electronic Commerce which established definitions and procedures to govern electronic evidence in the late 1990s (United Nations, 1999). E-commerce was initially the primary reason many countries were forced to deal with cybercrime. Definitions such as “data message” (United Nations, 1999) and “originator” are spelled out in the document. Such definitions can be used by each nation as they create their laws and procedures. The United States and the European Union (E.U.) along with the United Kingdom had some laws in place and have had to add more and more laws to deal with the changing landscape.

The U.N. Model Law unfortunately only focuses on civil or corporate law. Guidelines for how to approach criminal cases in the digital world were not addressed in the resolution⁵. Most countries approach their own civil and criminal cases much differently. Further examination of the literature confirms this statement. The situation is further complicated by the fact that a civil case can lead to a criminal case and vice-versa. So how does one deal with multijurisdictional cases?

In the United States, federal statutes and guidelines are in place for digital forensics and e-discovery. Take for example, the document from the U.S. Department of Justice (DOJ) entitled “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations” (U.S. Department of Justice, 2009). This document is updated as new technologies are released and offers guidelines not only for when subpoenas and warrants are necessary, but for standard polices that companies and

⁵ Note that the ISO Standard for Digital Forensics was passed and accepted in late 2012. Its effects are only now being incorporated at national levels.

government agencies should have in place. The Federal Rules of Civil Procedure (FRCP) was updated in 2006 with specific terms regarding e-discovery (U.S. House of Representatives, 2010). Because of the prevalence of email, text messaging, and instant messaging, the Electronic Communications Privacy Act (ECPA) (U.S. Department of Justice, 2010) has significant bearing on any digital forensics case in the United States. Even with these in place, the individual states approach digital evidence and even the practice of digital forensics in significantly different manners.

Digital forensics has grown over the last few decades into a recognized profession. Several challenges exist even in the United States: 1) there is no standard accreditation for the practitioner; and 2) no single forensics tool meets all the existing standards. The National Institute of Standards and Testing (NIST) has established testing standards (NIST, 2010) that conform to ISO Standards 17025 and 27001. Vendors such as Guidance Software and AccessData have various levels of certification that adhere to their particular forensic tools. However, not everyone uses their tools nor has access to their training.

Efforts have been made over the last five years to create a standard for the practitioner. To date, none have been ratified in the United States. Individual states have taken various steps to standardize the requirements for practitioners going as far as requiring all digital forensic investigators to be licensed as private investigators. Several states including Texas, South Carolina and Michigan instituted such laws and brought many investigations, both criminal and civil to a halt (Phillips & Nance, 2010). One case took digital evidence to the extreme and charged that since the company taking pictures

for people running red lights in a town in Texas was not licensed as a private investigator; all the tickets were invalid (Phillips & Nance, 2010). If such problems can occur within the United States when dealing with internal jurisdictions, imagine the situations that can transpire on the global scale.

Such an example occurred in 2011 when a Fortune 500 multinational company was conducting an internal investigation. The investigators tunneled into the suspected employee's computer on the corporate network, captured the Microsoft Outlook PST files and analyzed them. The employee was a foreign national living in his native country. He complained to the local authorities. When the U.S. investigator arrived in the country to retrieve the company computer, the investigator was arrested by the local authorities of being in violation of their laws even though it was corporate property (R. Godfrey, personal communication, June, 2011).

To resolve these issues, a systematic worldwide approach should be applied to the existing laws, statutes and policies. In their paper entitled *Legal Aspects of Digital Forensics: A Research Agenda*, Nance and Ryan examine the legal areas that need further study in regards to digital forensics (Nance & Ryan, 2011). They also explore the methodology applied to different aspects of digital forensics. Figure 1 shows the prototype they developed. The prototype looks at constitutional law, evidence law, criminal procedure and other items that may influence the legality of digital evidence.

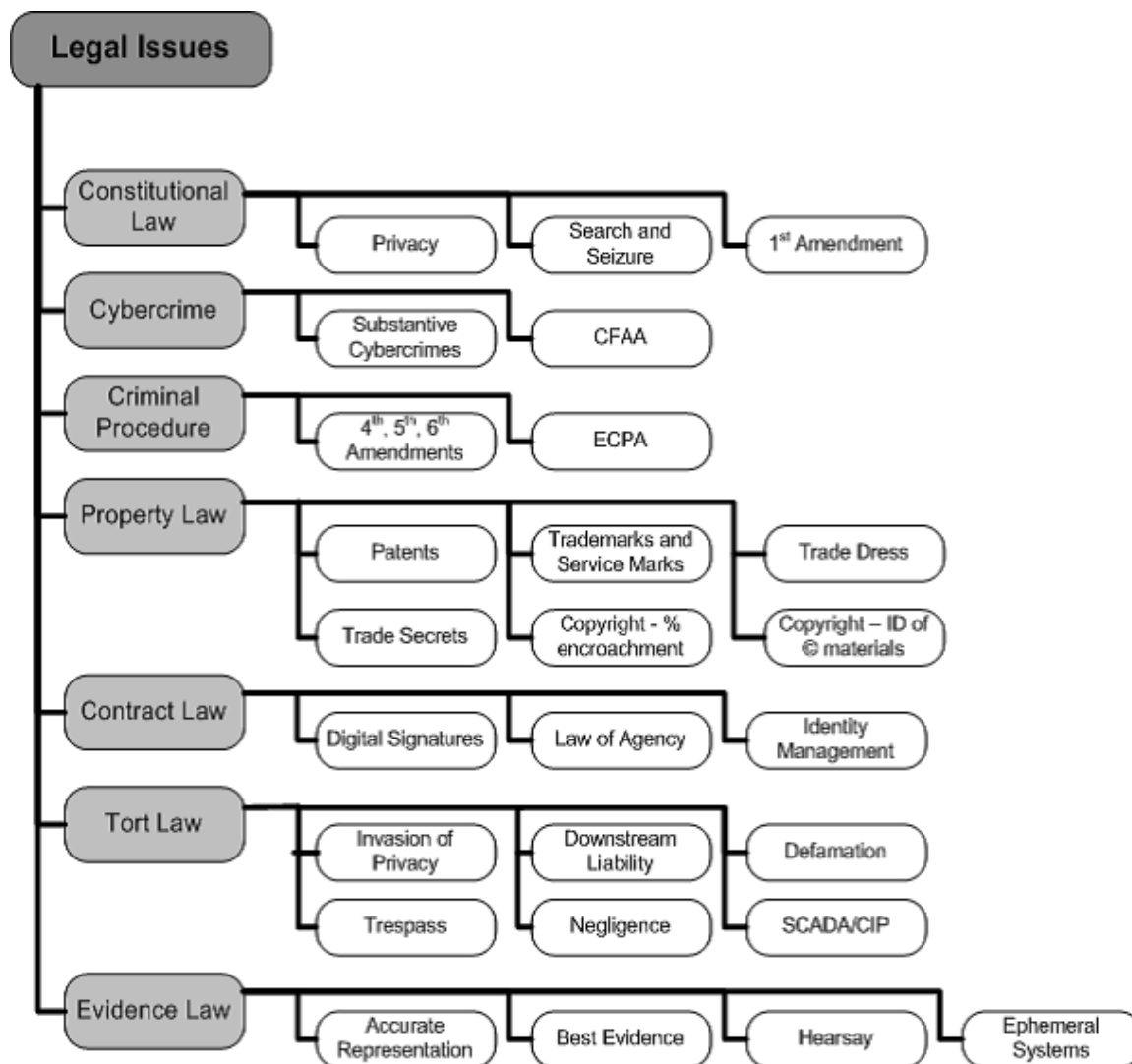


Figure 1 - Areas of Study (Nance & Ryan, 2011)

This paper does not attempt to address all of the items listed in the prototype. Instead the research focuses on very specific aspects, namely: constitutional law, evidence law, parts of tort law and cybercrime.

Purpose of the Current Study

The focus of this study is the ability to present digital evidence in court. Digital evidence is pervasive and crosses national borders. The question becomes how does one

insure the evidence will be accepted in foreign courts or in one's own. To accomplish this goal, the primary gap in knowledge is threefold:

1. If a case is being tried in another country, what conditions are there on the collection of the evidence, the investigator, forensic tools used, etc. for evidence collected in one's own country to be used in a foreign court?
2. If the case is being tried in one's own country, what conditions, procedures or laws need to be met for digital evidence collected elsewhere to be admissible in one's own court?
3. How does one qualify the digital forensic practitioner or investigator in one's own jurisdiction and what is required to have that expertise recognized in another jurisdiction?

The study targets the answers the questions listed above by examining three case studies in three countries and focuses on how their laws affect digital forensic investigations. Because each country will have its own nuances, the laws must be parsed and mapped to show the relationships. To accomplish this objective the study examines:

- the constitutional law of each country as it applies to privacy, search and seizure, and basic human rights
- their civil and criminal procedures
- their rules of evidence
- privacy laws and
- current case laws that exist for digital evidence and investigations

The desired outcome is to expand the groundwork for a standard approach to digital investigations that may be applicable and accepted in most countries. The study begins by looking at the current international bodies such as the U.N. that have established procedures. Next, the study identifies countries and regions to see how these procedures and policies are applied. By performing a qualitative analysis of the information gathered, a template can be generated that can be used when dealing with another country or when trying to assess how to present digital evidence in a country other than one's own.

Case Studies

After a preliminary investigation of countries and regions, three were selected for in-depth analysis. The first case study is the United States. One crucial element is that many countries that are currently creating new laws refer to the existing laws of other countries, such as the U.S., as a basis. If the existing laws have fallacies, how can those countries assist countries who are now establishing their laws from making the same mistakes? Collectively, the Fourth Amendment, the Federal Rules of Criminal Procedure, the Federal Rules of Civil Procedure and the DOJ's 2009 document (referred to at the start of this paper) create a framework from which to start in the examination of the United States. Because many multinational corporations are headquartered in the U.S., the issues that affect corporate investigations are more readily available. The Sedona Principles⁶ (Sedona Conference, 2011) were created in 2004 to address discovery of ESI prior to the update of the FRCP in 2006. Many states do apply these principles to e-

⁶ The Sedona Principles are discussed in detail in Chapter Two.

discovery and some of the principles can affect digital forensics.

The second and third case studies examine the laws of Namibia and South Africa. South Africa is one of the financial cornerstones of the African continent. In addition its influence on the rest of Africa is significant. South Africa is also an international hub with visitors from Europe, Brazil, Australia and the U.S. frequenting its shores annually. The nation has struggled against odds to grow and improve the lives of its peoples. Namibia, prior to the fall of apartheid, was referred to as South West Africa and was considered part of South Africa. Even after independence, many laws in Namibia parallel the laws in South Africa especially in regards to international issues. And, as will be shown, in some instances the laws are the same. One may question why are they not being examined as a region. The answer is quite straightforward. Namibians refer to their independence in much the same way citizens of the United States do, although independence was much more recent and still in the conscious memory of many who are not even middle-aged. Throughout this study, however, the effects of being a prior protectorate can be seen to have had an impact on the laws.

Both countries are part of the Southern Africa Development Community (SADC) region which is comprised of 15 countries. Of those countries, a limited number actually have e-laws, South Africa and Namibia being two of them. Countries in the SADC region work closely together to create laws and meet regularly. Therefore, examining two of the nations that have taken the lead in addressing e-laws can prove fruitful to understanding and influencing other nations in that region. Because of the trade and Internet access, both South Africa and Namibia look to the EU for guidance. Both

countries trade heavily with countries in the EU. Additionally, e-commerce companies may choose to use servers in countries such as Germany because of the greater bandwidth. Therefore, both countries have to be aware of the laws of the EU by default.

Another reason for choosing these two nations is that Namibia and South Africa both have e-laws that are relatively new and not mired in too many appeals. Care was taken in Namibia to align the laws with those of other countries; therefore the results are easily expandable to other developing nations. The South African Law Reform issued a document in 2010 to address digital evidence (South African Law Reform Commission, 2010). The Commission drew heavily from the U.N. Model Law and then added items to address criminal cases. The training of digital forensics investigators in Namibia is also recent. The first class in digital forensics at the Polytechnic of Namibia took place in 2005. Similar classes have been proposed and implemented at the University of Cape Town. Much of what is done in one country directly affects what happens in the other.

These three case studies represent a foundational step to begin addressing the problems of acceptance of digital evidence in courts worldwide and the qualifications of the digital forensic expert. Examination of the U.S. laws, policies and acts provides the baseline from which many countries draw their laws. The analysis of Namibia and South Africa targets countries whose laws are based on or drew directly from U.S. law and whose statutes were founded on British or Dutch law. The two nations also serve as an example of reciprocal arrangements.

Approach and Focus of the Investigation

As mentioned previously, this investigation is using a qualitative approach which differs from a quantitative approach in some key areas. While both are scientific methods, a quantitative method is more rigid and seeks to confirm a hypothesis as opposed to the qualitative method which is flexible and seeks to form a hypothesis.

Below are some other key items of a qualitative analysis:

- Explore phenomena
- Use of iterative questioning methods
- Semi-structured
- Open ended questions
- Describe variations
- Describe and explain relationships
- Study design is iterative – meaning the responses given by interviewees can affect the next question asked or the next step taken in the investigation

(Family Health International, 2005)

The use of a qualitative approach allows one to truly explore the case studies without a preformed hypothesis. This study is searching for the variations in the laws and rules that could become critical during a digital forensic investigation. This style of research also allows for cultural differences. The laws of nations are a direct result of their individual histories which can affect how things are accomplished.

By using a grounded theory approach, inductive reasoning is employed to create a theory based on the qualitative data that is collected. In this instance, the data will be done via the case studies – i.e. the laws and processes of the three chosen countries. To acquire the data, the focus of the investigation is how to effectively bring the items found in digital forensic investigations to trial. Digital forensics comes into play in both civil and criminal cases and rules of evidence affect how evidence is collected and handled in all three countries. Civil law and statutes pertain to situations such as a lawsuit between corporations or torts. Criminal laws come into effect when addressing theft, murder, and related actions.

The constitution and individual rights of plaintiffs in each nation must be considered when addressing criminal cases. Individual rights may also be relevant in certain civil cases. As a result, part of the focus of this investigation is to ascertain how deeply one must understand the individual rights when dealing with a criminal case that is multinational.

The United States, Namibia and South Africa are each common-law nations. In a common-law country, if a law does not exist such as for use of new technology, cases that have gone to trial can be used to “render a verdict or challenge a decision” (Phillips, Godfrey, Brown, & Steuart, 2014). In addition to examining which rules were used in cases to render a verdict, this investigation searches for pivotal cases that:

- resulted in new laws, rules or statutes
- are referenced frequently by other cases or
- were challenged later

Importance of the Study

As the world continues to evolve as a global society and more nations, citizens, and corporations communicate, store data, and conduct relations on digital devices, more and more data is in electronic form. And, more importantly, some of the evidence for civil and criminal cases is electronic and may be located or collected in another jurisdiction. While the international laws and treaties exist, they simply cannot accomplish what is needed in the day to day operations of digital investigations on their face because such laws rely upon the individual member nations to have local laws in place.

While this study focuses on common-law nations, which comprise less than 50% of all countries, it is relevant when many of those nations are the ones upon which countries entering the digital era base their laws. By examining the United States, which has differing laws among its fifty states and territories, it can be determined which items have the most variance. Next comparing those to the issues and laws in Namibia and South Africa, one can discover if those same items cause the most contention.

The database that is submitted with this investigation creates the foundation for a quick reference that future studies can add to. The database begins to create correlations on a granular level of data that exists, but tends to be in isolated areas and not easily linked.

Summary

By selecting three common law countries, two of which regularly do business cross borders, it should be possible to create a template by which to determine if the evidence in one country would be acceptable in the corresponding country's courts.

Each country's constitution must be examined with particular attention paid to the rights of the individual. The statutes, laws and policies that affect privacy, rules of evidence along with civil and criminal procedure in relation to digital evidence are researched and examined in this discourse.

CHAPTER TWO – LITERATURE REVIEW

In a qualitative analysis, all information gathered is part of the data that has to be examined. The literature review sets the stage to ascertain what work has already been done and to determine the level of the existing digital laws on the international scale. Next this same search must be applied to each country in order to glean a hypothesis from the questions that were put forward in Chapter One. As was shown in the prototype created by Nance and Ryan, items such as civil law, criminal law, rights of individuals and evidence law need to be found (Nance & Ryan, 2011). Because one is dealing with national and international law, the time frames span decades and in some cases, cross the century marks.

In creating the search terms, the focus of the topic was kept in view. The dissertation is focused on how to bring items to be accepted in a court of law; therefore some sources have been omitted because they did not bring anything new to the table. Others have been eliminated because the topics were not relevant to digital forensics in the United States, Namibia, or South Africa.

In searching the literature, combinations of the following terms were used: digital law, digital evidence, computer forensics, privacy laws, digital forensics, international digital law, South Africa, Namibia, and the United States. Recall that qualitative analysis is iterative. Therefore, after interviewing the experts, terms including extradition and foreign evidence were added.

The composition of the chapter evolved as the data was collected and the final result was to formulate the data with the case studies. As was noted in Chapter One,

international laws and treaties set the foundation for countries to meet. First, the international laws and treaties are explored. In the subsections that follow each nation along with the literature from experts are examined. Note that because email is so prevalent in each subsection and cross boundaries, it is in its own subsection. Case law literature is explored in depth. And finally the literature related to qualitative analysis, grounded theory and case studies is examined.

Literature Related to International/National Digital Evidence, Processes, Rules, and Training

Multijurisdictional evidence has become the norm rather than the exception in both civil and criminal cases. In searching for literature that is relevant to this investigation, one must first define where digital evidence may be found as well as the nature of the evidence. Digital evidence can be found on cell phones, smart phones, laptops, palmtops, and a multitude of devices. Such evidence is easily damaged, can be altered, etc., prior to acquisition. In searching for international, multijurisdictional digital evidence laws, the results were not as abundant as in other areas of international law.

In this section, the reader is presented first with international laws and statutes that relate directly to device forensics and its admissibility at the global level. Using the legal framework prototype introduced in Chapter One for each county in the case study, the following literature is examined from the perspective of collection and use of digital evidence:

- The rules of civil procedure

- The rules of criminal procedure
- The rules of evidence
- The qualifications of the digital forensic investigator and the tools
- Privacy laws including email
- The court system including judges and attorneys

Each of these affects what is accepted in a court of law whether it be in the United States, South Africa, Namibia or other common law nation. They vary according to the history of each nation, but the international laws and treaties try to make agreements with which each nation can comply.

International Digital Evidence Sources. An examination of international treaties - such as the Convention on Cybercrime (Council of Europe, 2001) - helps to determine the current status of international digital law. International digital law is the umbrella under which multinational jurisdictions are managed. Much of this is handled through treaties; therefore it is necessary to examine existing agreements and treaties before delving into the individual nations in order to ascertain how the international arrangements may affect the local laws.

The Convention on Cybercrime was initiated in 2001 and put into law in 2004. The U.S., Canada, Japan and South Africa are among the signatories on the Convention. This treaty requires each member state to create laws that address computer trespass, computer fraud, hacking and similar crimes. While parts of the treaty do address device forensic data, much of it deals with transmission of information which may be indicative

of where more work needs to be done. Other portions require international cooperation. In several of the amendments, the Convention states “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law” (Council of Europe, 2001). This raises interesting questions as to whether or not the domestic law of a country is adequate for presentation in a foreign court. Article 23 goes on to specify that international cooperation is to be handled by relevant instruments and that “to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence” (Council of Europe, 2001). If such instruments do not exist, the Convention goes on to describe the necessary steps.

Again there appears to be a need that has remained unsatisfied. In 2011, an article appeared regarding Australia joining the Convention and describes some of the items that the Australian courts must establish in order to be in compliance (Corner, 2011). A specific item was that Australia needed to develop a national data preservation policy for ISPs and other data carriers in the event warrants were delayed. The article also paid attention to the fact that the treaty had the intent on “helping authorities from one country to collect data in another country (Corner, 2011)”. The Convention also includes wording on human rights in regards to the collection of ESI. The Convention pays particular attention to the collection of real time data or network data as opposed to device data. This wording points to the need of local policy and laws in regards to digital evidence on devices. In reading the Articles of the Convention, much of the wording is geared

towards criminal laws and offenses. So some civil offenses may not be addressed by the existing agreements.

After the Convention on Cybercrime, the next item to be examined is the U.N. Model Law on International Commercial Arbitration which was created to address commerce and later, specifically e-commerce (United Nations Commission on International Trade, 2006) . The U.N. Secretariat states regarding the Model Law “the need for improvement and harmonisation is based on findings that domestic laws are often inappropriate for international cases and that considerable disparity exists between them” (U.N. Secretariat, 2010). The body goes on to explain how domestic laws are well-suited for situations that happen within the borders of a country but are ill-prepared to deal with lawyers or clients from other countries. As was noted in the citing from the Convention of Europe, the treaty relies on the member countries having domestic laws in place. Many countries simply do not have the laws established to deal with the overwhelmingly rapid progress of technology. The U.N. Secretariat’s summary is one that supports this study in regards to what is needed on the international level.

Many nations in the SADC region, including South Africa and Namibia, used the U.N. Model Law as a basis when creating several of their e-laws. The United Nations Economic Commission for Europe (UNECE) spells out the U.N. Model Law and establishes the requirements for Electronic Data Interchange (EDI) between countries (UNECE - United Nations Economic Commission for Europe, n.d.). While this deals primarily with civil matters, one of the goals is to address the differences in laws so that international cases are not halted due to such differences.

To locate international standards for digital forensics, the European Network of Forensic Science Institutes (ENFSI) was examined. In 2006, ENFSI created version 5 of a document for best practices in forensic examination of digital evidence (ENFSI Working Group Forensic IT, 2006). The document is more of a general procedures document that does not go into great detail. It contains definitions and expectations. The members of the EU could use this as a guideline in their forensic laboratories. But again it is not sufficient as a true procedural document. What is needed is something with more specific procedures.

The International Organization on Computer Evidence (IOCE) drafted several documents for the G8 (International Organization on Computer Evidence, 2000) which provides guidelines for forensic examination of digital technology. Again this is a best-practices document which defines digital evidence, prevention of contamination of evidence, proper search and seizure, documentation and training (International Organization on Computer Evidence, 2002). The IOCE also gives basic guidelines that members should enforce in their investigations:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
- Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles

(International Organization on Computer Evidence, 2002)

The standards for digital investigations and practitioners draw from similar backgrounds. Stephen Mason edited two books on the topic; the first is now in its second edition entitled “Electronic Evidence” (Mason, 2010). It is a collection of writings by experts from various countries on electronic evidence. The primary editor and writer, Stephen Mason is well written in the field and highly regarded. The second edition includes the European and International Legislation regarding electronic evidence. The writers also explore the handling of evidence, characteristics of e-evidence, and the authentication of the evidence and the management of same. They then go into various primary countries in this book. The primary ones of interest to this research are the U.S. and South Africa. The most useful item is that they list the relevant cases for each country. These are examined later in this chapter. The second book covers countries that are emerging on the cyber scene (such as Venezuela, Brazil, Mauritius, etc.) and creating e-laws, but the information may not be as readily available (Mason, 2008). That case law

is listed for each country points to the assumption that because technology outpaces the law, case law will be the source of how new situations are approached in common law nations

Privacy law is one of the most prominent items that affects digital investigations. Several articles were found pertaining to issues of international privacy law as it relates to electronic evidence. Yannella and Rein examine the adoption by Canada, Australia and the United Kingdom of U.S. style of e-discovery. The article makes the claim that countries are looking towards the U.S. for guidance in dealing with the “enormous complexities presented” (Yannella & Rein, 2009) in dealing with electronic evidence. The article discusses the additional problem of multinational corporations and rightly points out the issues regarding privacy laws that must be addressed when dealing with discovery orders. A fascinating statement was that the litigation hold – which is common in the U.S. – is now required in Nova Scotia along with the “meet and confer” that came from the 2006 FRCP revisions. The article gives insight that perhaps on the civil side of litigation, more structure exists.

While France is not one of the countries included in this investigation, a situation arose in 2009 which demonstrates a privacy challenge in a civil case. The case deals with pre-trial discovery when a U.S. court requests information from a French company. It addresses French data protection which is similar to EU law and examines cross border litigation. What constitutes a small amount of data? What has been sufficiently anonymized? "The CNIL (the French Data Protection Agency) urged companies to ensure that American authorities comply with French data protection principles even if the

personal data of French residents is already located on U.S. territory, such as in a centralized human resources database of an American company with a French subsidiary" (VenBrux, 2009). The article also discusses the Safe Harbor rule and points to corporate rules that have to be in place when doing business with foreign subsidiaries.

After privacy issues, the next item examined was cybercrime. The Twelfth United Nations Congress on Crime Prevention and Criminal Justice examines cybercrime from an international perspective (U.N. Secretariat, 2010). The paper explores the importance of cybercrime and why attention is needed on the part of member countries. The report cites that one of the issues is the lack of solid statistical data of the extent of cybercrime, including arrests, prosecutions and convictions (U.N. Secretariat, 2010). The report is useful in pointing out very definite shortcomings. Issues regarding differences in national laws are discussed and the report states "cybercrime is international in nature". Much of what is covered in the discussion involves email, transmissions and child pornography, but the relevance to this study lies in its reference to the U.N. Model Law upon which South Africa's e-laws are based. The document also examines the Convention on Cybercrime. It stresses that domestic laws change much more slowly than technology and as a result problems remain. The paper concludes with suggestions on how to eliminate safe havens. Both of these topics are relevant in determining what is needed in international and local digital laws.

One of the references listed in the Twelfth United Nations Congress discourse is the document *Understanding Cybercrime: A Guide for Developing Countries*. As with many international references, the focus is on real time monitoring of trafficking in illicit

materials including child pornography and terrorism. The paper addresses definitions, criminal law, computer forensics and relevant legislature in member nations. The conclusion drawn is similar to other sources; the reference comes back to the ability of the digital forensic expert. Whether dealing with child pornography, hate mail, fraud, identity theft, gambling or corporate espionage, the ability of the examiner is foremost (International Telecommunications Union, 2009). The paper goes on to say “despite the widely recognised importance of harmonisation, the process of implementing international legal standards is far away for being completed. One of the reasons why national approaches play an important role in the fight against cybercrime is that the impact of the crimes is not universally the same” (International Telecommunications Union, 2009). Domestic laws may fall short of what is needed. In examining international agreements, the paper notes:

The Convention on Cybercrime as well as the Commonwealth Model Law and the Stanford Draft Convention provide legal solutions for illegal interception only. It is questionable whether Article 3 of the Convention on Cybercrime applies to other cases than those where offences are carried out by intercepting data transfer processes. As noted below, the question of whether illegal access to information stored on a hard disk is covered by the Convention was discussed with great interest (International Telecommunications Union, 2009).

The distinction between network forensics and device forensics is particularly of interest here. If international agreements primarily exist to combat terrorism, child pornography, and transmission of illicit data, then internal breaches may not be addressed by such agreements. Another item that is mentioned is real time or what is called “live acquisition” of network devices. To date, digital forensics has customarily been performed on machines that are powered off. Live forensics means that the machine is on. And because items such as the RAM are changing during the acquisition itself, the results are not reproducible and therefore do not conform to forensic standards. This is an item that has not been truly tested in a U.S. or other court of law. It is one of the items that may stand out in this query.

As was mentioned in Chapter One, e-discovery procedures appear to be more structured and more established than forensic procedures. The International Competition Network, which was formed over a decade ago, surprisingly enough has assembled a manual which includes a very substantial chapter on the gathering of digital evidence. Chapter Three of their Anti-Cartel⁷ Enforcement Manual was assembled by sending out a questionnaire to their members which now includes “104 competition agencies from 92 jurisdictions” (International Competition Network, 2009a). Twenty four agencies responded including those from the United States., the United Kingdom and Japan. The U.S. Department of Justice and the U.S. Trade Commission are members. The manual details processes for dealing with digital evidence gathering within an organization, how to deal with privileged and private data, training of staff, what to do when data is stored

⁷ Note that the use of the term anti-cartel is synonymous with the term anti-trust in the United States.

offsite and a host of other items that this research is examining (International Competition Network, 2010). The only drawback to the manual is that in stating that respondents have items in place, the manual does not specify which country. Chapter One of the manual focuses on search and seizure of premises by spelling out how to prepare for a search, how to put together a team, how to conduct a search and search of an arrested person. It also examines when a search warrant is needed (International Competition Network, 2009b). Of all the processes and procedures examined, this is the most thorough.

As happens frequently in a qualitative study, the interview with Marthie Grobler⁸ detailed the imminent release of an ISO standard for digital evidence. The final ISO standard was released in October of 2012. The document defines the Digital Evidence First Responder (DEFER) as the one who collects the evidence, chain of custody, and storage of digital evidence. The details regarding the planning and responsibilities of the acquisition are well laid out including such items as dealing with powered on devices, encryption and suspected malware. Procedures to follow when dealing with servers that cannot be powered down or when the amount of data is such that only a partial image is practical are also discussed.

The ISO standard applies an approach similar to Bloom's taxonomy to the core skills that have been defined for the DEFER. The four core skills are digital evidence identification, collection, acquisition and preservation. The three competency levels that are defined by the standard are awareness, knowledge and skill (ISO/IEC 27037, 2012).

⁸ See Chapter Five, Expert One.

Similar to levels in Bloom's taxonomy of educational objectives the person progresses from awareness in which they know when to ask for help, to the expert at the skill competency level at which they operate independently and exercise critical thinking to solve complex problems.

Appendix B of the ISO standard lays a baseline for evidence transfer. The standard states that "the documentation requirements for cross-jurisdictional digital evidence transfer are not equal in different jurisdictions" (ISO/IEC 27037, 2012). The minimum requirements specified are:

- the relevant authority's name and address;
 - a statement of the DEFR's authorization, training and qualifications;
 - the purpose of the examination;
 - what actions were carried out;
 - who did what and when;
 - the chain of custody pertaining to the specific investigation;
 - descriptive listing of potential digital evidence and digital storage media collected and acquired; and
 - information regarding any examinations, tests or investigations used to create the evidence copy
- (ISO/IEC 27037, 2012)

As will be seen in Chapter Five, the Honorable Justice Mainga⁹ stated that he would accept evidence from another country if it were accompanied by a sworn affidavit. The minimum details laid out by ISO/IEC 27037 would provide him with that along with his additional requirements that proof be shown that the evidence was properly collected and that procedure was followed.

In exploring the international agreements, while some items have been addressed, on others there have been false starts without a final congealing. The new ISO standard shows that things have progressed. Many assume that international digital forensic laws exist because the cooperation is there for transmission of data and addressing such items as child pornography, illicit data transmission, money laundering, etc. However, an ISO standard does not supersede local law and even with such cooperation - when faced with local laws it appears things are not as clean cut.

United States Literature Search

Rules, Statutes and Legal History. After examining international law, the relevant history of each nation and its effect on the laws needs to be examined. There is a basic assumption that the United States is a common law nation. First the term “common law” needs to be defined. Common law comes from the British system in which rulings were done by what was customary instead of driven by statutes. Common law is “embodied in case law rather than legislative enactments” (Farlex Inc, 2005). The relevance of this in the current study is that case law determines how laws are applied and are based on previous rulings. If a type of case has not been tried before precedent can be

⁹ See Chapter Five, Expert Nine

set by the outcome of a new case. And bad case rulings can cause issues until new case law comes forward.

In stating the United States is a common law nation one must examine how true is that statement. In the paper *The Common Law and Civil Law Traditions* housed at the School of Law at the University of California, Berkeley, one is reminded that several countries colonized the continental United States, beginning with the Spanish (Robbins Religious and Civil Law Collection, n.d.). Beginning in the fifteenth century, Leif Ericson followed by Christopher Columbus explored parts of the U.S. Both men were leading Spanish explorers. The decades and centuries that followed saw the Dutch, the French along with Russians, Swedes and Portuguese making settlements in the continental U.S. (Beebe & Senkewicz, 2001). British colonization actually did not occur until the 17th century.

Like the United States, the examination of South Africa and Namibia will show that colonization by a number of European nations affected each of the case studies. From the original thirteen colonies that children are taught in school, in the colonial U.S. land was acquired as the people spread out over this seemingly endless new land. However, the indigenous peoples were being killed by new diseases, slavery, internment camps and wars with the newcomer (Faust, 1955). In the illustrated history of the Native American peoples, Alvin Josephy, shows how the great cities of the Native Americans were destroyed and changed forever with the coming of the settlers. His book is based on the documentary film *500 Nations* (Josephy, 1994). The tribes had their own laws and ways

of life. To this day on the reservations, certain crimes or offenses are handled by the tribal governments.

The French and the Spanish are civil law nations and as a result, the states of the U.S. that are former territories such as Louisiana still hold onto the civil law traditions. California “has a state civil code organized into sections that echo traditional Roman civil law categories pertaining to persons, things, and actions; yet the law contained within California’s code is mostly common law” (Robbins Religious and Civil Law Collection, n.d.).

The war for independence from Britain was fought in the late 18th century with the Declaration of Independence and later the Constitution of the United States being codified in 1787 and the Bill of Rights in 1791. The Bill of Rights contains the first ten amendments to the U.S. Constitution including the 4th and 5th Amendments which are heavily used in the forensics investigations and litigation in general (U.S. National Archives, 2013).

Each of the three case studies has the same basic structure – a judicial, legislative and executive branch. The judicial branch of the U.S. government is represented in all fifty states. The state courts deal with items such as divorce, probate, real estate, and criminal cases. Note that each state has its own hierarchy of courts ending in a State Supreme Court for appeals. Each state also has Federal courts which address items dealing with the constitution, bankruptcies and items such as treaties (United States Courts, 2012). There are ninety-four federal districts which are grouped into twelve Circuit Courts. Thus when one hears that a case is being heard in the Ninth or Second

Circuit Court, you can ascertain where the case may have been appealed. And finally there is the U.S. Supreme Court which has final say in matters of the U.S. Constitution. It is necessary to have at least a general understanding of this when reading about some of the case law that must be examined in common law nations.

As a result of having fifty states, one can see that having federal laws that all must abide by are a necessity. The United States has several rules, laws and statutes in place that directly deal with electronic or digital evidence at the federal level. Three are of primary interest to this research - the Federal Rules of Evidence (FRE), the Federal Rules of Civil Procedure (FRCP) and the Federal Rules of Criminal Procedure (FRCrP).

The FRCrPs were introduced in 1938 to provide “inexpensive” and “speedy” determination of matters (U.S. House of Representatives, 2010). Prior to this, procedures were conducted under formal proceedings and based on British Common Law along with others. The FRCP consists of 86 rules and updated biannually. In 2006, the FRCP was updated to include electronic evidence. That is the same year in which the U.S. ratified the treaty on the Convention on Cybercrime mentioned earlier in this Chapter. Digital evidence is affected by the following articles:

- FRCP Rule 16. Pretrial Conferences; Scheduling; Management
- FRCP Rule 26. Duty to Disclose; General Provisions Governing Discovery
- FRCP Rule 33. Interrogatories to Parties

- FRCP Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes
 - FRCP Rule 37. Failure to Make or to Cooperate in Discovery; Sanctions
- (U.S. House of Representatives, 2010)

The FRCrP address criminal law at the federal level. The U.S. House of Representatives initiated the FRCrP in 1944 and ratified them in 1946. One of the primary goals was to make criminal law more consistent from state to state. An objective of U.S. Federal laws is to standardize approaches to cases. Individual states have their own statutes; however, they can only be more stringent, not less than the federal law. Criminal law takes into account the rights of the accused. In the United States, this means paying attention to the Fourth Amendment which addresses unreasonable search and seizure. Rule 41 of the FRCrP specifically addresses search and seizure and how it can be obtained in a criminal case. The U.S. Department of Justice went on in 2002 to create the document *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (U.S. Department of Justice, 2009) which gives specific instructions for procedures both before, during and after acquisition of digital evidence.

Evidence must be presented in both criminal and civil cases, even though different rules apply. During the first half of the twentieth century courts wrangled with proper evidence and rules thereof. In 1957 a “proposal for uniform federal rules of evidence was referred to a judicial committee” (Federal Evidence Review, 2012). There was a standing

committee in the U.S. Supreme Court on Rules of Practice and Procedures with a Special Committee on Evidence during this time which was composed of members of the bar and academia. Their resolution was as follows:

1. Rules of evidence applied in the Federal courts should be improved; and
2. Rules of evidence, which would be uniform throughout the Federal court system, are both advisable and feasible.

(Federal Evidence Review, 2012).

The work began officially in 1965 to draft the rules of evidence. By 1973, the draft of the Federal Rules of Evidence had been forwarded to Congress. The Rules were placed before the President in 1973 after modifications had been made to the original verbiage. In 1975 the rules took effect as Public Law 93-595 *An Act to Establish Rules of Evidence for Certain Courts and Proceedings* (Federal Evidence Review, 2012). The FRE applies to evidence in both criminal and civil cases. This affects the current research in determining how evidence is handled. The FRE have not undergone extensive revisions due to electronic data. The interpretation and application of existing ones, however, has been updated. Eleven articles exist in the FRE with only certain ones specifically applicable to the digital arena.

- Article I, Rule 103. Rulings on Evidence
- Article I, Rule 105. Limited Admissibility
- Article I, Rule 106. Remainder of or Related Writings
or Recorded Statements

- Article IV. Relevancy and Its Limits—This article is certainly important, given the large amounts of digital information that must be sifted during e-discovery.
- Article VII. Opinions and Expert Testimony—This article directly affects the admissibility of digital evidence. The qualifications of the person extracting the evidence and presenting it in court affects the outcome of the hearing.
- Article VIII. Hearsay—This article is relevant to the admissibility of e-mail messages.
- Article X. Contents of Writings, Recordings, and Photographs—This article applies even in the digital world.

(The U.S. House of Representatives, 1975)

The Wiretap Act came into existence in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act (DHS/Office for Civil Rights and Civil Liberties, 2012). One of the more colorful cases that predate the Wiretap Act is that of *Olmstead v U.S.* which happened during the Prohibition in Seattle, Washington. Roy Olmstead ran a large bootlegging operation with the knowledge of some of the local law enforcement and business owners. Federal agents began wiretapping his phone in 1924 without a warrant (Federal Judicial Center, n.d.) The question of whether or not people had the right to privacy of their communications began to be heavily discussed.

Did callers have a right to privacy in their telephone conversations? Were telephone conversations similar to mailed letters, which were protected by the Fourth Amendment? (Federal Judicial Center, n.d.)

Roy Olmstead was convicted on the physical evidence, not the wiretaps. As will be seen later in the case of Namibia, with new technology this is often the case.

The Computer Fraud and Abuse Act (CFAA) was created in 1986 to update the Counterfeit Access Device and Abuse Act of 1984 which targeted fraud and similar criminal activities involving computers. Prior to the act, prosecutors had no specific laws to address computer abuse. Many hackers would claim that they only copied items, therefore nothing was stolen. The new law was instituted to address such nuances.

The CFAA was created as a criminal statute and is referenced as 18 U.S.C. § 1030 (read as "U.S. Code Title 18 Section 1030"). In 1996, it was amended, including changing the term "Federal interest computer" to "protected computer" (defined later in this section). As part of the National Information Infrastructure Protection Act of 1996, wording was added to the CFAA to cover extortion that threatens harm to a protected computer. Additional changes were made to the CFAA in 2001 and 2006 with the passage of the U.S. PATRIOT Act. A more recent amendment made as part of the Identity Theft Enforcement and Restitution Act of 2008 allows prosecution if the victim and perpetrator are in the same state (before this act, data had to cross state lines) and allows victims of identity theft to seek restitution (Phillips et al., 2014).

The CFAA addresses seven types of computer abuses:

- Accessing a computer or network without authorization or by exceeding authorization
- Accessing a computer or network to collect financial information, credit information, or other information from a government computer or any protected computer
- Making a computer or network unavailable for its intended use by a department of the U.S. government or another entity
- Transmitting programs, information, codes, or commands to intentionally cause harm or damage to networks or computers
- Accessing information on a computer or network to commit fraud or cause damage, whether intentionally or as a result of reckless actions
- Intentionally obtaining and trafficking in passwords
- Threatening harm to a computer or network for use in extortion or a similar practice (The U.S. House of Representatives, n.d.)

One fascinating criminal case in which the CFAA was applied (along with other laws) is described in the book *The Lure* (Schroeder, 2012). The book is about two Russian cybercriminals who hacked into companies, schools, and ISPs across the country. The FBI came up with a plan to catch them by setting up a fake start-up security company called Invita in Seattle. Schroeder, a retired DOJ Assistant States Attorney who prosecuted the case along with his colleagues, had to follow the law precisely to avoid a charge of entrapment. Therefore, the FBI filed a sealed complaint in Connecticut that

charged one of the hackers under U.S. Code Title 18, Section 1951, which deals with commerce and extortion threats, and Title 18, Section 1030 of the CFAA. In addition, Rule 15 of the Federal Rules for Criminal Procedure (FRCrP) was applied because it pertains to a detained witness's deposition (Phillips et al., 2014).

Later in this chapter it is shown that in South Africa, key events and cases triggered the creation of new laws. In the U.S., few corporate names evoke stronger feelings than the Enron Bankruptcy scandal. When most people hear the word "Enron," corporate greed comes to mind, but they aren't familiar with the case's facts. Before the scandal emerged in October 2001, Enron, with employees in 40 countries, was the largest seller of natural gas in the United States. After government deregulation was granted, Enron executives were allowed to "maintain agency" over the earnings reports sent to investors and employees (Laws.com, 2011). In other words, executives didn't have to report losses or their own financial statements, so they were able to present a profitable public image while pocketing the profits. Investors, however, lost more than \$70 billion. The company filed for Chapter 11 bankruptcy in December 2001 after a series of events, including investigation by the Securities and Exchange Commission (SEC) in November 2001.

Falsified earnings, hidden losses, and embezzlement caused the collapse of a powerful firm. In addition, the accounting and auditing firm Arthur Andersen was charged with obstruction of justice after destroying documents related to its audit of Enron (Kadlec, Weisskopf, & Zagorin, 2002).

The Sarbanes-Oxley Act was created in 2002 as a direct result of cases such as the Enron bankruptcy scandal along with the collapse of Arthur Andersen. Sarbanes-Oxley requires publicly held corporations to hold on to e-mail for five years and be able to turn over data, such as financial records, e-mail, and other documents, when requested by the courts. The Health Insurance Portability and Accountability Act (HIPAA), which was passed in 2001, protects a patient's medical history and specifies other privacy rights (U.S. Department of Health and Human Services, 2011). Before HIPAA, information such as a patient's prescriptions wasn't protected under doctor-patient privilege. Now patients must be notified when their medical records are shared with third parties. Medical records are gradually being required to be accessible online whether on a hospital mainframe or in the cloud, as a result, HIPAA takes on a more critical role (Phillips et al., 2014).

The Sedona Principles were created by a group of lawyers and professionals as guidelines for handling of electronic data and evidence. The fourteen principles link to the FRCP and are primarily for use in civil litigation but may hold clues for what is needed in criminal cases. In reading the Sedona Principles, the similarities between them and the articles of the Convention on Cybercrime can be drawn. Below is an excerpt from the working group regarding their objectives:

In Spring 2002, many of us who would later form the Sedona Conference Working Group on Electronic Document Production began discussing ways to develop 'best practices' for lawyers to follow in addressing

electronic document production. The collapse of Enron and Arthur Andersen, and the legislative response to these events, including the Sarbanes-Oxley Act of 2002, confirmed the importance of handling electronic document production in a defensible manner. Litigants, particularly entities that generated large volumes of electronic information, did not know what obligations might apply to the preservation and production of electronic data and files (Sedona Conference, 2007).

Multinational corporations, as mentioned earlier, have had to deal with the acquisition of digital data and ESI for many years. The Electronic Data Recovery Model (EDRM) is a model created by a group of the same name for civil cases (EDRM LLC, 2011a). The group is composed of companies such as AccessData and Guidance Software who are leaders in the field of computer forensics software. However, companies such as IBM and Lockheed Martin are also members to deal with corporate information. For most companies, winding up in a situation requiring e-discovery is inevitable, so having a method for producing electronic evidence is crucial. The EDRM serves as a roadmap for handling this task in civil cases, and it's widely used in the business and legal communities (Phillips et al., 2014).

The EDRM group created the Information Governance Reference Model (IGRM) to help companies address getting the information to legal counsel in an efficient manner (EDRM LLC, 2011b). Information governance and digital governance has appeared in

much of the reading . The EDRM has created a model that while some feel already exists, however, is being adopted by newer companies. The IGRM model reflects the common lack of communication and collaboration in dealing with information management, so it shows each group's effect on information management. The three main groups are business users; legal, regulatory, and risk-management departments; and IT support staff. The processes include value, duty, and asset. "Value" refers to the business purpose of the information, "duty" refers to the legal obligation to retain and store information, and "asset" refers to the information's actual container. Each group has skills needed to maintain or dispose of information: The regulatory group understands applicable laws or regulations, the IT group deals with security and storage, and the business group knows which documents contain which information. Clear communication between groups requires preserving data in a way that makes it easy to access and easy to send to a third party or legal counsel (Phillips et al., 2014).

The acquisition, analysis and reporting of digital evidence in the U.S. is covered in a variety of sources. Eoghan Casey's book, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, is referenced extensively by other authors (Casey, 2011). His definitions of items are relied upon by many. He covers device and network forensics along with child pornography, hackers, modus operandi, and the investigative process. His book contains cases of credit card fraud and others in which people were convicted. As a reference, it serves as a good touchstone for how things are defined in many countries.

The article entitled *Computer Forensics: The Need for Standardization and Certification* by Meyers and Rogers discusses the admissibility of electronic evidence, standards, analysis, chain of custody etc. that people are concerned about (Meyers & Rogers, 2004). While the article is dated, it lists several court cases of that time period that could still be relevant. The article looks at the impacts of Rule 41 and FRE 702. It helps with a perspective of the interpretation and application of the FRCP, FRCrP and the FRE. The article examines the criteria of Daubert which several other sources refer to as well. Meyers and Rogers also examine the "expert witness" qualifications which are of particular interest.

Next, in the book *Guide to Computer Forensics and Investigations*, Nelson, Phillips and Steuart define the basics of digital investigations, the law and processes (Nelson, Phillips, & Steuart, 2010). While it is written primarily from a U.S. centric perspective, the textbook is used both nationwide and internationally, including Australia and Namibia. The book lays the foundation for forensic procedure when dealing with digital evidence and covers the available certifications when referring to experts in the field. Like Eoghan Casey's book, this is one that has set standards for tools, processes and preparing testimony.

The evaluation of tools in the U.S. is done largely by the National Institute for Standards and Testing (NIST). NIST has created a guide for the testing of forensics tools. While the document applies to law enforcement, it helps in being "designed to provide a measure of assurance for the software tools used by law enforcement in computer

forensics investigations” (NIST, 2001). In a global context, if each country has a similar guide or standard it would make comparisons easier.

The U.S. is composed of fifty states which each has its own laws and procedures. Overly, a practicing attorney, has created a book that goes into great detail of the electronic evidence in California (Overly, 2004) which is one of the most populous states in the union and with the annual domestic product of some nations. The most revealing aspect of this book is that California goes to great detail in almost every aspect. One prime example is that of defining when a photographer taking pictures of children in the nude is art and when it is prosecutable. The book points out contrasts in laws where California is very fine tuned while states such as Washington simply add a statement onto the existing Revised Code of Washington (RCW) for trespass Correlating how many states have gone to such measures and the motivations behind them along with how this might play out in a global setting.

The U.S. CERT generated a document to give definitions, legal terms and a broad overview of what computer forensics is to managers of networks (U.S. CERT, 2008). The document looks at the law beginning with the Fourth and Fifth Amendments. Then it lists three others that are relevant to this study:

- Wiretap Act (18 U.S.C. 2510-22)
- Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
- Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)

U.S. CERT notes that any forensic examiner needs to be aware of these three items, because violation of these can result in federal charges against the investigator. The

document goes on to look at the rules of evidence. Four areas that it brings out need to be examined and compared in all three case studies: “hearsay, authenticity, reliability and best evidence” (U.S. CERT, 2008).

The texts by Casey and Nelson et al are listed as primary references for this document which shows commonality. A document by the U.S. Department of Justice created a document entitled “Forensic Examination of Digital Evidence: A Guide for Law Enforcement.” The authors of the document consider it to be the second in a series after "Electronic Crime Scene Investigation: A Guide for First Responders". The document appears to be a procedures manual of how to set up a department for digital evidence and how the polices need to be in place for them. Again the procedures set forth in the document show the consistency that exists, at least in the United States, for setting up and running a digital forensics lab and investigations. This is important when looking at the other two countries for standards in procedures and processes.

Training and Licensing of Experts. Throughout the research, the training and licensing of digital forensic examiners and experts is listed as a major obstacle. In their paper Bridging Differences in Digital Forensics for Law Enforcement and National Security Burd et al cite the National Academy of Sciences who in 2009 listed the following three items as a problem facing the field of digital forensics:

- The field has yet to agree upon the licensing or certification of digital forensic examiners
- Many states treat digital evidence as an investigation and not as a forensic procedure

- The qualifications vary widely on those who practice in the field

In their paper, Burd, Seazzu, & Jones (2011) mention the fact that in U.S. federal agencies, many practitioners know specialized tools and are only familiar with a particular type of technology. The situation on a global scale translates to vendor certifications and whether that is adequate. If the forensics examiner only understands the output of one product, the potential for misinterpretation or misapplication of facts/procedures exists.

As was mentioned in Chapter One, several states such as Texas, South Carolina and Michigan chose to require digital forensic examiners to be licensed as private investigators (PIs). Dave Kleiman in a presentation examines the opinion of the American Bar Association which resolved in 2008 for states to refrain from requiring those involved in digital forensic analysis, network intrusions or other network related investigations to be licensed as PIs (Kleiman, n.d.). The ABA goes on to support that while certification is needed, the private investigator route is not the correct path to take. Kleiman goes on to promote an idea that was funded by the National Institute of Justice to create the Digital Forensic Certification Board (DFCB) to promote “professionalism, trust, confidence in the digital forensics profession, and to provide professional certifications” (Kleiman, n.d.). The DFCB is now taking applications and may in the future help the profession.

In the paper *Computer Forensics Investigators or Private Investigators: Who is Investigating the Drive*, the authors delve deeper into some of the ramifications, both intentional and not when requiring digital forensic examiners to be licensed as PIs

(Phillips & Nance, 2010). The paper explores the definition and requirements of a digital forensics expert. The varying requirements in different states in the United States can directly affect whose testimony or work is admissible in court. For example, seven states have no requirements or provisions for becoming a private investigator. Others, such as Alaska only require a driver's license, that a person be of good character, post a bond and provide a criminal background check from each state of residency.

The state of California has the most stringent requirements for PIs which includes a background check by the FBI and a written exam. A primary concern that came from the paper is that there is no reciprocal agreement. If digital forensic investigators must have a PI license, what training is required of the PI in digital forensics? The answer is - none. This would mean that PIs with no digital forensic training could legally perform the investigation with no experience (Phillips & Nance, 2010). Crossing state lines becomes a serious issue as multijurisdictional cases become prevalent. If an investigator has to testify to something in another state, they must be licensed in that state. Or there has to be a national licensure. No such licensure exists for private investigators at the national level.

A situation arose for one company in Pennsylvania when they performed the analysis for a company in South Carolina. They were required to testify in court in South Carolina, but because they were not licensed as PIs (this is not required in Pennsylvania), to do so could result in their arrest and being fined. In Michigan, when their law went into effect in 2008, several ongoing investigations were shut down because the companies doing the investigations and analysis did not meet the statute. Michigan has since

modified their law to include persons with degrees and vendor certifications (Phillips & Nance, 2010).

Two cases in Texas put light on how interpretation of the laws can be taken to the extreme. In the first, Texas law implied that a computer repair technician would have to be licensed because they might be exposed to critical data when doing data recovery for a client. The second actually escalated to people wanting to file a class action suit. As in many states, Texas has video cameras at traffic lights that trigger when the light turns red. Many citizens have received tickets for illegally going through a red light. Because digital video has become a subset of digital forensics, the company issuing the tickets would have to be a licensed PI which they were not. This resulted in a conundrum.

Licensure and certification of digital forensics practitioners is needed, however, as previously stated, some laws that were invoked as stop gap measures have had unexpected consequences. The competency of the practitioner and credentials of some sort are needed to stand up in a court of law.

Gary Kessler goes into detail in his presentation on PI licensure, digital forensics and academia. He includes states that have no PI licensure, those that require digital forensics experts to have a PI license and those that do not. His presentation also looks at states that have no clear answer (Kessler, 2008). Kessler continues by examining the attempts to certify digital forensics examiners on their own. He compares the requirements of the International Association of Computer Investigative Specialists (IACIS), the Systems Administration, Networking and Security Institute (SANS), EC-Council and a host of others. He next sifts through the BS, AS and AAS degrees that are

being developed nationwide in the field. Kessler questions who vets their programs and asks the key question of whether or not a student upon completion is ready to start a practice (Kessler, 2008).

In addition to the forensic practitioners, what happens when the case actually gets to court? Kessler did his doctoral dissertation¹⁰ on the topic and in so doing, interviewed judges nationwide to come to several conclusions which had simply been assumed prior to his verifications. Kessler's paper was entitled *Judges' Awareness, Understanding, and Application of Digital Evidence* and was completed in 2010. Kessler goes into the awareness or lack thereof of judges dealing with digital evidence. He starts with the standard that most of the time the attorneys or paralegals deal with the information and many civil cases never make it to court. It is a qualitative assessment using grounded theory. Some of Kessler's conclusions were:

- There is an inverse correlation between age and familiarity with digital forensics, age and familiarity with ICT, and years served on the bench and familiarity with ICT.
- There is some confusion about clearly defining what digital evidence is as opposed to describing where digital evidence might come from.
- Respondents generally rated their knowledge of digital evidence and the computer forensics process at a level less

¹⁰ The results of an interview with Dr. Kessler is in Chapter Five

than they rated their knowledge of computer and Internet technology.

- One of the important roles of attorneys and expert witnesses is to inform and educate judges about digital technology and forensics.
- Most judges are satisfied with a technical witness who can demonstrate sufficient training and experience with digital forensics tools and processes rather than require the use of expert witnesses to offer opinions.
- Judges have the same issues with digital evidence as they do with physical evidence, namely, Constitutional issues of seizure and search, Rules of Evidence, relevance, and authenticity.

(Kessler, 2010)

Note that his conclusions are similar to ones already seen such as defining digital evidence. The inverse correlation of age and familiarity with digital forensics is not surprising. The primary items of interest are the importance of attorneys and expert witnesses to educate the judges. Also that the judges want a technical witness who can “demonstrate sufficient training and experience” in the field rather than someone who can offer opinions. As is shown later, this is the case in South Africa and Namibia as well.

The book *Managing Discovery of Electronic Information: A Pocket Guide for Judges* by Barbara Rothstein, Hedges, & Wiggins (2007) defines ESI along with other

laws when dealing with digital data in court. They cover what rules are applied, when and under what circumstances various things are needed by the Federal Judicial Center.

Judges use this text if they are hearing a case involving digital evidence. The impact this book has on the current study is in its illustration of what judges need to consider when dealing with ESI and that such a guide was needed. Coupled with Kessler's findings, the need for more guidance for the legal community is emerging.

In his conclusions, Kessler cites the importance of the rules of evidence. One of the foci of this research are the rules of evidence for the three case studies. Jonathan Frieden and Leigh Murray examine the admissibility of electronic evidence under the FRE under a paper by the same name. They focus on admissibility at trial and lack of information about what actually happens to the electronic evidence as it is being collected. While their paper is concerned more with electronic discovery than forensics, the cost factors are just as high if not higher (Frieden & Murray, 2011). They cite a key case *Lorraine v Markel American Insurance Company*. Judge Grimm gives a detailed explanation of what is expected of the admission of electronically stored information in court. He begins with relevance, authenticity, hearsay issues, and original documents. Judge Grimm also examines whether or not the information confuses the issue (Frieden & Murray, 2011). This is an item that is brought up again when comparing the laws of the countries, because a similar ruling happened in South Africa. Their article goes on to discuss logical relevance based on FRE 401 and 402. Next they examine pragmatic relevance which is under FRE 403 and targets "unfair prejudice".

Murray and Frieden bring up a fact that was also one of Kessler's conclusions that many judges are highly skeptical of electronic evidence on its base. Their discussion on authenticity using FRE 901(b)(8) which also applies to standard paper documents demonstrates how the addition of electronic evidence in 2006 under the FRCP, has not had a severe impact on the FRE. Their paper includes topics on computer generated files and hearsay in ESI. Therefore, it is logical to conclude that while some nuances exist, evidence is evidence whether electronic or not.

In the premise of this dissertation one question was "How can one deal with international jurisdictional issues if we are unable to address them adequately within the United States?" If the practitioners are running into obstacles regarding licensing or lack thereof, what challenges are the attorneys encountering? Stephen Giller describes in detail the UPL (unauthorized practice of law) in another state and what the implications would be. He discusses the implications of the Internet and the fact that many lawyers specialize now. The points he makes that are of interest to this research concern federal and international law which apply equally across the states. The arguments that an attorney is UPL even if they are physically in the state in which they are licensed and the client is in another state seems to apply primarily as to whether or not fees can be collected (Gillers, 2004). The Safe Harbor: Rule 5.5 of the ABA code of conduct that resulted may affect digital cases that cross state lines. The article is dated having been written in 2004. However, nothing indicating newer developments has been located. The caution is that the attorney should check the local laws and consult with an attorney licensed in that region or state. New York State added an enhancement to the Safe Harbor

Rule that would include foreign or non-U.S. licensed attorneys. It needs to be determined if South Africa and Namibia have any statutes that relate to foreign attorneys.

Legal collection of the evidence is a crucial factor. Orin Kerr in his article *Search Warrants in an Era of Digital Evidence* explores the limitations of the traditional search warrant when applied to digital media and data (Kerr, 2005). He wrote this in 2005, however, examining what changes have taken place since the updates in the 2006 amendments to the FRCP may prove fruitful. It would be good to compare the actual changes that have occurred as opposed to those left undone at this point in time. The article examines the traditional search and seizure process to what is needed in the digital world. That the data be admissible in court includes the legal right to the evidence gathering, this article is of interest. Kerr poses the challenge that in the case of digital evidence, it is a two-step procedure – the hardware is seized after a search is done of the premises and then the device is searched (Kerr, 2005). The relevance of his topic to this dissertation has to do with how effective are search warrants in the digital age. Is the investigator obligated to return the hardware within a certain period of time? Do they have to specify that they are only looking for files regarding money or emails on a particular topic? This certainly has been raised in several instances and has been challenged in court.

Michael Rustad et al wrote the book *Internet Law* which covers Internet law from the legal perspective (Rustad, 2009). It is written by law professors to take a serious look at how the interconnectivity of our world affects the way they have to view and interpret the law. The book starts with a foundation in basic network terminology and then moves

into cyber jurisdiction, e-commerce law, torts and cyber regulations. While the book goes into some topics that are out of the scope of this dissertation, it cites several relevant case law examples.

In the end, the concern of all the researchers is the acceptance of the testimony of the forensic expert in court. The case of *Frye v. United States* had long been used when examining the admissibility of expert testimony. The *Frye* case held that evidence had to meet the “general acceptance” standard to be admitted. In the case of *Daubert v. Merrell Dow Pharmaceuticals* the Supreme Court held that “the Federal Rules of Evidence, not *Frye* provide the standard for admitting expert scientific testimony in a federal trial” (Daubert v. Merrell Dow Pharmaceuticals, 1993). The court determined that the adoption of the FRE overruled the prior doctrine. FRE 702 specifically deals with expert testimony (The U.S. House of Representatives, 1975).

In the summary, the Supreme Court states that a judge must first look at the FRE 104 and determine if the “underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue” (Daubert v. Merrell Dow Pharmaceuticals, 1993). Once the judge has determined this, he or she is obligated to look at the methodology, not the conclusions per se. The following list contains the steps involved:

1. Determine if the methodology or technique has been tested
2. Has it been peer reviewed?
3. Is the error rate known?
4. Existence of maintenance standards

5. Is it accepted among the professionals of that scientific community?

(*Daubert v. Merrell Dow Pharmaceuticals*, 1993)

The *Daubert* standard has replaced the *Frye* doctrine at the federal level and most states at this point in time when dealing with the testimony of an expert witness. In a search of the Westlaw database, over 3900 entries cite the *Daubert* standard and it can be concluded that for the time being the *Daubert* standard is the one most referenced.

Another constitutional issue regarding privacy involves the 5th Amendment. In her blog, Susan Brenner explores the case of Sebastien Boucher who refused to provide the passwords to his laptop because of self-incrimination. This is a case that is similar to *U.S. v. Kirschner* where the defendant refused to give the password (Brenner, 2010). So if the defendant was compelled to give up that password and subsequently the case was tried in a foreign court, would the evidence be admissible? This article provides information on a case that has impacted the digital forensic community as to what can be required of a defendant in a criminal case.

Privacy issues are examined further by the Deputy Assistant Attorney General Jason Weinstein in his testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law. He is particularly concerned about the widespread use of smart phones and citizens reliance upon them. While much of the testimony is around transmissions and telecommunications, Mr. Weinstein raises the issue of when to apply the CFAA. He cites that the prosecutors must look at the “particulars of the case, the law of the applicable circuit, the severity of the conduct and the needs of justice” (Waters,

2011). Another issue is determining whether or not an incident should be pursued as a civil or criminal case. Weinstein's testimony goes on to stress the need of law enforcement to examine mobile devices and the relevance of the Electronic Communications Privacy Act (ECPA) in those investigations.

South African Related Literature

Rules, Statutes and Legal History. South Africa is a blend of laws as a direct result of having indigenous peoples and having been settled by various European nations. One of the premises of this investigation is that all three nations are common law. In many of the writings, the native tribes are referred to as the Bantu. Vasco da Gama and other explorers stumbled upon the South African coast in the 1480s. And similar to the Americas, the Dutch East India Company established a colony in Table Bay in the 1600s (BBC News, 2012). The British appeared in the late 1700s and the early 1800s saw the rise of Shaka Zulu. Wars between the British and the Zulus continued for almost 50 years. The infamous Boer Wars between the descendants of the original Dutch settlers (Afrikaners) and the British also took place during this time. In 1902 a treaty was signed and the Transvaal and the Orange Free State were "self-governing colonies of the British Empire".

1919 saw the annexation of South West Africa also known as Namibia as part by South Africa. In 1948, apartheid became the law of the land with the National Party took control. The events that ensued have been covered many times in world history books, the most important being the interim constitution in 1993 and the elections that occurred in 1994 in which Nelson Mandela became president and apartheid was abolished.

The history of South African law can be found on the South African Encyclopedia online which explores African tribal laws, the introduction of Roman-Dutch law and the overall influence of British common law. The formation of the Union of South Africa in 1910 saw parts of Roman-Dutch law discarded. One of the more significant items is in the recognition of the indigenous African laws and the human rights law (Myfundi.co.za, 2011). Wille's *Principles of South African Law* describes South African law as a “blended or hybrid” system. The three systems are the those of the indigenous tribes and varies by location; Roman-Dutch law which seems to influence contract law, personal law, torts and family law; and finally British common law which influences criminal and civil procedures, corporate law and rules of evidence.

The S.A. Criminal Procedures Act seems to deal with tariffs and travel allowances; it does have some tables that show the breakout according to tribes, etc. A map of South Africa and its provinces since independence is shown in Figure 2.



Figure 2 Republic of South Africa (citation in footnote)¹¹

¹¹ Retrieved on 19 August 2013 from <http://www.mapsopensource.com/south-africa-provinces-map.html>. Written permission from open source and free site.

The Constitution of the Republic of South Africa contains a Bill of Rights much like the United States. The Bill of Rights includes statements on equality, human dignity, the right to life and freedom from torture. The two that stand out in regards to this research are section 12(b) which states a person cannot to detained without a trial and section 14 which covers privacy (Republic of South Africa, 1999). Article 14(d) specifically refers to privacy of their communications which would presumably include email. The constitution also goes into the rights of arrested persons including the right to remain silent and the right to a fair trial.

The South African Government created the Criminal Procedures Act (CPA) 51 of 1977 which was amended in 2003 (South African Government, 2003). The amended document includes the International Co-operation in Criminal Matters Act 9 of 2000 which would be of interest in this research. It also contains information about search warrants and seizure of property. Chapter 16 discusses jurisdiction which plays a role in where cases may be tried or admissibility of foreign evidence. Chapter 24 covers evidence while Chapter 33 contains general provisions. There are actual cases are listed that may be of interest. Most, however, do not pertain to electronic evidence.

The Electronic Communications and Transactions (ECT) Act 25 of 2002 of South Africa goes into the admissibility of data messages, evidentiary weight and retention of same. It also goes into cryptography and other relevant items about electronic evidence. The ECT covers privacy, government statutes and other items that affect this research including the responsibilities of ISPs, cyber inspectors and looks at cybercrime in

Chapters XI, XII and XIII. A key point is that it defines the terminology that is used which is paramount to understanding how electronic evidence is viewed in S.A.

The paper entitled *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* by the South African Law Reform Commission in 2010 reviewed the laws of evidence as they pertained to digital data (South African Law Reform Commission, 2010). It examines specific case law that generated changes in South African law in the past, along with a comparison to the U.N. Model Law. Items such as how to define data messages, documents, are explored in great detail. It goes on to examine digital evidence in both civil and criminal proceedings while citing key cases for both. While the paper states that it is not to be viewed as the final decision of the commission, it gives great insight into how the laws are viewed in South Africa with respect to digital evidence.

Fawzia Cassim wrote the paper *Addressing the Challenges posed by Cybercrime: a South African Perspective* (Cassim, 2010). The author goes through the British-Dutch common law similar to this investigation. Then he points out the shortcomings of common law to digital crime and proceeds to look at the inadequacies in the ECT Act of 2002. Cassim also looks into how the Act may violate the right to privacy in the way the cyber inspectors go about their routine. He states that 1) very few cyber inspectors have been appointed and 2) they don't work well in practice. Cassim also cites recent case law that is relevant. An interesting point in his paper he states that South Africa has adopted the Council of Europe's Convention on Cybercrime ("COECC"), but has not ratified it. Cassim examines banking and privacy issues along with his view of the way forward. His

examination of jurisdiction cites the ECT which states a court of S.A. may try a case when

- a) Where the offence was committed in the Republic;
- b) Where part of the offence was committed in the Republic or the result of the offence had an effect in the Republic;
- c) Where the offence was committed by a South African citizen or a person with permanent residence in the Republic or a person carrying on business in the Republic;
- d) or the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight from the Republic at the time that the offence was committed. (Cassim, 2010)

So the question becomes, in the case of digital evidence, might South Africa assume one or more of these conditions exists and choose to claim jurisdiction. Steve Esselaar et al wrote the document *South African ICT Sector Performance Review 2009/2010: Towards Evidence-based ICT Policy and Regulation*. The paper examines the South African infrastructure including the undersea cables that provide the communications and Internet access for South Africa in particular and the African continent as a whole (Esselaar, Gillwald, Moyo, & Naidoo, 2010). The telecommunications industry in South Africa is changing as more satellite technology is added. This affects the availability of email and cell phone usage.

Narayan Gangalaramsamy's presentation on Cybersecurity in Africa goes into the challenges in the SADC region while addressing the infrastructure of Mauritius and surrounding territories (Gangalaramsamy, 2010). While Mauritius is a small island east of Madagascar, it shares the same telecommunications cable as South Africa (see Figure 2), gets it training in digital evidence from Botswana and is a member of the SADC region. So it is interesting to note how the countries influence each other.

Marthie Grobler examines the need for international standards in her paper *Digital Forensics Standards: International Progress*. She looks at ISO and the South African Bureau of Standards (Grobler, 2010). Grobler goes into jurisdictional issues and the challenges facing countries when information comes to them from other places. The paper lists the efforts that have been done to date to standardize digital forensics. Then she goes into her passion of digital forensics readiness. Overall, the paper gives insight into certain aspects of this research.

In the current digital era, at some point a large percentage of companies will have to deal with a digital forensics investigation or e-discovery. In the paper *Managing Digital Evidence – the Governance of Digital Forensics*, Grobler in conjunction with Dlamini examines digital governance (Grobler & Dlamini, 2010). In this paper Grobler lays out the framework for how a company should prepare for such an event. In dealing with multinational corporations, it will become more and more critical that each exercise digital governance in order to be ready for what appears to be inevitable.

Johann Hershensohn in 2005 wrote a brief paper entitled *I.T. Forensics: The Collection and Presentation of Digital Evidence*. The author sets out to look at the digital

framework in S.A. (Hershensohn, 2005). He explores the issue of digital evidence and hearsay which is an issue in S.A. or at least has been thus far. He cites several case law examples and explores their implication. One of the cases involves an employee emailing sensitive information to a company that has offered her a new position. The article is dated in laying out the definitions, however, at the time such guidance was sorely needed. He references Casey on digital forensic procedures. Hershensohn focused on five items: authorization, acquisition, authentication, analysis, and reporting. These are topics that are stressed continuously when dealing with digital evidence as we saw in Chapter One in the statement by Zatyko. He concludes by stating the South Africa has not had much chance to litigate such matters and look to the United States and the United Kingdom for cases involving such matters. This is an interesting statement that ties in nicely with the interview with the Honorable Justice Mainga in Chapter Five.

The report, *Evidence-Based Governance in the Electronic Age Case Study - Legal and Judicial Records and Information Systems in South Africa* goes heavily into the court system, bill of rights and other items pertinent to court cases in S.A. (International Records Management, 2002). The study was sponsored by the World Bank and while the focus in the report is on digital records management, it is a topic that will later affect cases as things become available on line. Even in 2002, the S.A. court system had a list of acceptable electronic document management systems (EDMS). One of the conclusions stated was that IT professionals did not regard the preservation of data as a “records management function” (International Records Management, 2002). This presents a problem that is addressed by the Electronic Discovery Reference Model (EDRM) in

showing how the various parts of organizations need and can work well together. The paper also explains the judicial system hierarchy which may help in determining where and how cases are heard. The Constitutional Court of South Africa deals with issues related to the constitution followed by the Supreme Court of Appeals and the High Courts. Because there are eleven national languages in S.A., the cases may be heard or presented in any of them legally which presents quite the challenge to interpreters.

Surya Prakash Joymungul's presentation *Digital Forensics –Challenges in Solving Cyber Crimes in African Countries* given at the Cyber Crime Summit in Johannesburg in 2008 gives a good overview of the various definitions that exist for cybercrime and their focus (Joymungul, 2008). For example, one slide explores three definitions. One focuses on the computer abuse, one on the technology such as digital evidence and the third on the criminal act. Surya also focuses on the challenges in the region. He brings out the fact that the SADC region has been trying to harmonize their laws and while the progress has been slow, it indicates that the countries in the region will agree upon the basics.

Several theses and dissertations cover topics that impact digital investigations in the region. Ngoman's thesis is entitled *The Use of Electronic Evidence in Forensic Investigation* was presented at the University of South Africa, Pretoria (Ngomane & Horne, 2010). This thesis looks at electronic evidence and its admissibility at trial. Ngoman stresses the implications of helping the judge to understand and what the investigator has to keep in mind as they present evidence. His results are similar to the challenges presented by Kessler in his dissertation on judges in the U.S.

Sandra Maat wrote her thesis entitled *Cyber Crime- A Comparative Law Analysis* in 2004. While her focus is on hacking, her review of South African, U.S. and EU law is relevant to this paper (Maat, 2009). She examines search and seizure, extradition, real vs. hearsay evidence and other topics. These topics are important in comparing the three case studies in this research.

Two senior lecturers at University of Cape Town (UCT) examine the need of forensics courses at universities and how cybercrime is affecting South Africa (Stander, Johnston, Town, & Africa, 2007). The lecturers -Stander and Johnston - propose an End-to-End Digital Investigation (EEDI) process that can be applied to digital investigations. It goes into the admissibility of electronic evidence in South Africa which is of particular interest in this research. The ECT Act of 2002 is mentioned and described (Stander et al., 2007).

Schatz challenges the current tool centric method of digital forensics and examines challenges such as synchronizing global time, evidence quality, reliability of the evidence and other issues (Schatz, 2007). His paper addresses a key issue being addressed in this research which is verifying the digital forensic practitioner.

Next Stork has an interesting presentation on how many people in SADC region have mobile phones but no bank accounts. His presentation was really pushing the need for easier access to open bank accounts and for mobile banking. This is of interest for fraud accounting and the electronic evidence that is from mobile devices (Stork, 2011).

The Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries created for Rand Europe focuses on the computer and network misuse laws in

the EU (Rathmell & Valeri, 2002). This report is of interest because both S.A. and Namibia look to the EU (a major source of business, revenue and trade) for their e-laws. It contains a summary of the laws that existed at the time of the report. It begins with some definitions. The most telling chapters go into the legal aspects of digital evidence and legal definitions. One chapter examines forensic principles and the admissibility of electronic evidence. The second half of the report goes into the origin of laws in each member country and the court system. It spells out in broad detail how the laws deal with computer abuse and network intrusion, not necessarily digital forensic law. The report lays a good foundation for international matters and multijurisdictional issues.

Murdoch Watney's paper *Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position* examines many of the same items that are addressed in the 2010 document on ECT (Watney, 2009). It includes definitions on whether digital evidence is considered hearsay, documentary or real evidence. The admissibility of electronic evidence compared to other types of evidence is discussed.

Namibian Related Literature

Rules, Statutes and Legal History. One of the assumptions in this study is that all three countries are common-law which allows for similarity in the ways laws are formed and administrated. To understand the origin of Namibian laws, one must understand the history. In examining the languages spoken by the people of Namibia, most learn their tribal tongue first, then Afrikaans and / or German, and finally English. The legal landscape is much the same. The laws of Namibia begin with the tribal and community

attainment of independence” (Legal Assistance Reform Centre, 2010). Tensions ran high and many Acts and exchanges of power occurred until Independence in 1990, when the Constitution of the Republic of Namibia became law. It would be an appropriate conclusion that Namibia is a merging of tribal, Roman-Dutch and common law derived from South Africa.

It was mentioned in the previous section South Africa has a Constitutional Court, the Supreme Court of Appeals and the High Courts. Namibia’s judicial system is similar with one exception – The Supreme Court “functions both as a court of last resort over disputes in all areas of the law as well as an equivalent of a constitutional court” (Supreme Court of Namibia, 2007). When examining where cases are heard, this fact becomes relevant.

NamLex – the Index to the Laws of Namibia was originally created in 1997, several years after independence. In it the authors specify why the term "South West Africa" is used to distinguish between terms used before and after independence (Legal Assistance Reform Centre, 2010). In addition to an explanation of the legal history of Namibia explored above, it also contains contract law and Criminal Law & Procedure which is of use to the research at hand. Finance law, international law and interpretation of laws are also listed. The document also lists statutes and relevant cases.

The Namibian Parliament created *The Computer Misuse and Cybercrime Act* in 2003, also known as Act 22. This document defines items from a Namibian perspective and can be compared to the U.S. laws such as the Computer Fraud and Abuse Act.

Namibia tends to follow after S.A., so a comparison of the corresponding S.A. act can demonstrate how much they track.

The next work examined was by Werner Kanita whose research was entitled the *Namibian ECT Bill & Computer Breaches* at the Polytechnic of Namibia for his Masters in Information Technology (Kanita, 2008). One of his supervisors is the Director of the Namibian National Forensic Science Institute. This mini thesis contains many of the issues addressed in this dissertation and comes from a Namibian standpoint. He also examined Namibian cases. "This mini-thesis examines the impact and effectiveness of the Namibian ECT Bill, which is still to be passed in the Namibian parliament. The Namibia ECT Bill in its current format, will it be effective in an attempt to combat cybercrimes and computer breaches" (Kanita, 2008) The author examines jurisdiction and what may be legal in one country is not in another.

Tana Pistorius gave a presentation entitled *Symposium Draft use of Electronic Transactions and Communications Bill for Namibia*. The author is from the University of South Africa (Pistorius, n.d.). She examines international best practices such as the UN Commission on International Trade Laws (UNCITRAL) Model Laws, the SADC Model Law on E-Transactions & Signatures; Australian Electronic Travel Authority (ETA), Canadian Uniform Electronic Commerce Act (UECA); U.S. Uniform Electronic Transactions Act (UETA), Mauritius and India along with their effects on Namibian ICT Policy. Her perspective is from the e-commerce impacts of the law. Specifically Pistorius examines:

- UNCITRAL Model Law on Contract Formation

- UNCITRAL Model Law on Electronic Signatures
- SADC Model Law on E-Transactions & Signatures
- U.N. Convention on the Use of Electronic Communications in International Contracts
- European Convention for the Protection of Individuals with reference to the Processing of Personal Information
- EU Directive on the Protection of Individuals with regard Processing of Personal Data & Free movement Data
- Council of Europe's Convention on Cybercrime (created in 2001, put into effect in 2004)
- Additional Protocol to the Cybercrime Convention

Some of these laws directly affect digital investigations and evidence handling; others do not affect such investigations, or have a work around in the S.A. or Namibian government rulings. Pistorius presents an excellent comparison table for the SADC region listing E-communications, cybercrime bills and data/privacy laws. The presentation is a good reminder of the vision of Namibia which is

To transform Namibia into a knowledge-based, highly competitive, industrialised and eco-friendly nation, with sustainable economic growth and high quality of life by 2030.

In continuing to explore the laws in the SADC region, the document *CESPAM Executive Training Programme: Combating Cybercrime in the SADC Region* is examined which summarizes a seminar held in 2007 (CESPAM, 2007). CESPAM stands for The

Centre of Specialisation in Public Administration and Management and actually resides in Botswana. The program was set up by SADC. This seminar was held to look at e-Government and Information and Communication Technology (ICT) in the SADC region. This was the tenth in the series. The document works very well by showing what laws are in place and what is needed. Session 2 of the seminar looked at legal issues while Session 3 focused on computer forensics and investigations. One presentation shows that balance is needed regarding universal privacy laws. Section four explores case studies which specify Namibia and gaps in their laws and procedures. These items are explored in Chapter Four when the case studies are compared.

Email Issues on the International and National Scenes

Privacy is of utmost concern to users of email in particular and the Internet in general. Since email is a transnational issue, the literature regarding it is presented here. Beginning with a 2011 ruling in which the Israeli National Labor Court established new principles in what employers could and could not do when monitoring employee emails. The Israeli National Labor Court overruled a Regional Labor Court regarding what an employer could or could not view in regards to an employee's email. This ruling increased employee email privacy rights (Mirchin, 2011). Mirchin's article brings out that even on the international scale, corporate email policies need to be well crafted to be enforceable.

From the international level to a national level - the U.S. Electronic Communications Privacy Act (ECPA) was created in 1986. The act addresses privacy online and specifically when data is in transit. The ECPA has been updated several times

since it was first passed. The item of interest in this investigation is Title II, namely the Stored Communications Act (SCA) which was enacted at the same time as the ECPA. This applies directly to email and what laws and statutes apply (U.S. Department of Justice, 2010).

As seen with the recent scandal regarding U.S. General Petraeus, changes have been recommended in the ECPA because of the advances in technology since the act was created in 1986. As the head of the Central Intelligence Agency (CIA) allegations or the potential for blackmail are certainly matters of national security. This allowed the Federal Bureau of Investigation (FBI) to obtain the emails without a warrant; only a subpoena from a federal prosecutor was needed (Ngak, 2012). What the search exposes are loopholes and gaps that also affect the emails of ordinary citizens who use services like Yahoo and Gmail.

In the case of Steven Warshak, he sued the U.S. government claiming that paragraph 2703(d) of the Stored Communications Act was unconstitutional and a violation of his Fourth Amendment rights (Steven Warshak v. United States of America., 2007). The salient point in the case that affects General Petraeus and the average citizen is that emails older than 180 days or approximately six months do not require a warrant. Emails less than that in age do, however, require a warrant (Steven Warshak v. United States of America, 2008). The laws were created when storage was costly and space was at a premium therefore most emails were deleted shortly after receipt (Ngak, 2012). Now with the newer technology, people retain email for years and possibly in the future, they can be retained for decades.

As a direct result of such issues, the members of the House of Representatives have proposed a new bill entitled the *Online Communications and Geolocation Protection Act* (OCGPA) which would serve as an amendment to the ECPA and severely restrict the tracking of citizens using the GPS locators in their cell phones or other mobile devices (Whittaker, 2013). It would mean that law enforcement authorities would be required to obtain a warrant for all electronic communications regardless of the age of the data as opposed to only being obliged to submit a subpoena now. The hearings for this bill are ongoing. The U.S. Department of Justice is challenging the limitations as it could severely hamper criminal investigations.

Whether addressing criminal or civil cases, email constitutes a significant portion of the data that may be presented in court. If an employee is using their company email address in correspondence, does the content belong to the employee or the employer? In the article written by Corey A. Ciocchetti in 2001, this topic was examined. His work entitled *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy* was published in the Duke Law Review (Ciocchetti, 2001). The article addresses one of the early considerations in the United States of the rights of employees pertaining to email that is housed on company servers. Ciocchetti explores the impact of the Electronic Communications Privacy Act and the item of consent. How far can a company go when an employee signs a consent form acknowledging that the email may be monitored? He brings out that the courts have used two methods to evaluate the regular course of business approach- content and context. The content approach allows the employer to monitor things related to the regular course of business, but not personal email. The

context approach determines if the company had a legitimate cause to monitor the email. The article ties in well with proper acquisition of data. What must be in place for employers to use the email records of an employee?

The Petraeus scandal which has cost the head of the Central Intelligence Agency (CIA) his job stresses two facts – 1) lack of privacy in regards to email and 2) the right of the government to access such information without a warrant in the interest of national security or similar concern. Online and email privacy in the United States continues to be an issue whether dealing with the corporate setting or personal.

The article *Silenced South Africa* from Privacy International goes into the privacy laws of S.A. and brings out how the 2002 law may affect the way ISPs save information about their customers (Privacy International, 2004). This may link back to the paper on the South African ICT infrastructure. Recall that the right to privacy is in the South African constitution so the impact may be different than what would be experienced in the United States. Many of the studies regarding South Africa address similar issues found in the U.S. concerning judges, practitioners and definitions.

Case Law

Common law nations use case law to codify items when they arise (Robbins Religious and Civil Law Collection, n.d.). Case law, as a result, is heavily relied upon to reach a decision when dealing with new technology and a changing legal landscape. In this section, the case law of each of the nation is examined. In this section, the focus is on case law for each nation in regards to specific items including search and seizure law, email privacy, the computer as a container and search of an arrested person.

U.S. Case Law

One of the questions put forth in Chapter One is that of pivotal cases in each country. For the United States, one such case that is referred to often is *Katz*. In 1967, Charles Katz was convicted of taking bets over the phone by wiretaps applied to a public pay phone. It was originally argued that since the device did not penetrate the walls of the telephone booth, it did not constitute “search and seizure” under the law (“*Charles Katz v. U.S.*,” 1967). The case of *Olmstead v. U.S.* determined that “eavesdropping” meant violating the physical space of a premises or structure. With the new devices, this was no longer the case.

So can one expect privacy of a conversation in a phone booth? The ruling from the court says that if conditions are met this is indeed the case. First the individual must demonstrate that they expected privacy. When one closes the door to a public phone booth, privacy is indicated. Secondly, “is the expectation one that society is prepared to recognize as reasonable” (*Charles Katz v. U.S.*, 1967). Electronic eavesdropping when the conditions are satisfied violates the expected privacy of a person in a phone booth and is a violation of the 4th Amendment. The *Katz* case overturned the ruling in the *Olmstead* case because both conditions were met. Both Namibian and South African law have items specific to the search of an arrested person in their constitutions. The United States has had that as an assumed principle. Several cases regarding this have arisen over the years to challenge the validity and scope of this assumption and regular practice.

In the case of *Chimel v. California*, the police had waited for the suspect at his home. They were in possession of a warrant for his arrest, but proceeded to search his

home in addition to his person. He charged that the evidence seized was in violation of his rights (FindLaw, 1969). The Supreme Court ruled on the findings stating that

An arresting officer may search the arrestee's person to discover and remove weapons and to seize evidence to prevent its concealment or destruction, and may search the area "within the immediate control" of the person arrested, meaning the area from which he might gain possession of a weapon or destructible evidence. (FindLaw, 1969)

Therefore, it is reasonable to search the physical person of a suspect to remove any weapons, cell phones, or other items that the person may attempt to destroy or dispose of in the interim. However, it is a 4th Amendment violation to search beyond that space which is what happened to Chimel. In a similar case, *U.S. v. Robinson*, the defendant was pulled over for traffic violation, was physically patted down upon which the officer found a "crumpled cigarette package" which held heroin (U.S. Department of Justice, 2009). The Supreme Court ruled this was permissible.

Another case involving a man arrested for driving with a suspended license. He was handcuffed and placed in the back of a police car. The police then proceeded to search his car; finding drugs and a handgun. Rodney Gant, the arrestee, asked that the evidence against for drug possession and the firearm be thrown out. Both the Arizona courts and the U.S. Supreme Court upheld his request because the search was not warranted because 1) he was arrested for a traffic violation and 2) he was not near the

vehicle to destroy evidence or obtain a weapon to use against them (Legal Information Institute, 2009).

In her article entitled *Redefining Searches Incident to Arrest: Gant's effect on Chimel*, Jackie Starbuck explores long standing premise that the arresting officer has the right to search a person as demonstrated in *Weeks v. U.S. (1914)* (Starbuck, 2012). The questions that arise include: 1) do you search the passenger compartment of a vehicle and all contents; 2) can you only search the room in which the person was arrested in or the entire premises? Various courts have interpreted these differently until the cases of *Chimel* and *Gant* (Starbuck, 2012).

An impounded vehicle presents a different challenge in regards to the Fourth Amendment. It is standard procedure to inventory the contents of an impounded vehicle to protect the property of the arrestee and to shield the police from a lawsuit (USLegal.com, 2001). Any items found during such inventory can be considered under the plain view doctrine as evidence.

There have been a large number of cases which both expand and limit the scope of such inventory searches. In the case of *People v. Farquharson*, the results of a secondary inventory search were suppressed because it was done with the intent to find more drugs. It was ruled that since a standard policy regarding how and when inventory searches are to be carried out, the drugs found after the initial marijuana buds were not allowed as evidence (New York Criminal Law and Procedure, 2009).

In 1990, the U.S. Supreme Court heard the case of *Florida v. Wells*. In this case the defendant was pulled over after driving recklessly. The officer smelled alcohol and

arrested him. Wells gave them permission to open his trunk wherein they found some marijuana butts and a suitcase. The item of interest here is the suitcase. Upon opening it during an inventory search, the officers found it was contained a substantial amount of marijuana. Wells tried to have the marijuana suppressed as evidence under the Fourth Amendment. In the evaluation of the case, the Supreme Court, the trial court cited “that *Colorado v. Bertine*, 479 U.S. 367, requires police to mandate either that all containers be opened during such searches, or that no containers be opened”. Since the Highway Patrol did not have a policy regarding the opening of closed containers, the State Supreme Court determined the search was improper.¹³ The U.S. Supreme Court states in their ruling that the case of *Colorado v. Bertine* does not allow law enforcement any possibility of critical thinking when dealing with individual cases. However, they affirmed that the marijuana be suppressed.

In a five to four vote, the U.S. Supreme Court ruled in April of 2012 that any person arrested for any offense can be strip searched before being put in a secure facility. Albert Florence took his case to the highest court after being strip searched twice for a minor item. The ruling was viewed with surprise because several states have statutes against strip searches. The reasoning, however, “people detained for minor offenses can turn out to be the most devious and dangerous criminals” – a key case for that being upheld is the U.S. domestic terrorist Timothy McVeigh (Liptak, 2012). While the ruling does not make it mandatory to perform such invasive searches, it has been determined that a strip search does not violate the Fourth Amendment rights of an arrested person.

¹³ The issue of closed containers and inventory searches are covered in detail in Chapter Three under U.S. Case Law

A key case in the overstepping of a warrant is in the Bay Area Lab Cooperative (Balco) case in which the named company was suspected of supplying illicit drugs to major league baseball players. The government investigators were initially looking into the alleged use of said drugs by 10 players. During the examination, they discovered evidence for almost two hundred more players. The agents applied the plain view doctrine. The court, however, ruled that the plain view does not apply in the case of electronic evidence. The search warrant must be specific in what is being searched for and if the agents cannot abide by said restrictions, a third party known as a special master must be brought in (Vijayan, 2009).

The need for search warrants in the U.S. when dealing with electronic evidence is explained in the document created by the U.S. Department of Justice entitled “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.” In regards to the Fourth Amendment and computers, the document states that law enforcement would be prevented “from accessing and viewing information stored in a computer if it would be prohibited from opening a closed container and examining its contents in the same situation” (U.S. Department of Justice, 2009). This applies to cell phones as well. In the case of *U.S. v. Reyes* in New York 1996, it was determined that there was reasonable expectation of privacy of data stored on an electronic pager. The courts differ in the interpretation and context of these rulings. For example, in the case of *United States v. Gorshkov* the defendant did not have an expectation of privacy when he was not the owner of the computer, knew his activities could be monitored and had someone looking over his shoulder (Internet Law Treatise, 2010).

The case of *United States v. Walser* in the Tenth Circuit gave grounds for concern, especially as more people are “plugged in” as shown below in their statement

[b]ecause computers can hold so much information touching on many different areas of a person’s life, there is greater potential for the ‘intermingling’ of documents and a consequent invasion of privacy when police execute a search for evidence on a computer. (U.S. Department of Justice, 2009)

The guidelines in the DOJ document go on to explain that the person relinquishes their right to privacy when they give the information to a third party including, surprisingly enough, a repair shop. This comes under the guise of “private searches” in which a party who is not an agent of law enforcement conducts a search whether on a computer or premises and reports it to law enforcement. The restrictions on law enforcement in many jurisdictions in the U.S. is that a warrantless search may not exceed what was done by the private search (U.S. Department of Justice, 2009). A recent case which has yet to be decided involves the FBI and Google. Google refused to give the FBI “an alleged pimp’s cellphone” which uses Android the ability to crack the password. This refusal came even after the FBI produced a warrant (Angwin, 2012). As a third party, it is unclear if their refusal falls under the Supreme Court ruling on Third Party Doctrine or not.

Continuing the discussion on warrantless searches, the Foreign Intelligence Surveillance Act (FISA) Amendment of 2008 was just voted upon in Congress in

September of 2012 and was extended five additional years. This has resulted in the NSA having the ability to perform warrantless wiretaps on anyone doing foreign correspondence without their knowledge. The ACLU brought charges in 2011 and the Second Circuit Court of Appeals ruled they had grounds to challenge the constitutionality of the law (Gross, 2012). When the House of Representatives voted to extend FISA, the ACLU filed charges again (Kravets, 2012). On October 29, 2012, the U.S. Supreme Court heard the arguments from the ACLU of how this violates the privacy of American citizens who are not even aware they are under surveillance. The continued use of such warrantless searches will be ruled upon by mid-December. The ruling will play a significant role as to when the government can use a warrantless search in matters of national security.

In a case that is sure to give police officers pause before they take action is a recent one in July of 2012 in which the police were mistreating a citizen. Another gentleman nearby, Earl Staley Jr., took out his cell phone and recorded the incident. The police confiscated his phone which is a violation of his First and Fourth Amendment rights. The phone was returned minus the memory card. The ACLU filed charges against the D.C. police on Staley's behalf (ACLU, 2012). Unlawful search and seizure of a witness and potentially the freedom of the press is of grave concern.

Part of the premise in this research is that cases result in new laws. One of the foundation cases that resulted in the Sarbanes-Oxley Act in the United States was the Enron Bankruptcy. The case spanned criminal, civil and bankruptcy law. Other cases that

contributed were WorldCom and Tyco International. The Gramm-Leach-Bliley Act was also the result of such corporate greed.

The Zubulake (*Zubulake v. UBS Warburg LLC*) case is a key case in e-discovery for cost shifting. In many instances one party will claim it is cost prohibitive to produce electronic evidence. This case caused the formation of new laws in the U.S. regarding who should pay for retrieval of evidence in a civil case.

The recent decision by the New Zealand High Court in the case of *MegaUpload* may have interesting outcomes. The FBI was investigating MegaUpload for violating copyright law by allowing people to store and transmit bootlegged copies of digital information. The New Zealand police gave ghost copies of the hard drives to the FBI after conducting a raid of the owner's home. The High Court ruled that the seizure was unconstitutional and in addition, the drive images should never have left the country (Jones, 2012). The High Court has asked the return of the drive images by the FBI. The question becomes is the FBI bound by ruling that if they received the evidence in good faith from a legal source, namely the New Zealand police?

South Africa and the United States have several pivotal laws that have resulted from case law. In the analysis phase of this dissertation, the types of cases that caused changes are examined and compared.

Case Law in South Africa and Namibia

In examination of South African and Namibian case law, let us begin with the case of *S v Mashiyi and Another 2002* which questions if computer generated documents can be used in a criminal case. In this case, some documents had been scanned – which

were admissible under the law at the time – and others were generated by the Medscheme program which processes medical payments. The court reasoned that the case of *Narlis v South African Bank of Athens 1976* it was ruled that computer generated documents were inadmissible which caused considerable concern in the banking industry since monthly statements are computer generated. The Computer Evidence Act of 1983 was a direct result of the Narlis proceedings. The judge had to consider section 221 of the Criminal Procedure Act of 1977 which states that a document includes “any device by which information is recorded or stored” (*S v. Mashiyi And Another 2002, 2002*). Because at this period of time, the perspective was that the computer created the documents and was not a person, the evidence was inadmissible. Therefore those documents were not allowed.

The case of *S v. Koralev and Another 2006*, which was in the Natal Province of South Africa, deals with child pornography. This case brings up concerns such as verifying the birth dates and ages of the individuals in the pictures. The pictures were discovered by a repair technician. Warrants were obtained to search the homes after the fact. The defendants were convicted under various acts including the Sexual Offences Act 23 D of 1957 and of the Criminal Procedure Act 51 of 1977. On appeal, the defendants counsel argued that these were “not original images since ... they had been either downloaded from Internet or transferred from digital camera - Original images would be those contained in camera or in original source from which they had been loaded onto Internet site” (*S v. Koralev and Another 2006, 2006*). While many other items were considered in this case including the failure of the repair technician to testify, the item of

the accuracy and authenticity of the digital evidence resulted in the cases being dismissed.

The case of *S v. Mdlongwa* involves the admissibility of bank security cameras. The incident involved a case of aggravated robbery and resulted in a twenty year prison sentence. The appeal challenged the bank footage which was rejected because it could be proven that this had not been tampered with and qualified as real evidence. Challenge of a witness and then of the expert involved were also part of the appeal. This is of interest because the expert did not have “academic qualifications” but had over thirty years on the police force with eighteen of those being on facial recognition. The ruling from the Supreme Court of Appeal was that the defendant was challenging the officer’s academic standings and not the quality of her work. This is quite significant when looking at how to qualify digital forensics experts.

There were several sources of evidence in this case including eye witnesses. The court made this statement which will certainly apply to digital evidence: “A court does not look at the evidence implicating the accused in isolation in order to determine whether there is proof beyond reasonable doubt, and so too does it not look at the exculpatory evidence in isolation to determine whether it is reasonably possible that it might be true” (*S v Mdlongwa* 2010, 2010). The original ruling was upheld.

The rights of the accused stand out in the case of *S v Mphala and Another* in which the accused was not informed they had counsel waiting and a confession was coerced in direct violation of the Bill of Rights. The conduct of the officer to fail to inform them that a family member had hired counsel for them and had instructed them

not to say anything taints all evidence found. Their right to a fair trial had been impinged upon. The admissions were dismissed.

A case which involves hearsay and computer generated documents is *S v Ndiki and Others*. This case was heard in 2006 with the defendants charged with fraud and theft. The definition of documents was still under heavy debate. The term *trial within a trial* is used here as in others discussed above because the State introduced computer generated documents and it had to be determined what category of documents they would be ascribed to (*S v. Ndiki And Others* 2008, 2008). The defense claimed that because the incident occurred prior to the ECT of 2002, it could not be applied. However, part of the argument did address retrospectivity and whether or not it should apply. The other relevant acts were the Civil Proceedings Act of 1977, the Law of Evidence and the Criminal Procedures Act. After much discussion, the exhibits were conditionally admitted into evidence but would have to hold up under closer scrutiny.

The case of *S v. Teek* is an excellent example of the close linkages between the Namibian and South African systems. This is an appeal of case of abduction and rape of minors in the Namibian Supreme Court. Throughout the case document, references are made to South African courts. Specifically “the common-law crime of kidnapping has acquired a dualistic character in both South African and Namibian law... known as child-stealing” (*S v. Teek*, 2009). In this case, the acquittal was reversed.

When examining the law of search and seizure in Namibia, one interesting case is that of David Swartz against a police officer and the police force. It was heard in the High Court in late 2011. The complainant put forth that the search of his home by the Drug

Law Enforcement Group was illegal as it was done without a warrant and demanded return of his goods which included vehicles, a significant amount of cash (over N\$47,000.00), furniture and smart phones. The respondents claim they had the right to search and seize the items under sections 20 and 22 of the Criminal Procedures Act (Swartz v. Indongo and Others, 2012). Mr Swartz was charged with drug dealing and money laundering. The respondents made their case linking him to a known cocaine trafficker in Swakopmund.

In the case of a warrantless search, an officer may proceed if he believes one would be granted and time does not permit him or her to wait. Mr Swartz made the claim that they should have applied section 51 of the Prevention of Organized Crime Act (POCA) against him instead. The ruling made was that the search was legal and because of the luxury items seized where the complainant could not prove how he could afford same, they were the results of the money laundering and need not be returned. A few of the items were deemed to be returned after the investigation. Note that in the Namibian constitution, a citizen can seek restitution for illegal search and seizure in a monetary amount.

Several members of the Namibian legal profession were interviewed in person. Of interest to all of them is the case of Jacob “Kobi” Alexander who was the CEO of Converse Technologies. In 2006 he was charged with conspiracy, money laundering and securities fraud to the tune of US\$138 million (Goeiman, 2012). After transferring large sums of money estimated at US\$40 million out of the United States, Kobi went on holiday to his native Israel and failed to return. He instead took his family and chose to

settle in Namibia. When the U.S. requested extradition, the country was not in the Namibian Extradition Act of 1995. Kobi has fought extradition for the last six years. In the first case he claimed a phrase in the Namibian Extradition Act was unconstitutional – and won. “The Windhoek High Court ruled that the Extradition Act in its present form may result in foreigners and Namibians being held in custody for years until their cases are disposed of by the Namibian legal system” (Goeiman, 2012). Meantime, Kobi is engendering himself with the Namibian people by proclaiming to set up scholarship funds and making donations. In this way he was able to prove he was not a flight risk. This case brings a high focus to the rights of individuals under the Namibian constitution. And to find a case between two of the countries being examined is significant. In August of 2006, President Hifikepunye Pohamba signed Proclamation 10 which amended the Extradition Act to include the United States. Kobi was arrested a few days later. His attorneys, in April of 2012, charged that the Proclamation is unconstitutional because it is directed against an individual, namely Kobi Alexander. The case is being referred to the Namibian Supreme Court.

Another extradition case in Namibia involves a man from Lebanon married to a Namibian woman. In the early part of 2012, the French authorities tracked him to Katutura and filed an extradition request in regards to a 1991 rape charge. He was arrested and bail denied in this case (Menges, 2012). Of interest in this case is that he was convicted in absentia. Namibia would require that the conviction be set aside so that he can have a new trial before he is extradited. It will prove fruitful to compare all three countries policies in such matters.

Extradition Law

In examining the Kobi Alexander case, it became evident that in dealing with digital evidence from other countries or jurisdictions, sooner or later someone will need to be extradited to the jurisdiction in which the trial is being held. Beginning with the U.S. this section looks at the relevant laws and treaties that currently exist. The United States has treaties to deal with extraditions and the list is contained under the FRCrP. At the time of this writing, the U.S. had treaties with over one hundred nations. There are several countries with whom diplomatic relations exist but no treaty. “However, some countries grant extradition without a treaty. However, every such country requires an offer of reciprocity when extradition is accorded in the absence of a treaty” (U.S. Code, Title 18, 2006). It is therefore logical to assume that some degree of negotiation may be needed when dealing with countries in the absence of an extradition treaty.

South Africa has treaties for extradition and mutual legal assistance in criminal matters in effect or in the process of being ratified with over twenty nations. They also are part of the SADC Protocols on Extradition and Mutual Legal Assistance in Criminal Matters (Department of Justice - Republic of South Africa, 2011).

Namibia has the Extradition Act which was signed into law in 1996. There must be a valid request for someone who either is at large after being convicted of a crime elsewhere or who is wanted in connection with an offense. There are specific conditions set out for return of the person such as not for political reasons or for military inscription. The two standards are that a treaty be in place or by proclamation of the President (Office of the Prime Minister, 1996). When considering the Kobi Alexander case, the

Proclamation 10 declaring the United States as a nation Namibia would extradite to, that portion is perfectly legal. It will, however, be of interest if it is ruled unconstitutional because of the motivation of the creation of Proclamation 10.

Literature Related to Qualitative Analysis, Case Studies, and Grounded Theory

Qualitative research is a scientific research method that poses a question, uses a set of procedures to find the answer, collects evidence and produces a conclusion that was not predetermined (Family Health International, 2005). Qualitative methods examine the human side of the equation and may identify intangible factors. Three methods were listed – focus groups, in-depth interviews and participant observation. The research involved in this dissertation involves guided conversations with experts from each country in different fields.

Qualitative analysis differs from quantitative in a few key areas. First and foremost is the flexibility. A qualitative analysis seeks to explore an issue whereas a quantitative analysis seeks to prove a hypothesis. Qualitative studies seek to describe the variations in the data using open ended questions to gather the information. This allows the researcher to adjust the questions based on the response of the interviewee. The data format is textual vs. numerical.

A key difference between quantitative and qualitative is that the data gathering is iterative in qualitative. The questions are adjusted as more research is gathered. Also, typically the relationship is less formal between the researcher and the interviewee. The researcher, however, must be willing to probe the answers and find the “why” things are a

certain way. The interviewee may also be surprised by the answers. The benefits of the open ended questions are that the answers are:

- Meaningful and culturally salient to the participant
- Unanticipated by the researcher
- Rich and explanatory in nature (Family Health International, 2005)

Professional ethics are important as well. The three categories of ethics given are respect, beneficence and justice. The interviewee should know the purpose of the research and should give informed consent to the use of their name, etc. in the paper.

Dapzury Valenzuela and Pallavi Shrivastava describe using the interview technique in a qualitative analysis (Valenzuela & Shrivastava, n.d.). They list the free flowing conversational interview and the general interview guide approach. In this research, there is a guide so that each respondent addresses the same or similar question about their country and field of expertise. The researcher appreciates their points on the interviewer can slant the questions and bias the results. It is critical to remain open and objective about the answers and the course of the interview process. In their presentation, Valenzuela and Shrivastava describe the qualifications of the interviewer, how to prepare for the interview, the topics and sequence of questions, and finally the stages of the interview. They also describe what to do after the interview.

The next style of research is the case study. The approach to this was intriguing because it requires going back and doing more research as the case progresses. The guide describes a good case study as a mystery novel. The researcher has to lead the reader

through the case in the same or similar discovery path that they themselves took in uncovering the information for analysis. One objective is to challenge the reader and keep them intrigued throughout the case, much a mystery novelist would do. The paper shows three phases – research, analysis and writing with the caution that more research may be required (Guidelines, n.d.). The actual steps given are:

1. Research
 - a. Library and Internet research
 - b. Interview people
2. Analysis
 - a. Put the information together and cull
 - b. Formulate the case problem in a few sentences
3. Writing
 - a. Describe the case or problem the reader needs to solve
 - b. Organize the sections that have to be addressed
 - c. Give a conclusion

In her description of qualitative studies in a dissertation, Eva Mason stresses that a qualitative study is neither non-skilled nor non-systematic in approach. And she adds that it can generate a hypothesis which for this study would be a welcome conclusion based on the comparative study (Mason, 2009).

The third research method used in this dissertation is grounded theory. The methodology came from Straus and Glaser in the 1960s. The objective is to generate new theory from data which is quite similar to generating a hypothesis at the end of a case

study . Grounded theory tends to come from qualitative data. Straus and Glaser's paper goes into coding which is more suited for studying entire populations, but is not required when doing qualitative analysis. On the other hand, the link to creating a new theory is applicable to this investigation (Birks & Mills, 2010).

Grounded theory requires one to approach the data with the objective of finding a theory rather than proving a theory. The question becomes "what's really going on, and how" along with the fact that in grounded theory "everything related to the subject of the study is data" (Hamilton, 2011). By constantly comparing the data as it is collected allows one to begin to form a new hypothesis. Hamilton goes on to list questions that need to be addressed in regards to fit, relevance, workability and modifiability as shown below:

- Fit
 - Do the concepts fit with what's been described (i.e., incidents) by participants?
- Relevance
 - Does the study address something of concern to the people affected by a given phenomenon?
- Workability
 - Does the theory explain how a phenomenon is being addressed/solved/managed?
- Modifiability

- Can the theory be modified upon introduction of new data?

(Hamilton, 2011)

When examining “fit”, this study compares the literature collected to the opinions voiced by the experts in Chapter Five. The “relevance” of the study emerges with the data that is collected. The need to understand the acceptance or lack thereof of digital evidence in various situations and in light of the laws that currently exist or are being proposed is examined in each case study. The workability of the theory formed will be to show how things are managed and addressed in each case study. Finally the modifiability of the theory is examined in Chapter Six with the challenges that can be expected as more countries are added or examined using the theory and the database template being introduced.

This dissertation is a blended method that involves case studies, grounded theory and qualitative analysis. As stated, grounded theory uses qualitative methods and case studies to produce hypotheses. The figure below illustrates how the information flows. While the study begins with an examination of international law, the actual case studies are the three nations chosen as shown in Figure 4. As the data is gathered, it is constantly sorted and compared with commonalities in one area and variances in another. These feed into the resulting grounded theory. A step that is not shown in the figure are the interviews. These have been employed in this research to address the fit, relevance and workability of the grounded theory being proposed.

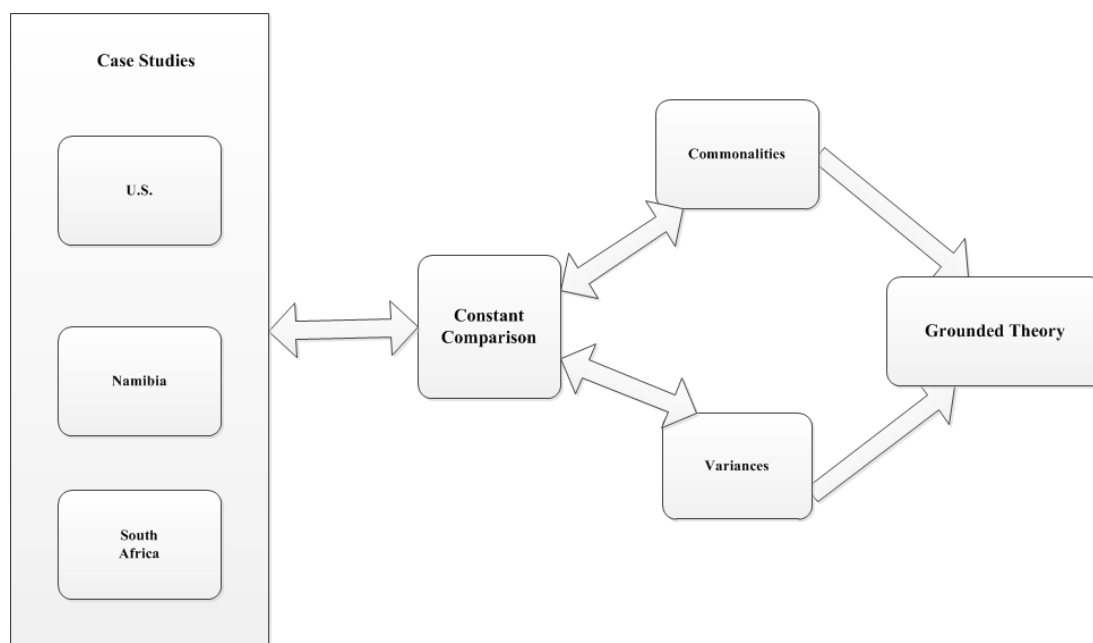


Figure 4 - Use of Case Studies with Grounded Theory

Summary

In examining the international laws, it can be concluded that several items have been put forth such as those by the IOCE. Many fall short of extensive guidelines in handling and the use of digital evidence. The Convention on Cybercrime requires each nation to create its own laws; however, it was noted that local or domestic laws fall short of dealing with international issues. The variation in privacy laws is apparent when examining the three cases. This is an item that needs to be compared carefully.

The fact that each study concerns a nation that is primarily or at least a hybrid of common law is significant in examining the cases that each has heard in regards to what applies when persons are convicted or set free. The International Competition Network appears to have the best compilation of data for digital investigations processes and search and seizure methods; however, they do not release which nation does what.

The table shown below is a part of the database that has been created as part of this analysis. As common law countries, each appears to have laws that address similar issues in one form or another. In the interviews, the focus is placed on the commonalities and variances found while seeking the relevance to each interviewee.

Table 1 - Comparison of the Laws of the Three Countries

	Rules of Evidence	Rules of Civil Procedure	Rules of Criminal Procedure	Privacy Laws	Computer Abuse
United States	FRE	FRCP	FRCrP	ECPA - limited in scope	CFAA
South Africa	Law of Evidence Amendment Act 45 of 1988	Civil Proceedings Evidence Act 25 of 1965	Criminal Procedures Act 51	in constitution	ECT Act 25 of 2002
Namibia	Law of Evidence Amendment Act 45 of 1988	Civil Proceedings Evidence Act 25 of 1965	Criminal Procedures Act 25	in constitution	Computer Misuse and Cybercrime Act

As a combination of qualitative, grounded theory and case studies, this research brings out several additional items that need to be compiled not only for the countries in the case studies but for other common law nations to facilitate cooperation between nations when dealing with digital evidence both in civil and criminal matters.

CHAPTER THREE – COMPARISON OF CASE LAW

The use of qualitative theory implies that one must continuously go back and refine the information and the questions as more data is gathered. In this chapter, the case law of the three countries is examined in depth. One of the assumptions of this discourse is that the case law helped to drive changes in the laws of each country.

U.S. Case law

As mentioned earlier, the *Daubert* standard has been used in a variety of cases both for and against expert witnesses. In the case of *U.S. v. Sharron Grinnage* the defendant appealed a decision regarding DNA evidence in the death of his wife. He alleged that a pretrial *Daubert* hearing should have taken place because of the new methodology that was used addressing sparse evidence. The court upheld the charges showing that the method had been accepted by other courts.

Another plaintiff, Donn Olson, sued his attorney for failure to get the settlement Donn felt had been verbally agreed upon. He then got two more attorneys and attempted to block expert witnesses using the *Daubert* standard. Mr. Olson failed to produce the needed documentation and his case failed (*Donn Olson v. Michael Reynolds*, 2012).

Applying the *Daubert* standard to ESI cases seems straightforward. Has the method been tested? The software and hardware tools for digital forensics have been tested by groups such as NIST and is a standard for most practitioners to verify that new versions of software perform as the previous (Nelson et al., 2010). Is there a standard for

error and is it accepted among a group of professionals? Yes, would be the answer to both of these questions.

The *Olmstead* case dealt with eavesdropping and was later overturned by *Katz*. What is “eavesdropping” – does it only apply to physical structures and is physical intrusion the only violation of the 4th Amendment? The issue is one of definitions and new technology. The use of digital eavesdropping devices does violate the 4th Amendment because if it encroaches on a person’s expectation of privacy in communications (*Charles Katz v. U.S.*, 1967). The Supreme Court ruled in favor of *Katz* because both conditions were met.

The use of Global Positioning Systems (GPS) devices illustrates another case of new technology and definitions. The use of GPS devices to track suspects has become common. Two seminal cases regarding tracking devices are *United States v. Knotts* and *United States v. Karo*. In the case of *United States v. Knotts*, a tracking device was placed in the chloroform containers¹⁴ purchased by the defendant. The case was appealed to the U.S. Supreme Court as a violation of the 4th Amendment. However, since the tracking device only augmented what officers could observe following a vehicle on the street, no expectation of privacy could be upheld and therefore the conviction was held (*United States v. Knotts*, 1983). The case of *United States v. Karo* is similar in that law enforcement planted a tracking device in a container of ether. The portion of the case that violated the 4th Amendment was when the tracking device was used once the container

¹⁴ Note that chloroform is one ingredient used to produce illegal methamphetamines.

entered private property. Inside the house, an expectation of privacy was reasonable (United States v. Karo, 1984). And at that point, a warrant was required and was used.

GPS tracking and privacy play a key part in when a warrant is needed. In the case of *U.S. v. Antoine Jones*, it was determined that the GPS data would not be admissible because while the agents had obtained a warrant they failed to attach it within the ten day time limit. The search of the vehicle was upheld because no expectation of privacy exists when parked on city streets. The key items in this case are the attachment of a GPS device “constitutes a search” under the 4th Amendment and “the *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test” under the 4th Amendment (*U.S. v. Jones*, 2011).

Privacy rights continue with the search of an arrested person and their surroundings. In Chapter Two, the precedent was introduced that an officer can search an arrested person and their immediate surroundings. Exactly what is meant by these terms? In the *Gant* case, his car was searched when he had already been handcuffed and placed in a police vehicle. The products of the search were later thrown out by the Supreme Court (Starbuck, 2012). Two related cases are *Chimel* and *Robinson* which were discussed in Chapter Two as well. The police had a warrant for Chimel’s arrest but proceeded to search his home after being told “no” by his wife. This was a 4th Amendment violation of “search incident to arrest” (FindLaw, 1969). The court ruled that anything within the “immediate control” of the suspect could be searched. In the case of *Robinson*, the police did a physical pat down which revealed a packet with heroin on his person. The Supreme Court upheld this search as reasonable.

If a person is in possession of a cell phone or other mobile device, does that immediately mean the officer can also search the contents of the phone such as contacts, text messages, etc.? To thoroughly explore this, two issues must be considered: 1) inventory searches and 2) closed containers. Search incident to arrest means that the officers can search anything that the suspect or arrestee can access or is in his or her immediate control. In the case of *Illinois v. Lafayette*, the shoulder bag was searched and inventoried. Drugs were found in the bag and further charges were filed. Upon appeal, it was ruled that “it is proper for police to remove and list or inventory” items that are in the possession of an arrested person about to be jailed (*Illinois v. Lafayette*, 1983).

The case of *South Dakota v. Opperman* also addresses inventory searches – in this case that of an impounded vehicle. The case of *People v. Farquharson* introduced in Chapter Two demonstrates that there is a right and a wrong way to apply the reasonableness of an inventory search. In the case of *Farquharson*, the search was done with the intent to find drugs. In the case of *Opperman*, his car had been impounded for being illegally parked. To minimize claims against the city, the police followed established policies and inventoried the contents. Finding marijuana, the police arrested Opperman when he came to claim his vehicle. The U.S. Supreme Court ruled that the inventory search was reasonable (*South Dakota v. Opperman*, 1976).

The second item in regards to mobile devices is that of closed containers. A historical case is that of *California v. Acevedo* in which police had probable cause to pull the defendant over and search a specific container they believed to contain marijuana.

When appealed, the warrantless search was upheld because of exigent circumstances – in this case, that the evidence would be compromised (*California v. Acevedo*, 1991).

In dealing with the search of mobile devices which contain, in this day and age, very personal information about a person, careful consideration must be given. Based on the cases presented search incident to arrest is reasonable. And many people will have their cell phones or mobile devices on their person or in their possession. It would therefore be reasonable to take it and list it as part of the inventory. The next question becomes, is it reasonable to search the contents of said device? Two State Supreme Courts have ruled on this matter. The State Supreme Court of Ohio ruled in 2009 that police are obligated to obtain a warrant to search the data on a cell phone “when the search is not necessary to protect the safety of law enforcement officers and there are no exigent circumstances” (Supreme Court of Ohio, 2009). In 2012, the Oregon Supreme Court made a similar ruling stating that in the case of *Schlossberg v. Solesbee* that “warrantless searches of such devices are not reasonable incident to a valid arrest absent a showing that the search was necessary to prevent the destruction of evidence, to ensure officer safety, or that other exigent circumstances exist” (Brown, 2012).

Figure 5 illustrates the decision structure that should be followed based upon the cases shown. It assumes that a cell phone or mobile device was seized incident to arrest. The next decision is whether or not the contents can be searched without a warrant. As quoted from the Oregon Supreme Court, one of three conditions must be met. First – is the officer in danger? If the cell phone is a bomb trigger this most likely applies to the physical device itself not the data on the phone. Secondly, is there evidence that can be

destroyed? If the suspect still had the device in their immediate possession, that would be true, but if it has already been seized, this is not likely. Exigent circumstances such as tracking down a kidnap victim or similar certainly applies. Also if it were suspected that a remote wipe of the device could occur, it would be prudent to take a forensic image of the drive and then obtain a warrant. Mobile devices and which laws to apply will become more and more prevalent with the advancement of technology.

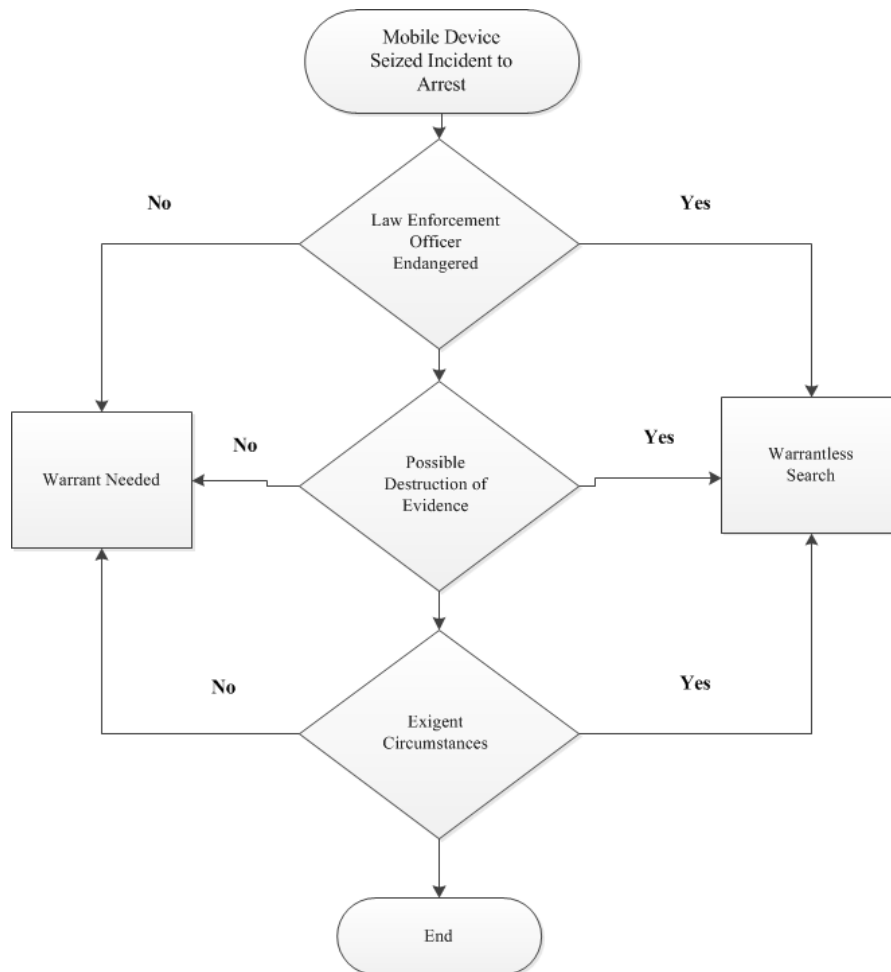


Figure 5 - Mobile Device Warrant Decision Flow

From mobile devices, the next area of case law is civil. Digital evidence has been used in court for several decades now in the United States. As mentioned in the literature

search, a pivotal case in the U.S. was the Enron scandal. Deregulation had allowed the executives to produce misleading financial reports which later resulted in the bankruptcy of the company and the loss of millions of dollars to both investors and employees. The resulting law of Sarbanes-Oxley affects the storage of financial documents and transparency of same (Garrie, Armstrong, Adler, Burdett, & Routt, 2002).

Another case that involved criminal fraud was WorldCom. In 2002, WorldCom which was the world's second largest telecommunications company at the time filed for Chapter 11 bankruptcy. It was the largest in U.S. history in the amount of \$107 billion (Romero & Atlas, 2002). The WorldCom CEO was involved in securities fraud, including millions of dollars of personal loans to himself and friends, so the investigation focused on how corporate assets were handled, among other issues.

The case of *Zubulake v. UBS Warburg LLC* resulted in new standards for cost-shifting. In civil e-discovery, the company being sued will claim undue burden to retrieve the files or email or other e-evidence. The Zubulake case, which was heard prior to the 2006 FRCP amendments, was concerned with gender discrimination (Laura Zubulake v UBS Warburg LLC, UBS Warburg, and UBS AG, 2004). Ms. Zubulake filed an EEOC case and produced more than 400 pages of e-mail evidence to prove she hadn't been promoted because of her gender, and the company retaliated against her by firing her two weeks after she filed the case under Title VII (New York State Human Rights Law). The company failed to save some electronic evidence, such as e-mail, on backup tapes. Ms. Zubulake asked that UBS be required to carry the cost burden of the discovery process, but UBS claimed the cost was excessive. In the end, UBS was found at fault for failing to

retain the backup tapes and they had to bear 75% of the cost of discovery which totaled almost \$300,000. The ruling was groundbreaking in creating requirements for retention that would later become law. Another case that caused the court system to take a closer look at the cost burden was *Rowe Entertainment v. The William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. 2002) and developed a test consisting of the following seven factors to determine cost shifting:

- The extent to which a request is tailored to discover relevant information
- The availability of information from other sources
- The total cost of production, compared with the amount in controversy
- The total cost of production, compared with the resources available to each party
- Each party's ability and incentive to control costs
- The importance of issues at stake in the litigation
- The benefits to both parties of obtaining the information

(Garrie et al., 2002)

The Zubulake case is an excellent example of how case law can lead to actual laws being created to deal with changes not only in technology but the unexpected consequences that develop (Phillips et al., 2014)

In addressing the rights of individuals not to incriminate themselves, two cases have appeared in the U.S. courts and have not been completely resolved. The first is in *U.S. v. Kirschner*, 2010 WL 1257355 (2010). In this case, the defendant was being

charged with possession of child pornography and had been served with a subpoena to supply the passwords to his computer. He filed to have the subpoena quashed under the 5th Amendment. Because this case had several facets, the judge involved had to separate out items namely whether the subpoena was “being utilized post-indictment to investigate additional charges” (Brenner, 2010). The arguments focused on the fact that if Kirschner did testify before the grand jury and gave his password, the prosecution would be unable to use any evidence found as a result of said testimony.

A similar case regarding the rights of the accused concerns Sebastien Boucher. Mr. Boucher was crossing the U.S. – Canadian border with the laptop in plain sight which was viewed by the border agent. Mr. Boucher volunteered that sometimes child pornography sites would put things on his computer, but he would try to delete them immediately. He was Mirandized, but waived his rights. The case becomes more complicated at that point because the computer was shut down and put into evidence. The investigators later found an encrypted area on the drive. They demanded the password to which his response was giving of same would violate his 5th Amendment rights and he cited the Kirschner case. The case first was ruled in his favor, however, the ruling was later reversed because he had already freely given the government access to the computer (Hughes, 2009). Boucher was able to reach an agreement with the prosecutor and gave the names of others involved in the many child pornography files that were found on his drive.

The Boucher case was significantly different from the Kirshner case because the defendant had already waived his rights and had even discussed the items with the border

agent. However, the two cases go to further the issue that case law has its drawbacks especially when there are reversals.

In an appeal of the case of *U.S. v. John Doe* filed in Florida in 2012 (the original case was heard in 2011) the circuit judge Martin Tjoflat reviewed the case. The final question came down to whether or not the production of the password by the defendant was in fact testimonial. In this case, Doe had a laptop and five external hard drives which were encrypted. The Attorney General asked that Doe be granted immunity for the act of the production of the unencrypted drives, but not for the derivative use of the decrypted drives (*U.S. v. John Doe*, 2012). John Doe refused to testify and was found in contempt. His reasoning was that decrypting the files would imply that he had actually placed said files on the machines.

The appeal found that the district court had erred in its claim that the decryption and production of the files was not testimonial. It had also erred in trying to limit the immunity. The court of appeals goes on to describe former cases, namely *Fischer v U.S.* and *U.S. v Hubbell*. In former case the court knew the existence of the documents and that the defendant had possession of same which had been corroborated by others; while in the latter, the court did not know and production of same constituted testimony. The doctrine of “foregone conclusion” only applies to cases in which the government knows of the existence and the device on which the files are located. Therefore the defendant’s rights were upheld.

The case of *Donato APONTE-NAVEDO, et al., Plaintiffs v. NALCO CHEMICAL COMPANY, et al* involves employees at a plant in Puerto Rico suing Nalco Chemical on

the grounds of discrimination under the Americans with Disabilities Act (ADA), age discrimination and Title VII. The plaintiffs were charged with being overbroad in their requests for personnel files and not “complying with meet and confer requirements” (Donato Aponte Navedo v. Nalco Chemical Company, 2010). The FRCP played heavily in this case, particularly Section 34(b)(2)(C). The case continued with discovery requests being unfilled, challenged or declared too broad. In the end, monetary damages regarding failure to deliver were not imposed on the defendants because it was determined that neither party was at fault.

The issues presented in the cases thus far include civil, criminal fraud, child pornography, and self-incrimination. Many have been appealed to higher courts for the final decision. One type of case not addressed is criminal e-discovery. In early February of 2012, the U.S. DOJ’s Joint Electronic Technology Working Group produced a 21 page document giving guidance on criminal e-discovery (U.S. DOJ’s Joint Electronic Technology Working Group, 2012). Criminal e-discovery currently constitutes a small percentage of e-discovery. As a result, the commercially available software and training focus on the civil cases. Andrew Goldsmith, national criminal e-discovery coordinator states “[Electronically stored information] was going to threaten to swallow prosecutors and defenders alike, and the judiciary for that matter” (Koblentz, 2012). While this is not a specific case, the workload in the judiciary system has prompted the DOJ to create procedures along with a checklist. Criminal e-discovery is typically only applied in four situations:

- when information may clear a defendant,

- when a statement is easily disproved,
- when a witness' prior statement needs to be explored, or
- when investigations fall under Criminal Rule 16 which addresses the government's obligation to disclose information to be used at trial

An infamous case in which the suspect was given ten consecutive life sentences (Coates, 2005) involved the Bind, Torture, Kill (BTK) killer in which the suspect taunted the authorities for years. Authorities were able to lay a trap when a discarded box was located linked to the suspect. In one of the documents found in the box he asked if sending in a floppy disk would be traceable to him. If he could do so without fear of discovery, he asked them to post an ad that stated "Rex, it will be OK." The authorities posted the ad and the suspect mailed the disk to the Fox News station in Wichita, Kansas (Hansen, 2006). The investigators were able to determine who had written the files and traced it back to Dennis Rader. Because the floppy disk was voluntarily mailed and not encrypted, it was a straightforward case for the prosecution for murders that had spanned decades.

The case *Einstein and Boyd v 357 LLC and the Corcoran Group, et al* upheld the obligation of a company to retain electronic evidence such as emails when a discovery hold is in place. This pivotal New York state case delivered sanctions on the defendant when it was proven they had purposefully misled prosecutors and the plaintiff as to the existence of emails. The requirements and obligations for companies in litigation are very well spelled out at the federal and state levels.

South African Case Law

South Africa in 2010 finished the review of their ECT Act of 2002. Many of the pivotal cases are included in this document. The earliest case was *Narlis v South Africa Bank of Athens* in 1976. At the time this case came to trial, the definition of a document was that it was produced by a person. However, bank statements are generated by a computer and therefore were inadmissible in court. This resulted in the Computer Evidence Act 57 of 1983 which allowed computer generated evidence be admissible but only in civil cases. There were however, stipulations such as:

authenticated computer-print-out [was] admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible. “Authenticated” required the printout being accompanied by an authenticated affidavit and other supplementary affidavits necessary to establish the reliability of the information contained in the printout. (South African Law Reform Commission, 2010)

This became an issue, because the judge could choose to use as little or as much of the evidence at his or her discretion. Poor and conflicting case law was a direct result of such discretion. In the case *Ex parte Rosche* the court ruled that the computer printouts documenting call records of specific phone numbers were real evidence and free from “human error or dishonesty” (South African Law Reform Commission, 2010). This was a deviation from Act 57 and the reasoning was that the software that produced the bills had

been used for several years and generally accepted. Also the carbon copies from the hotel operator demonstrated the same evidence.

ECT Act 57 introduced other challenges as well, not the least being, that it was not applicable in criminal cases. The rule was overturned with the ECT Act 25 of 2002 which defines data messages and their acceptability in a court of law when performed in the normal course of business.

The Criminal Procedures Act (CPA) 51 of 1977 presented challenges when contemplating the definition of the term “document.” In criminal proceedings, section 221 requires that computer printouts or devices be of business records and section 226 that they be of banking records. The latter also requires an affidavit that the evidence is authentic and has been in the custody of the bank.

The challenge came in the form of *S v Harper* when the term “document” was interpreted to mean store and record information. No calculations or adjustments or other activities were admissible or so it seemed from a dictum by Milne J. Later courts would note that Milne J had been misinterpreted (South African Law Reform Commission, 2010). As a result, the documents were admitted in *Harper* case.

In the case of *S v De Villiers 1993 (Nm)* the interpretation of CPA 25 of 1977 was questioned again. The computer printouts were deemed authentic, duplicates of the originals and admissible in court. The interpretation of section 221 was deemed that since no rebuttal to the information was made, the evidence stood as is. Note that during this period all computer evidence had to be presented as hard copies, not digital files. In the case of *S v Mashiyi and another*, the opposite ruling occurred when interpreting Milne J’s

dictum. Because the records were sorted, calculations made, and more than simply recording and storing of information, the computer printouts were deemed inadmissible (South African Law Reform Commission, 2010).

Such contradictions in case law begged the creation of the ECT Act 25 of 2002. The Act drew heavily from the UNCITRAL (U.N. Commission on International Trade Law) Model Law on e-commerce known simply as the U.N. Model Law. Then adjustments were made to apply to criminal law as well. The South African Law Reform Commission looked at the definitions of electronic and digital evidence specifically when it came to the differences between analog and digital data. They compared Eoghan Casey's definition which focuses on criminal investigations to Stephen Mason's definition which encompasses civil and criminal. Casey appears to focus on the definition of "device", while Mason focuses on "electronic evidence." The Act chose to conform more to the Model Law by using the terms "data" and "data message" which includes analog messages stored on a digital device.

Since the passage of ECT 25 of 2002, digital evidence has been interpreted in South Africa as "real computer evidence" and "hearsay computer evidence". In the case of *Ndiovu v. Minister of Correctional Services* it was ruled that the contents of a data message still depend upon the reliability of the person sending the message and therefore the normal rules that apply to hearsay stand. In the case of *S v Ndiki and others 2008*, the judge ruled that ECT Act 25 of 2002 was "inclusionary as opposed to exclusionary" (South African Law Reform Commission, 2010). The data message would be accepted as real evidence, however the court would determine the weight to give the contents.

While the ECT Act 25 solved many issues, there were still more to be addressed. In Chapter Two, the case of *S v Koralev and Another 2006* dealt with child pornography being on the accused's computer. His attorney presented the argument that the pictures were not the original items since they had to either be downloaded from the Internet or copied from a camera. The ruling in this case which questioned the authenticity and accuracy of the digital evidence went in favor of the accused. Possession of the child pornography was not enough to convict because it could not be proven that they had taken or put the images on the computer. Other evidence was needed to make the charges hold.

Bank security cameras were called into question in the case of *S v Mdlongwa*. The accuracy and veracity of the bank cameras could be verified and shown that the evidence had not been tampered with. Note that this case occurred in 2010 which points to where concerns still exist regarding digital evidence. In Chapter Two it was also presented that the expert witness was challenged because of her lack of academic credentials. The judge accepted her testimony, however, based on her experience in the field. He also made a statement that evidence had to be examined in its totality, not accepted or rejected on its face.

The rights of the accused are especially important as seen in the case of *S v Mphala and Another* when the two suspects were not informed their family had hired counsel for them. The conclusion that can be drawn is that South African case law is evolving in regards to addressing digital evidence and that the legal system takes existing law and cases into account when trying to rule on items that have not been addressed before.

Namibian Case Law

As a former protectorate of South Africa, Namibian case law overlaps with that of South Africa. While the case of *S v De Villiers 1993 (1) SACR 574 (Nm)* was listed in the S.A. Law Reform report; it took place in the Namibian court. This may account for why, in the literature search, no cases were easily found in reference to digital evidence or electronic data used in Namibian courts. The conversation with the Namibian Supreme Court Justice expands upon this and offers explanations as to the reasons why in the analysis in Chapter 5. The case of *S v Teek* illustrates the close linkages between the two legal systems when the ruling refers to the dualistic nature of the kidnapping of children being classified as child stealing.

The Namibian Computer Misuse and Cybercrime Act came into effect in 2003. It includes unauthorized access to data, denial of service and other relevant items. As in many developing nations, Namibian companies were realizing the advantages of the Internet and e-commerce. At the time, however, most companies who did business online utilized servers in countries such as Germany because of the low bandwidth available in Namibia.

In 2004, an E-Laws Working Group was formed. The group was comprised of “the Law Reform and Development Commission, the Namibian Communications Commission, the Law Society of Namibia and academia. In particular, a successful interactive workshop¹⁵ was held in Windhoek in May 2005 which was attended by many stakeholders” (Office of the Prime Minister, 2010b). The resulting document and

¹⁵ Amelia Phillips was a member of academia who participated in the workshop

recommendations were used in the creation of Electronic Communications and Transactions Bill. The government notice found in the literature search refers to it as the Electronic Transactions and Communications Act which was put before the Parliament.

Warrantless searches are allowed in all three countries under specific conditions. The case of *David Swartz v the Namibian Police* bears out that in Namibia, if an officer ascertains that a warrant will probably be issued and the evidence may be destroyed in the interim, he or she can search without a warrant.

Summary

The case laws between the nations have some similarities. There are, however, some significant differences which directly correlate to the perspective of the country involved. The Case Law table which is described in detail in Appendix A was developed as a result of comparing the legal rulings from each of the case studies. The treatment of new technology and how data from same could be used emerged. Definitions of terms changed as a result of the new technology. The table below presents the items that had to either be defined or redefined as cases went to court. These items led to the creation of the Common Search Criteria table of the database. It also lends itself to consistency in the phrases used.

Table 2 - Development of Common Search Criteria

Common Search Criteria	U.S.	South Africa	Namibia
Definition of “eavesdropping”	x		
Corporate transparency	x		
Criminal fraud in a corporate setting	x		
Cost shifting	x		
Search and seizure in regards to electronic devices	x	x	x

Table 2 Development of Common Search Criteria (continued)

Common Search Criteria	U.S.	South Africa	Namibia
Self-incrimination	x	x	x
Search of an arrested person	x	x	x
Inventory search limitations	x	x	x
New procedures for criminal e-discovery	x		
Significant sanctions for misleading, lying, non-retention of ESI when a discovery order has been issued	x		
Definitions of terms such as “document”, “data”, and “data message”		x	x
Criminal case definitions of terms listed above		x	x
“real computer evidence” vs. “hearsay computer evidence”	x	x	x
Warrantless searches	x	x	x

In addition to the items included in the table, it was noted the close ties between Namibian and South African case law. As will be seen in Chapter Five, because Namibia is a former protectorate, the case law prior to independence (1990) is the same.

CHAPTER FOUR - HYPOTHESES AND COMPARISONS

In grounded theory, the objective is to derive theory from the data examined. Hamilton states that “everything related to the subject of study is data” (Hamilton, 2011). The sections of this chapter examine the information gathered. First examined are the commonalities in the nations studied while the following section looks at the variances. From these, the hypotheses can be derived.

The original questions asked in this investigation involved the acceptability of digital evidence collected in one country in a foreign court; and the qualifications needed for forensic investigators and how those qualifications are recognized in another or foreign jurisdiction. To accomplish this task, the laws, statutes and cases of each country are investigated and compared.

In order to ascertain where problems might be found, variances between the countries and their laws need to be pinpointed. By comparing each set of laws, one can eliminate the items that have little or no variance and focus on the items in which the variance is high. The variances will show practitioners where to focus their efforts when dealing with such cases.

As shown in their prototype in Chapter One for comparison of the legal statutes, Nance and Ryan listed several areas of study including constitutional law, cybercrime, criminal procedure, tort law, and evidence law (Nance & Ryan, 2011). By focusing on these items, hypotheses were formed.

After examination of the data gathered in Chapter Two and comparison of case law in Chapter Three, several things in regards to common law nations take shape. The

first portion of this chapter examines the areas the case studies have in common and those in which there are significant differences. The chapter ends by putting forth additional hypotheses.

1. Areas in which there are commonalities
 - a. Common law countries take similar approaches
 - b. There are similarities in the civil laws
 - c. There are similarities in the criminal laws
 - d. There are similarities in the evidence laws
 - i. Hearsay rules
 - e. Pivotal cases exist in each country which drive the laws
 - f. There are similar cases in each country demonstrating that countries are dealing with the same or similar issues
2. Areas in which there are significant variances
 - a. There are significant differences in privacy laws
 - b. Despite much cooperation in criminal cases, courts are dissimilar in the sanctions applied or penalties, specifically
 - i. Cooperation in web defacement is not prevalent
 - ii. International cooperation in regards to financial hacking is very fine tuned
3. Issues between individual states in the U.S. may be similar to differences in approaches across the countries.

4. The requirements for the digital forensic examiner will vary, but may currently rely upon the vendors on an international scale.
5. International cooperation exists, but does not address all the issues.

Examination of Commonalities

Each of the three nations being examined is a blend of laws. The United States, South Africa and Namibia each have their own indigenous populations and were former colonies of various European nations including the Dutch, the British, the Spanish and the Germans. At the federal level, the U.S. is a common law nation, however, various states such as Louisiana have adopted the civil law of the colonizers (Robbins Religious and Civil Law Collection, n.d.). As shown in Chapter Two, both South Africa and Namibia have legal systems that consist of the tribal laws, Roman-Dutch Law and British Common Law.

Each country has a Bill of Rights and their peoples have constitutional rights whether built in or implied. The idea to keep in mind when comparing the laws is that the U.S. Constitution was put into place long before modern technology was even imagined. Both South Africa and Namibia wrote their constitutions with the issues of modern day life firmly in mind. Specifically, privacy and the search of an arrested person are in their constitutions. In the U.S. these items are covered by other acts or case law.

The first commonality exists between the civil laws. In examining the Federal Rules of Civil Procedure (FRCP) in the United States and the rules at the state levels, one encounters varying degrees of consistency. A compilation of the state rules of civil procedure was found in *Electronic Discovery Law and Practice*. The database that

accompanies this dissertation puts this information in a more readily accessible format to allow comparisons of the various rules. As shown in Chapter 2, the FRCP rules pertain to pretrial conferences, duty to disclose, interrogatories, production of documents including ESI, and failure to cooperate in discovery along with sanctions.

The FRCP was updated in 2006 and while many states updated their civil procedures, many did not. Over half of the states have not updated their rules of civil procedure since the 2006 amendments to the FRCP. Of the states that have made adjustments to their civil procedures, several are worth mentioning. Connecticut requires a showing of good cause if ESI is to be used. Illinois acknowledges ESI, but requires that it be printed to be admissible in court. The states of Louisiana and Minnesota have the same requirements as the revised FRCP, however, the meet and confer is optional. In Massachusetts, their civil procedures were updated in 2008, but it was felt they did not fully address e-discovery. Mississippi's laws actually predate the 2006 FRCP amendments regarding ESI (Cohen & Lender, 2012).

In South Africa Section 33 of the Civil Procedures and Evidence Act 25 of 1965 with its standing amendments refers to documents as "'document' includes any book, map, plan, drawing or photograph." This was updated by the ECT Act 25 of 2002 in order to clarify the meaning of the word "document". The same document definition is in effect in Namibia with similar issues resulting from interpretation of the terms as technology has continued to evolve.

It can be concluded that to some degree each nation has updated its laws to account for the way evidence is presented and interpreted in regards to ESI. It is interesting to note

that Illinois still requires ESI be printed to admissible in court. Until recently this was also true in Namibia (Ludik, 2006).

In the same way the common laws are similar, the data examined in Chapter 2 indicate that the criminal laws are also comparable. When examining the criminal rules of procedure, one encounters items such as the right to a swift trial, representation of plaintiff and defendant, pre-trial issues, arraignment, dismissal, etc. Each of the three countries in this study has such items in their rules or laws of criminal procedure.

The United States has the Federal Rules of Criminal Procedure (FRCrP) which were established for consistency from state to state. Rule 41 is the primary one that applies in digital investigations and addresses search and seizure law. The table below shows the primary items of concern when examining Rule 41. The U.S. Department of Justice (DOJ) document on *Searching and Seizing Computers* goes into greater depth of how Rule 41 applies in digital criminal investigations. Table 3 below shows the subsections of Rule 41. In the development of the database, these subsections are incorporated in the table entitled Federal Rules sections and subsections.¹⁶ As will be shown in the Appendix A, this feature assists in comparing the laws of the nations.

Table 3 FRCrP Rule 41 and Relevant Sections

Section of Rule 41	Description
41(a)	Scope and definitions
41(b)	Who has authority to issue a warrant
41(c)	When a warrant may be issued
41(e)	The warrant must be issued to someone with authority to execute
41(g)	Motion to return property

¹⁶ See Appendix A

In the U.S. it has been assumed reasonable to search an arrested person. As seen in the literature search, many cases have come before the courts which are appealed at the Supreme Court level regarding “how far is reasonable.” The Supreme Court ruled that an officer may search a person to remove any weapons and to prevent potential evidence from being destroyed or discarded (Starbuck, 2012). There have been further rulings on inventory searches when a vehicle is in impound.

South Africa’s corresponding law to FRCrP 41 is the Criminal Procedures Act 51 (CPA) of 1977. Chapter 2 of the CPA addresses search warrants, entering of premises, seizure and related topics. The Table 4 below summarizes the various sections and what they address.

Table 4 - Chapter 2 of CPA Act 51

Section of CPA	Description
Section 21	Articles to be seized under a search warrant
Section 22	When items may be seized without a search warrant
Section 23	Search of an arrested person
Section 25	Authority to enter premises in interest of national security
Section 27	Resisting arrest or search
Section 28	Wrongful search and award of damages

When examining the items listed in the CPA, they are very similar to those in the FRCrP Rule 41. There are sections which detail when a search warrant is needed and when objects can be seized without a search warrant. Section 28 specifically deals with wrongful search and seizure. In the case of *Minister of Safety and Security v Liddell 2002*

the defendant was awarded R20,000¹⁷ for wrongful search and seizure, imprisonment and defamation of character (Ngomane & Horne, 2010).

In comparison, Namibia has the Criminal Procedures Act 25 of 2004 (Namibian Parliament, 2004). The items relating to search warrants, entering premises and seizure are contained in Chapter 4 of the Act. In examining the contents, they track South Africa's closely as shown in Table 4.

Table 5 - Namibian Act 25 of 2004

Section of Namibian Act 25 of 2004	Description
Section 21	Items to be seized under search warrant
Section 22	When items can be seized without a search warrant
Section 23	Search of an arrested person
Section 25	The right to enter premises for national security
Section 27	Resisting arrest or entry
Section 28	Wrongful search and award of compensation

The criminal laws of each nation track each other fairly closely. In regards to electronic evidence – specifically search and seizure law – all three countries have approximately the same principles in place. There are a few nuances, however. Note that in the U.S. the warrant may be to search a person or premises. In South Africa and Namibia, there is a separate item for the search of an arrested person. Rules regarding national security exist in the United States, but not under the FRCrP Rule 41. Both Namibia and South Africa list resisting arrest, yet that is not found under the FRCrP

¹⁷ R stands for Rand, the currency of South Africa

which is of note. Another item is that all three countries list wrongful search, however the U.S. lists return of items, while the other two countries list compensation.

The third item to compare is the rules of evidence. The Constitution of South Africa in Section 35(5) states any evidence that is obtained that violates the Bill of Rights must be excluded if it renders the trial unfair. There have been cases, however, when evidence was admitted in the interest of fairness when the method used to obtain the evidence was unconstitutional.

The rules of evidence in South Africa still apply to electronic evidence, but certain items have been affected by the ECT Act 25 of 2002. The Law of Evidence Amendment Act 45 of 1988 considers three items: witnesses, objects (otherwise referred to as real evidence) and documents (Watney, 2009). “The South African law of evidence also requires that anyone who wants to use a document as evidence has to satisfy the court that it is authentic; in other words, that the document is what it purports to be” (Lekala, 2011).

South Africa also distinguishes between public and private documents. When considered in context, this is logical. Public documents can be retrieved and authenticated. Private documents require that the person who created them appear in court and testify to their validity (Watney, 2009). In the discussion on hearsay, this requirement regarding documents becomes important. Note that Namibia also uses the Law of Evidence Amendment Act 45 of 1988 as this was created prior to independence and has not been changed.

In the United States, the Federal Rules of Evidence (FRE) determine items admissible in federal courts. The table below shows a summary of what was presented in Chapter 2. It begins with Rule 103 in which evidence can be removed for reasons such as affecting the rights of a party. Rule 105 addresses when limitations may be placed on evidence so that it can be used against one party but not against another. In civil cases, relevancy of the evidence and limitations as spelled out in Rules 401 and 402 helps in keeping the scope and amount of evidence presented relevant to the case. Rules 702 and 703 are addressed in the section on the Forensic Expert as they deal with expert testimony. Rules 802 through 804 are targeted towards excluding hearsay and when to allow hearsay (The U.S. House of Representatives, 1975).

Table 6 - Applicable Rules of the FRE

Article	Rule	Description
Article I	Rule 103	Rulings on Evidence
Article I	Rule 105	Limited Admissibility
Article I	Rule 106	Remainder of or Related Writings or Recorded Statements
Article IV	Rules 401 and 402	Relevancy and Its Limits
Article VII	Rule 702	Expert Testimony
Article VII	Rule 703	Bases for the Opinion of Expert Testimony
Article VIII	Rule 802	The Rule Against Hearsay
Article VIII	Rules 803 and 804	Exceptions to the Rule Against Hearsay
Article IX	Rules 1002 and 1003	Contents of Writings, Recordings, and Photographs

The interesting items from the U.S. laws that are similar to South Africa and Namibia are Rules 1002 and 1003. These state the requirement of the original document, which includes photographs, writings, and recordings, and the acceptance of duplicates.

The rules of evidence for the three countries have similar points that cause consternation in the courts with a primary one being admissibility of the evidence. Overall, however, the rules of evidence for all three nations show only minor variances.

The next item of commonality is in regards to computer abuse-related acts and laws. Each of the three countries has instituted laws concerning the use and misuse of computers or electronic communications. In the U.S. the Computer Fraud and Abuse Act set out to correct items left out of the original Counterfeit Access Device and Abuse Act of 1984. The CFAA specifically deals with unauthorized access which had not been addressed in the original act. Exceeding authorization, misuse including divulging trade secrets, and End User License Agreements (EULA's) which targets appropriate use of social media are now included.

In criminal cases, the rights of the individual are paramount as evidenced by each the data from each country. Proper warrants, subpoenas, and procedures must be followed to ensure the evidence is lawfully obtained and the evidence is not tainted. Again, the DOJ's document on Search and Seizure in Criminal Investigations can be used in the U.S.

The case of *U.S. v. Middleton* saw the application of the CFAA when the damages done by the defendant using unauthorized access could be calculated from the amount of man hours needed to repair the damage and lock down the system. In the case of *U.S. v. Morris* the creation of a malicious piece of software was upheld as violating the CFAA (The U.S. House of Representatives, n.d.). In much the same way, the FRCP varied from state to state in regards to which ones had updated their laws in regards to the 2006 Amendments to the FRCP; each state differs in how it defines and describes computer

access, crime, etc. The definitions range from unauthorized access, computer trespass, computer access, computer damage, to computer crime. The consequences are listed from criminal misdemeanor to a felony. Washington State, for example, lists criminal trespass in the second degree as a gross misdemeanor and criminal trespass in the first degree as a level C felony. In Alaska, there is no misdemeanor level and has a class C felony charge if you “obtain or change information about a person” (FindLaw, 2012).

Nevada is one of the states that distinguish between which actions constitute a misdemeanor or felony as shown in the following list:

- Unlawful access is a misdemeanor as well as unlawful interference with or denial of access or use
- Unlawful access done to defraud or obtain property or causing damages excess of \$500 or interrupts/impairs public service/utility is a class C felony; unlawful interference with or denial of access of use done to defraud or obtain property is a class C felony. (FindLaw, 2012)

Most states list the mental state of the person as being done with intent, deliberate, knowingly, or with malice. California states that a common defense is when a person performs such acts within the scope of lawful employment.

Several papers explored the South African ECT Act 25 of 2002. The report by the South African Law Commission supports unauthorized access being a crime because it infringes on an individual’s personal privacy. Also if the information is personal, financial

or economic in nature, it violates the constitution and should be a punishable offense (South African Law Reform Commission, 2010). Similar to the U.S. ECPA which lists protected computers, Section 71(2) of the South African Police Services makes it a criminal offense to access any computers belonging to the South African Police (Maat, 2009)

The ECT Act 25 of 2002 also covers several topics including the rights of the consumer, limiting the liability of the Internet Service Providers, legal requirements for data messages, domain name authority, appointment of cyber inspectors, defining cybercrime, and examining court jurisdictions and common law.

In his paper on electronic evidence, Watney voices concern that moving from the exclusionary form of law to inclusionary may have its drawbacks. His concerns are on whether or not a data message is “real evidence” or “documentary” (Watney, 2009). The evidentiary weight applied would be significantly more if it is considered real evidence. For a document to be introduced into evidence, by the law of evidence, it must be relevant and admissible (Cassim, 2010). This is not unlike the FRE in the United States. Likewise, the section in the ECT Act 25 on defining cybercrime includes language similar to what is included in the CFAA such as “unauthorised access to, interception of or interference with data” and “computer-related extortion, fraud and forgery” (Parliament of South Africa, 2002).

Similarly, Namibia first saw the introduction of the Computer Misuse and Cybercrime Act in 2003. This Act covers offences such as unauthorized access, unauthorized interception of data, unauthorized disclosure of password, and several

others which one would expect in a cybercrime bill. The Computer Misuse and Cybercrime Act 2003, however, lacked any real force of law by stating “No prosecution shall be instituted under this Act except on an information filed by, or with the consent of, the Director of Public Prosecutions” (Namibian Parliament, 2003).

In examining the ECT Bill of Namibia, several items such as those encountered in South Africa become apparent. Section 6 of this bill gives legal recognition of data messages and states that “information cannot be denied legal effect” because it is in the form of a data message (Office of the Prime Minister, 2010a). Also similar to what was done in S.A., limitations on the liability of ISPs is listed so that they cannot be held liable for crimes committed by third parties when acting as a “mere conduit”.

In Sections 33 – 37, offences such as unauthorized access, unauthorized interception, transmission or interference are now listed as criminal offences with Section 40 listing the penalties. The lowest offense level is for the equivalent of a misdemeanor with a fine and imprisonment for up to twenty-four months and the highest is for a felony charge such as criminal trespass with a fine and up to five years in jail. Overall, computer crime and abuse laws appear to have features in common.

The next item to examine is hearsay. In the U.S. hearsay comes under the FRE, specifically Rules 802 – 804. Rule 802 begins by saying the hearsay is inadmissible unless another federal statute or rule allows it. Rules 803 and 804 list the exceptions such as a recorded recollection – Rule 802(5)(A), (B) or (C). The use of email is the prevalent item that falls under the hearsay rule. Information included in emails may be personal in

nature or may be part of the daily conduct of business. This includes text messages, instant messages, etc. Is the content of these alone enough to admit them into evidence? Content alone is not enough for them to be admitted into evidence. The items must be reliable and authentic. FRE Rules 901 and 902 address authenticity. FRE 901(a) states “To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” This statement is very similar to what is stated in South African law. FRE 902(7) addresses how business emails can be authenticated by showing company logos or by a declaration stating the emails were retrieved from the company’s email server.

In South Africa, a data message cannot be excluded simply on the grounds of it being electronic. Under the best evidence rule, the original must be produced. In the case of data messages, an authenticated printout of same is admissible (Hershensohn, 2005). Evidentiary weight is given to a data message based on the reliability of its authenticity, that the content has not been damaged and that the originator has been identified or at least to the degree possible based on login information.

As mentioned earlier, South African courts distinguish between “real computer evidence” and “hearsay computer evidence”. Section 15 of the ECT Act 25 of 2002 creates the dilemma which appears to still be under debate in the South African courts. If admitted into evidence is a data message real or hearsay? If real, what restrictions should be put on said message or its contents (South African Law Reform Commission, 2010)? In the case “*Mdani v Allianz Insurance Ltd 1991* the court held that a statement does not

amount to hearsay if it is not tendered to prove the truth of its contents” (Ngomane & Horne, 2010). Thus if a data message is presented merely to prove its existence and not to prove the contents thereof, it can be admitted as real evidence. Namibia also has laws excluding hearsay but has yet to deal in the court system with it in regards to data messages. Overall, each country has similar rules of evidence.

Examination of Variances

The privacy laws vary the most significantly. In the United States people refer to the 4th Amendment when they think about privacy. The actual amendment deals with unreasonable search and seizure without probable cause. The Electronic Communications and Privacy Act (ECPA) along with the Stored Communications Act (SCA) does give privacy in regards to email both in transit and stored, but is not a true guarantee of privacy. And as was seen in the case of *Petraeus*, the ECPA has not kept pace with the advances in technology resulting in emails that have not been accessed by the owner in the last 180 days to not require a warrant, only a subpoena (Guynn, 2012).

In addition, each state of the U.S. which has its own privacy laws these can potentially affect what can be done in an investigation. As mentioned earlier, California has the most detailed laws regarding digital investigations (Overly, 2004). Privacy is also written into its state constitution as “an inalienable right” (California Legislature, n.d.). Another state that includes privacy in its constitution is Montana. Article 2, Section 10 of its constitution states "The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest” (Montana Legislature, 2011).

The South African Constitution specifically addresses privacy. Section 14 is shown below and is included in the database:

14. Privacy.-Everyone has the right to privacy, which includes the right not to have-

- (a) their person or home searched;
- (b) their property searched;
- (c) their possessions seized; or
- (d) the privacy of their communications infringed

The Constitution of the Republic of Namibia also has privacy written into its verbiage. It was written in 1990 during a period of time in the world when such concerns were paramount. The actual passage of Article 13 entitled Privacy is:

No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

(Constitution of the Republic of Namibia, 1990).

Note that what is addressed in the U.S. ECPA is written into the constitutions of the other two nations. This is a direct result of a constitution written two centuries ago versus those written in the last twenty-five years. The fact that privacy is in the

constitution can play a significant role when conducting internal corporate investigations. Unlike the United States where employees can be investigated without their knowledge, in both South Africa and Namibia, the employee must be notified.

Case law in the U.S. can be used to demonstrate when the 4th Amendment has been exceeded. Examples include the use of digital devices such as electronic eavesdropping and GPS devices. The *Olmstead* case during Prohibition stated that there was no physical intrusion and therefore did not violate search and seizure under the 4th Amendment. It was overturned by *Katz* in 1967 by stating physical intrusion was not needed in light of new technology and put clear boundaries on when a search warrant is needed in such cases.

Forensic Investigators and the Judiciary

A key question posed in Chapter One of this investigation concerned how one qualifies the digital investigator. The issue of properly trained digital forensic investigators in South Africa was addressed by Amanda Ngomane in her Master's thesis on Forensic Investigations. She spoke with five experts regarding digital evidence in the courts. Three stated that "there are no procedures on the collection of electronic evidence that have been tested by courts" (Ngomane & Horne, 2010). Two other experts felt that the methodology set by INTERPOL (International Criminal Police Organization) could be fine-tuned for the South African court system. Of the participants in the study, separate from the experts, over 75% agreed that electronic evidence should only be collected by those trained in the field. This is indicative of the lack of cases that have gone to trial as yet in South Africa in regards to electronic evidence.

Chapter XII of the ECT Act 25 of 2002 introduced the appointment of cyber inspectors in South Africa. A cyber inspector must be given a certificate from the Director-General and must show this to anyone who is being investigated or to anyone who requests to see the certificate. The cyber inspector can monitor Internet traffic, inspect computers or other devices and conduct lawful computer search and seizure. The South African Police can enlist the services of said cyber inspectors for their investigations. A major concern is that the inspectors could potentially violate the right to privacy because they fall under the Department of Communications and not the South African police (Maat, 2009).

The Private Security Industry Regulation Act 56 of 2001 allows corporations to conduct preliminary investigations such as interviews and obtaining statements, however criminal matters must be turned over to the South African Police (Ngomane & Horne, 2010). In the U.S. as well, if an internal investigation appears to be a criminal matter and not a civil offense, the internal corporate investigator is obligated to inform the authorities and turn the evidence over to the law to avoid becoming an agent of law enforcement which then requires a warrant.

In her study, Ngomane enlisted five experts, of them four stated “judges and lawyers are not specialists in computer crimes and have few or no computer skills and as a result they find it difficult to deal with cases that involve electronic evidence successfully” (Ngomane & Horne, 2010). This is similar to the conclusion reached by Kessler in regard to U.S. judges. Another conclusion reached in her paper was that if the investigators are not trained in the proper handling of electronic evidence it is not

admissible in court. The digital divide is greater in both South Africa and Namibia than in the U.S. While a large majority of people in the countries own cell phones and smart phones, a much lower percentage are computer literate.

The judiciary in the U.S. is not very different. In his dissertation, Kessler came to the conclusion that the judges needed to be educated by the experts in terms of electronic evidence. Murray and Frieden bring up a fact that was also one of Kessler's conclusions that many judges are highly skeptical of electronic evidence on its base (Frieden & Murray, 2011).

FRE Rules 702 and 703 address expert testimony and their opinions based on evidence they have examined or observed. The question becomes "Who is the expert?" In the U.S. states such as South Carolina, Texas and Michigan attempted to regulate computer/digital forensics investigators by requiring a private investigators license. In spite of a recommendation from the American Bar Association to the contrary, states such as North Carolina are following suit.

There have been a plethora of papers including *Computer Forensics Investigators or Private Investigators: Who is Investigating the Drive* by Phillips & Nance (2010) and the presentation by Dave Kleiman entitled *Digital Forensics: DCFB and the ABA Resolution*. They examine the need for certification and / or licensing of digital forensic practitioners while looking at the laws that are quickly being put into place without consideration of the consequences. In several instances practitioners could not present in another state because they were not licensed in that state.

The case law in the U.S. is still examining who qualifies as an expert witness under FRE 702 and the corresponding state laws. In his article entitled *Unpredictable and Inconsistent: Nevada's Expert Witness Standard after Higgs v. State*, Ryan Henry discusses the admissibility standards of expert witnesses in a case in which the state's expert witness did not fully comprehend or even examine all the evidence in the case. By applying the *Daubert* standard, the judges can focus on the soundness of the scientific method and not the conclusions drawn by an expert (Henry, 2011). However, the principle is still not uniformly applied.

If this is happening between states, what happens when evidence has to be presented in a foreign court? As seen above, the cyber inspectors in South Africa fall under the Department of Communications. Ngomane's study subjects and experts in South Africa all recognize the need for proper qualifications of the digital forensics examiners. Four of the five experts she interviewed cited recovery of deleted items when purposefully deleted by a suspect as a requirement of the field. One expert stressed that "computer forensics is unquestionably a highly specialised field and that as a result not everyone is skilled enough to handle electronic evidence and produce high quality evidence" (Ngomane & Horne, 2010).

If one were to look online, one would find several computer forensics investigators employed by insurance companies, banks, and independent companies in South Africa. An example is Cyanre (Cyanre, 2013). The managing director appears to be a former South African Police officer. Having former law enforcement as the founders or owners of such firms is not unusual in the U.S. as well. But what happens as this

profession becomes more mainstream? Does there need to be more of a balance as this affects corporations as well?

International Cooperation

As technology interlinks the world, peoples, corporations and communication, international cooperation in regards to digital investigations is needed. Both Namibia and South Africa created the International Co-operation in Criminal Matters Act 9 of 2000. In Namibia this act repealed the Foreign Courts Evidence Act of 1995 which had been carried over from South Africa (Namibian Parliament, 1995). While the original purpose of this Act was to address child trafficking, money laundering and terrorism, the digital world is not that far removed from any of these topics. The International Co-operation in Criminal Matters Act outlines the procedures to be followed when issuing a request to or receiving a request from a foreign government or tribunal for evidence. Provisions in terms of financial support are made for citizens having to bear witness abroad. Of particular interest to this study is the provision of evidence obtained by a letter of request. In such a case, four conditions exist, two of which bear mentioning here. The first is that the witness giving testimony is told under the laws of “the requested State... properly warned to tell the truth” (Office of the Prime Minister, 2000). The second is the fourth condition which states the evidence becomes a part of the trial proceedings as long as it is not inadmissible under Namibian law. So the question must be asked under what laws evidence would be inadmissible?

Namibia lists the same conditions as South Africa for when the Republic has jurisdiction including if the offense was committed locally, had repercussions in the

Republic, was committed by a citizen or permanent resident or on board a craft inbound or outbound from the Republic.

In South Africa one also deals with the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Recall in Section A. 1. the International Telecommunications Group Union stated that the Convention on Cybercrime deals with interception of data but also said “the question of whether illegal access to information stored on a hard disk is covered by the Convention was discussed with great interest” (International Telecommunications Union, 2009). So it would appear that countries work well together when data is being transmitted, but when device forensics enters and local laws prevail is when problems can arise. Both the United States and South Africa are members of the Convention on Cybercrime which attempts to address this matter. Maat concludes that in Section 90 of the ECT Act 25 of 2000, South Africa goes beyond what is agreed upon in the Convention by stating “any offense that has an effect on the Republic” is extraditable (Maat, 2009).

The Convention on Cybercrime also deals with extradition in regards to cybercrime. Each nation has an extradition act and requires a treaty with reciprocal arrangements. South Africa’s Extradition Act limits when a person would be extradited to the country in which the offense occurred or affected. “It is clear that a perpetrator will only be extradited for a serious offence and a perpetrator that merely gained unauthorised access to a system without causing damage, might not be extradited” (Maat, 2009). The situation explored in Chapter Two in which a person wanted in the United States settled in Namibia illustrates the complications that can arise when diplomatic relations exist,

but a treaty does not. Recall that the President of Namibia signed a Proclamation naming the United States as someone to whom they would extradite to; however Kobi Alexander is now charging the proclamation is unconstitutional because it is aimed at a particular individual.

Despite much cooperation in criminal cases, courts are dissimilar in the sanctions or penalties applied. The most noticeable example here is the statement that for unauthorized access to a website, South Africa would not extradite a citizen to another country when the penalty would be less than six months. This is discussed more in detail in the responses from experts in Chapter Five.

Summary

This chapter examined the commonalities and variances between the laws of the nations in question with regards to their impact on digital law. In general, it can be concluded that common law nations do take similar approaches. While both South Africa and Namibia are the combination of three types of laws including tribal law, overall they follow the British common law or Roman-Dutch law. The U.S. is effectively a common law nation as well. All three case studies use the same three branches of government, namely – executive, judicial and legislative.

Similarities also exist in the civil and criminal laws along with the rules of evidence. The civil laws are very similar in nature and effect. The internal differences seen between the states of the U.S. and the other countries do have some correlation. The two most significant ones being to show relevance for ESI and the printing out of ESI which is still required in Illinois and until recently in Namibia and South Africa.

There were few differences in the national criminal laws of the countries. The FRCrP, the CPA Act 51, and the Namibian Act 25 of 2004 all address the need for a warrant, when a warrant can be issued, search and seizure, and wrongful seizure. The primary differences were 1) in the U.S. the warrant was to search a person or premises; 2) in Namibia and South Africa, the search of an arrested person is a separate line item; 3) entering a location is in U.S. laws but not stated in the FRCrP, however in Namibia and South Africa, the situation is stated in the Act; and 4) people are compensated for wrongful seizure in South Africa and Namibia; by default in the U.S. they are not. Overall, the differences are not likely significant enough to cause issues in cooperation in digital investigations.

The evidence laws for each of the three countries are very similar. Each of the countries has had to address how digital evidence affects the laws of evidence. Overall, none has had to make significant changes other than definitions. And on the topic of hearsay, each country denies hearsay outright and then lists the exceptions. The evidentiary weight of email that is not in the standard course of business has to be weighed by each court.

The most significant differences were in the privacy laws. In the U.S. there is an expectation of privacy under the 4th Amendment. Also Acts such as the Electronic Communications Privacy Act and Stored Communications Act protect email and communications. And in several states – including California and Montana – privacy is a right under the individual state constitutions. Case law is constantly changing to address new issues under the 4th Amendment presented by new technology.

Both South Africa and Namibia have privacy written into their constitutions. The privacy provisions include the rights not only with regards to unlawful search and seizure, but protection regarding communication and correspondence. This directly affects the way data can be acquired as well as notification of the person under investigation.

Issues between States in the U.S. may be similar to differences in approaches between the countries. As noted earlier, various states in the U.S. approach licensing, privacy and other issues differently.

Pivotal cases exist in each country which drive the laws. In regards to the U.S. and South Africa, this is supported by the data. In South Africa, the case of *Narlis v South Africa Bank of Athens* which caused the definition of the term “document” to be updated is certainly one. Per the South African Law Commission, both South Africa and Namibia have had cases where the case law conflicted, which resulted in some of the verbiage of the ECT Act 25 of 2002 and later a similar act in Namibia. In the *Olmstead* case in the United States, the definition of “eavesdropping” had to be addressed in regards to electronic eavesdropping and physical intrusion which was visited again under the *Katz* case. Each of the countries is addressing the issue of email being allowed as hearsay or real evidence. The question of admissibility is always present based on the laws of evidence which have been determined to be similar.

CHAPTER FIVE - EXPERT OPINIONS

The experts interviewed in this chapter deal with the laws and procedures of digital evidence in the daily execution of their jobs. In performing a qualitative analysis, one relies upon non-quantitative data. The sample size is generally small and non-statistical (McRoy, n.d.). The responses from legal and corporate experts in the three countries explore the situations presented in Chapters Three and Four.

When conducting a qualitative analysis, interviews can lead to new ideas that had not occurred to the researcher or the interviewee prior to the discussion. In the case of some experts, questions were initially tailored to elicit a response or simply allowed to become an informal guided conversation. Questions were posed to each of the experts who chose to answer them in their own fashion. In many of the cases, the interviewee did not address any of the questions but presented issues that had not been considered. Some of the questions, which are meant as guidelines only, were:

1. Have you accepted electronic evidence from another country? If so, what restrictions did you enforce?
2. Have you ever submitted electronic evidence for use in a foreign court? If yes, what restrictions were there?
3. Have you ever been a witness in a foreign court for e-evidence? If yes, what requirements were there?
4. If a multinational company with a subsidiary in <respective country> collected e-evidence which would be used against a <respective country> citizen that violated <respective

country> laws but satisfied the laws of the home country of the company would the evidence be admissible?

5. What requirements are there for a forensic investigator?
6. Are there any health information privacy laws in <respective country>?
7. Alternate question – Can you think of any case law that caused significant changes in the way e-evidence is handled?

A total of nine experts were interviewed using a variety of formats including email, face to face dialogues and telephone conversations. Their expertise includes corporate digital investigators, senior researchers in the field, directors of forensic science, and those with legal expertise. The examination of the data revealed items that are currently lacking, have only recently had standards enacted, or that have not been codified in the practice.

Expert One

Professor Marthie Grobler is a senior researcher in Cyber Defense and is on the South African Council for Scientific and Industrial Research. Several of her papers were used as references in this research which contributed to her being put on the list of experts to be interviewed. While she has not been involved in digital investigations, she is the co-editor of “international standard ISO/IEC 27037 where ...[the] specified minimum documentation requirements for evidence transfer” (Grobler, 2012) are

established. Dr. Grobler chose not to address the questions posed, but to forward the document instead.

At the time of the interview, this ISO standard was in the final draft phase and being reviewed. It is entitled *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*. It was officially approved and released in October of 2012. The preferred method for evidence transfer in the document is encrypted which is also the method used by Expert Two. Such standard guidelines will aid in mutual acceptance of procedures between nations when dealing with digital evidence. The document also spells out the skills and various skill levels for the Digital Evidence First Responder (DEFR) and Digital Evidence Specialist (DES).

The lack of an international standard stood out in the literature search. The creation of one would be beneficial to the field. Now that the ISO standard exists, some guidelines which have been codified can assist countries in solidifying or creating their own. It will also assist in international cooperation and multinational cases.

Expert Two

Stephanie Scheuermann works for a Fortune 500 company¹⁸ and gave this statement as the preamble to her response:

My practical experience is in the private sector for a U.S. based company that is a Global Enterprise. Often digital data located in foreign countries is relevant to an

¹⁸ Ms. Scheuermann requested the company not be named specifically

investigation or litigation matter. The majority of cases requiring testimony (affidavit, deposition or courtroom testimony) from me have been civil cases not criminal.

Therefore it is also important that civil litigation is primarily an American phenomenon. U.S. courts often do not have much patience for businesses that intentionally choose to offshore their business and expect compliance to discovery demands, meaning it is the companies issue to resolve the foreign requirements for individual privacy laws.

With that caveat I will answer your questions. (S. Sheuermann, private correspondence, 2012)

Ms. Sheuermann's statement that it is the responsibility of the corporation to deal with foreign privacy laws is telling. In examining the variances, privacy issues were considered to be an issue and this helps in confirming it as something of which investigators must be aware. In a civil corporate case the handling of the evidence is negotiated beforehand. Her company uses methods that are forensically sound with a verified chain of custody. She used the term "method adhered to generally accepted practices" which implies that standards do exist for e-evidence on a global level. The delivery of the evidence could be physical – meaning shipped via Federal Express or

similar transport - or transmitted. In each option, she stated that the data would be encrypted with adequate safeguards on both.

As regards to whether or not she has ever submitted evidence for use in a foreign court, her company chooses to have “specialized analysts” who “comply with local obligations.” The analysts have unique positions in dealing with allegations within the company. Some cases may be “disclosed” which means they are already in court, while others may be “undisclosed” which can be advantageous if the allegation turns out to be erroneous or to prevent the suspect from destroying data.

When asked about certification of digital investigators, her response was that the forensic investigators of her company undergo training and certification on a regular basis. They use credentials which are recognized on an international level which may include vendor certification. This is important to note when addressing civil cases. In Chapter Two it was noted that other than vendors, many certifications are limited to law enforcement or government employees. Private or civilian corporations almost always have to rely upon vendors for such training.

Expert Three

Ron Godfrey works for a Fortune 500 company in the Northwestern United States which has foreign subsidiaries. He has over 20 years of experience in information technology with fourteen of those being in digital forensics. An objective of this paper was that evidence collected and perhaps analyzed elsewhere can be used in a foreign court. He also conducts digital investigations for two private firms including an attorney’s office. His response to the first question regarding acceptance of forensic evidence from

another country is yes. However, only the forensic drive images are done by the experts or technicians overseas, he and his team perform the actual analysis. He states that in cases such as this one has to rely upon the IT personnel to use write blockers¹⁹ and follow forensic procedure (R. Godfrey, personal interview, 2012). In this type of situation, he has to be sure to include in his reports that he did not perform the actual drive imaging in the event it is challenged later.

Surprisingly he could answer in the affirmative to questions preparing evidence for use in a foreign country, being an expert witness in a foreign court, and dealing with the laws of another country. In a particular case, a wholly owned subsidiary in another country²⁰ was suspected of fraud. He and his team had to fly to that country and conduct a full forensic examination of the associated drives, email servers, etc. After obtaining the forensic evidence, they returned to the U.S. and upon examination of the evidence, the company terminated the employees. The employees appealed which meant he and his team had to return to the country to present the evidence and testify.

The hearing was a mini-court conducted by the local labor board of the other nation. He and his team had to educate the board members as to what computer forensics is and how his teams obtained the evidence. Being able to convey the information to the lay person, Mr. Godfrey feels is the most critical part of being successful in the courtroom.

¹⁹ Write blockers are used when making a forensic copy of the suspect drive to ensure no data is altered during the process.

²⁰ Mr. Godfrey has requested that the name of the country be withheld

In addressing the question regarding requirements for the forensic investigator, his response focused on the method of acquisition and the privacy laws of the country in which the evidence was acquired. He gave an excellent example of the privacy issue. In Australia they would not allow the digital device to be shipped out of their country. Privacy comes into the arena, because the data contained on it may contain personal information. Employees can use their work computers for minimal personal use such as online banking, emails to spouse, etc. In a full forensic examination the investigator would see that data. This was a case in which they would have to send the software to an examiner in that country and walk them through the process. It becomes a challenge to the competency of the examiner. If they terminate the employee and that person sues for wrongful termination, the employee or their attorney could ask “Who was the examiner and what are their qualifications?”

A possible solution would be to fly an investigator to that country and have the corporate investigator present as the forensic examiner does their job. The forensic examiner however may still be violating their privacy laws because he or she is not a citizen of that country. These are issues that corporate investigators face on a daily basis.

His most striking statement was “my most successful cases are when I sit down on conference call and explain things to the legal team” (R. Godfrey, personal interview, 2012). He educates the attorneys and paralegals on what he does to retrieve the information they did so they can explain it in court.

This was one of the more telling interviews. Mr. Godfrey was able to directly answer most of the questions and address the issues that arise when dealing with the laws and courts of other nations in which a multinational company operates.

Expert Four

Mr. Cain is a research fellow and former security officer in the United States. His perspective is a blend of academician and former practitioner. He chose to ignore the questions and give a general treatise on the associated topic instead. His suggestion was to look at the recent development known as Mutual Legal Assistance Treaties or MLATs. In researching these, they apply primarily to criminal cases and provide information to the prosecutor. The treaties are done on a country by country basis (U.S. State Department, 1997). He noted that they can take six months or more to fulfill (P. Cain, personal correspondence, 2012). His opinion is that the “rules for civil procedure are made on the ‘fly’”. It is interesting to note his perspective that since he and those in his organization are not sworn officers, they cannot present evidence for the U.S. State Department. This is certainly true given that his focus is on criminal investigations. Recall also that the opinion in South Africa regarding the cyber investigators was that they were violating the constitution because they are not actually part of the South African Police Force. The overlap is something of note.

The prior two experts focused on civil procedures. As has already been shown, in common law nations, civil cases and criminal cases are handled differently. His mentioning of the MLATs resulted in research into how they may affect the handling and acquisition of digital evidence.

Expert Five

Gib Sorebo is a Chief Cybersecurity Technologist. He selected the questions to which he felt his expertise could be most useful. His response regarding evidence collected against a U.S. citizen is that it would only matter if the trial were held in the U.S. Mr. Sorebo adds that the qualifications for forensic investigators are “in flux” everywhere much the way they are in this country. Therefore an actual answer cannot be given.

An interesting observation is “Nearly all other countries have less liberal policies regarding discovery, so that is likely to impact the relevance of forensics investigators, particularly in civil cases” (G. Sorebo, personal correspondence, 2012). He also pointed out that there would be marked differences in the way common law countries handle things vs. civil law countries.

The issue of conflicting privacy laws is emphasized in his commentary shown below from a paper on remote discovery:

Aside from forensic examinations, the very notion of remotely collecting data in other states raises a number of issues relating to the state’s desire to accord privileges to its citizens. Because most state privacy laws target personal data about its citizens without regard to location, the privacy aspects seem not to be implicated. Moreover, constitutional protections of interstate commerce would seem to preclude a state from restricting the flow of such

data. However, because this data may be destined for a court, practitioners should be wary of state specific privileges that may arise. Conflict of law principles are far from settled in this area as it is unclear whether privileges apply to data at its generation point or in the state where the court is located. (G. Sorebo, personal correspondence, 2012)

That privacy issues would arise in transferring data between states or presentation of data acquired across state lines may violate privacy laws is of grave concern. This adds credence to the hypothesis that issues within the United States may point to issues that could be encountered when dealing with other countries.

Expert Six

Dr. Gary Kessler was interviewed because his works were cited continuously and as he serves both as an academic and a practitioner, his opinions may prove useful. He has over 20 years of experience in this field. Dr. Kessler does not have experience in dealing with international cases and could not address the first four questions. He does, however, have extensive experience in cases that cross state lines and dealing with local law enforcement. He believes that the procedure is valid for digital forensics. When evaluating the forensics examiner, he believes in looking at the totality which includes their training, education, experience and certifications. This appears to concur with how judges and others conclude the examiners expertise.

His opinion is that the key issue will boil down to the mobile forensics world. The Fourth Amendment will affect how the laws regarding mobile forensics develop. In the case law relating to cryptography and passwords, there are conflicting decisions. Some cases require the accused to render an unencrypted version of the drive. The Ninth Circuit Court dealt with a comprehensive drug test which we explored in Chapter Two – Balco.

In Vermont, which is part of the Second Circuit, there are twelve amendments related to digital evidence. The Attorney General in Vermont took it to the State Supreme Court that you cannot tell the police how to do their job. A particular case showed a letter from the company Staples saying “the only way to fix the hard drives would be to replace the hard drive” due to a virus. The civil judge called it “purposefully committed spoliation” (G. Kessler, personal interview, 2012)(Kessler, 2012). In another case which involved embezzlement, the police had already investigated; however, they had never examined the computer. They may have to re-open the case as a result.

Dr. Kessler described how he was a key player in enacting the rewording of the Vermont Computer Crime Legislation. In the 1990s, there were no known statutes. Very similar to what has been seen elsewhere if people only copied the data, they did not render the owner unable to use the data. Therefore the “theft of computer data” had to be redefined. Being very precise with definitions, similar to what we have seen in Namibia and South Africa, had to take place.

Dr. Kessler describes the digital forensics field as “fun and frustrating.” The new frontier consists of mobile devices. This is complicated in his opinion by the fact that many law enforcement officials feel that “mobile device stuff is not forensics.” Because

the tool Cellebrite²¹ is easy to use, many departments will allow officers to retrieve evidence with no training. That would not occur with any other type of digital evidence. Dr. Kessler makes his concern plainly known when he says “we are throwing the least experienced at the most valuable evidence.” Many inexperienced investigators do not know how to proceed if no evidence is found when later it is determined that they had it set to the WRONG device. It is a case of someone being trained on a particular piece of software without adequate understanding of the underlying technology. The most significant quote from Dr. Kessler is “phones will have more probative value than the computer.” When one considers what can be stored on a smartphone and that a large percentage of individuals own one or have access to one, this statement cannot be ignored.

On the issue of states requiring a private investigator (PI) license, he pointed to an event in which Scott Moulton – a renowned digital forensics expert – was called as an expert witness but was not a licensed PI, the judge responded “I qualify experts.” Here was a person who is well published and qualified nationwide, but because of a new ruling was being challenged is utterly absurd. Dr. Kessler agrees that change is on the horizon; however it is not clear how easily that is going to be achieved.

Speaking with Dr. Kessler gave a good indication of what is happening in the United States and what might be on the horizon for the digital forensics industry. The challenge of how to qualify experts and the current shortcomings are critical items.

²¹ Cellebrite is a popular forensics tool that is used for smartphones and other mobile devices. The company provides new connectors on a periodic basis to address new devices coming on the market.

Expert Seven

Dr. Paul Ludik is the Director of the National Forensic Science Institute under the Bureau of Home Affairs in Namibia. He is a practitioner as well as a supervisor of investigators. When he did not immediately respond to the questions posed, a different tack was taken and specific cases were addressed. As it turns out, it appears there have not been many in the Republic. One which Dr. Ludik recalled occurred approximately six years ago. In it the suspect owned a private gymnasium and was suspected of being a “peeping tom” and filming the women in their locker room, including minors. His description is of a situation that can happen all too easily:

We investigated and found his shoe prints in the dust on the ceiling but he defended that he was there to fix the geyser which happened to be located in that area. We also found a small hole above the cloakroom which off course was rejected as too circumstantial.

We then found recorded images from some of his PCs that we linked to his video camera. Unfortunately the Police Crime Scene examiners did not request our assistance when seizing the PCs; of which he happened to erase and rewrite some of the hard drives remotely (P. Ludik, private correspondence, 2012).

This case description is a textbook example of what can happen when inexperienced persons conduct digital evidence investigations. Dr. Ludik also makes a

telling statement in his statement ” that in our Courts we need to supplement all digital evidence cases with other forms of physical evidence in order to guarantee proper grasp from Court” (P. Ludik, private correspondence, 2012). In Chapter Two it was presented Dr. Kessler stated in his dissertation that judges suspect digital evidence on its face (Kessler, 2010). The lack of acceptance of digital evidence appears to cross borders.

To determine how digital evidence is acquired and accepted in other nations, it is critical to observe how it is perceived in other nations. Dr. Ludik’s perspective on the lack of adequate training and resources emphasizes where the challenges exist.

Expert Eight

Anna Matebele works for the Communications Regulatory Authority of Namibia (CRAN) which was created in May 2011. The passing of appropriate acts and laws in emerging countries is one of the important issues facing the 21st century and multinational jurisdictions. Her interview was more open ended to accommodate her field of expertise and as a result the questions posed at the start of this chapter were set aside. Anna worked in financial regulations for approximately seven years before being hired by the commission in March of 2012. The committee is creating regulations and oversees the Communications Bill. She is responsible for establishing the legal department and the hiring of said personnel.

It was her opinion that sometimes groups in Namibia need to push the government to move on some items that may not seem as pressing as the jobless rate and

poverty. There is currently interest in getting the Electronic Commerce Transaction (ECT)²² Bill passed.

Currently one high focus is the Universal Service Access which means that each area of the country needs some form of communication. She noted that all servers or ISPs are local companies. An interesting side note she mentioned is the work of a retired politician who now has a farm near the San Bushmen of Namibia. It is possible a mobile communications tower will be placed near their primary dwellings. So imagine a San Bushman in traditional garb out in the bush using a Blackberry. It is not that far off. And it may help with increasing the educational access in those regions as well.

Anna noted that Namibia, unlike the reputation of the U.S., is not a litigious society. When asked if IWay (a Namibian ISP) has a process in place for receipt of a warrant, she was not sure. Telecon would make sure to cover their legal risks first. They would err on the side of caution. And there would certainly need to be a legal process in place. There would also be a Human Rights watchdog.

In discussion of communications legislation, there are certainly provisions in place for government investigations. The case she related had to do with a company not paying the proper amount to family members for funeral benefits. The company was paying N\$10,000 instead of the prescribed N\$15,000. It was thought that misappropriation was occurring. In such a case, the computers, etc. can be seized as long as they have a reasonable suspicion of regulation violations. In a similar case protecting pensions, they seized two laptops, however the evidence never got to court.

²² The San Bushmen are indigenous people to the SADC region

The interview with Anna made it very clear that digital investigations affect not only corporations and law enforcement but the everyday citizen as well as noted in the case above regarding misappropriation. Many of the new developments may help in the future for job creation and attraction of outside investors.

Expert Nine

The Honorable Justice Sylvester Mainga of the Namibian Supreme Court provided a face-to-face interview for this study. Because one of the objectives of this research is to determine if items would be admitted in foreign courts, it is fortuitous that one of the Justices of the final appeals court of the nation granted an audience.

Justice Mainga was on the Namibian High Court from 1999 to 2010. He was appointed to the Supreme Court in May 2010. In Namibia, the High Courts receive the appeals from the District Courts along with serious crimes such as murder and rape. The Namibian Supreme Court is the equivalent of the U.S. Supreme Court – their ruling is the final stop for appeals. A more detailed description of this court is found in Chapter Two.

When asked about the role of digital forensics experts, he agreed that judges do rely upon the experts to properly present the evidence. He wants to see that the evidence was properly collected and that if a procedure exists it is followed. This demonstrates the correlation between his opinion and the judges interviewed in Kessler's dissertation.

Of interest was his response that the Computer Evidence Act only applies in civil matters. With criminal proceedings, they rely upon section 221 of the CPA. Also there is an exception to the hearsay act in section 244. Upon examining that section of the CPA, it refers to an accused giving testimony and 244 does refer to hearsay.

When asked about evidence collected in another country, Justice Mainga replied that it would be accepted if accompanied by a sworn affidavit from the investigator with their credentials, the accepted procedure in their country and the procedure they followed to obtain the evidence. That is supported by section 239 of the CPA. One issue that did come up in the conversation was the interview of children. If they were interviewed in a separate room, their expressions could not be seen. This would present a problem in the acceptance of said testimony.

On the question of extradition, he did not hesitate in saying Namibia would extradite. The Honorable Justice Mainga states that extradition should be done quickly. Namibia has an extradition act. He explains that the countries should agree upon the terms. It forbids extradition if the accused was convicted in absentia. For example, in the case of a Namibian who was accused of rape in France. He was tried and convicted in absentia. Namibia agreed to extradite him if he was granted a new trial.

The notable case involving extradition, as discussed in Chapter Two, is that of Kobi Alexander who has been fighting extradition back to the United States since 2005. In addition to donating millions of dollars for student scholarships and other humanitarian issues in Namibia, he hires attorneys to fight every detail. His latest is that the Proclamation 10 adding the U.S. to the Extradition Act is a constitutional violation because it was directed specifically at him.

On the topic of warrantless searches, raids can be done in Namibia without a warrant if, as shown in the examination of the law, the officers assume a warrant would be granted or if it is feared the evidence may be destroyed or tampered with.

The conversation turned to the requirements of licensing of digital experts. As was explored in the article *Who is Inspecting the Drive?*, the state of Texas is one that requires digital investigators have a private investigators license. The Justice was amused when the situation regarding a Texas company taking photos was not a licensed private investigation agency. In Namibia in the case of traffic photos and tickets – the question becomes who was actually driving? The laws in Namibia are different in that the insurance does not increase as a result of tickets as it can in the U.S. It is highly possible that an amendment may be needed to the Criminal Procedures Act or similar to handle the new technology.

In regards to the cyber inspectors now being used in South Africa mentioned in Chapter Two, an ordinary person can make an arrest; therefore it is probably not a constitutional violation. The Honorable Justice Mainga pointed out that Namibia shares the same legal system as South Africa. For rulings prior to independence in 1990, Namibia uses South African case law²³. However, post-independence they are under no obligation to use South African case law.

If the case law does not exist in Namibia, then they look to South Africa, the United Kingdom, Canada, the United States, and India. Interpretation is always given on the Human Rights Provisions. Justice Mainga was curious as to why U.S. courts do not look outside of the national borders when deciding cases. South Africa actually has a provision to look outside of their borders in the Constitution. To find this he referred to

²³ The intertwining of Namibian and South African case law was discussed at the end of Chapter Three.

the Execution of a foreign courts judgment which can be found in Section 41 of the Namibian constitution.

Understanding how the judicial system and judges specifically in their perspective of digital evidence is of key interest to this investigation. Being able to discuss the matter with a member of the final appeals court of one of the case studies was particularly revealing. That judges expect a procedure to in place in the country in question and that the procedure is followed is an important revelation in terms of how to prepare evidence for use in another country.

Summary

Recall that when dealing with grounded theory the sample size is small and non-statistical in nature. In addition, four items should be addressed: fit, relevance, workability and modifiability (Hamilton, 2011). The grounded theory being formed assumes commonalities and variances in the three case studies. According to the commentary from the experts, an international standard for the training of professionals is underway. Proper training of forensics professionals and those who interface with them along with discovery laws are issues in civil and criminal cases in all countries. Proper training not only of the investigators, but of those in the legal profession is critical.

In the experts from the United States who were queried the interesting item to note was that in general each was either only familiar on the civil matters or only on the criminal matters, but not both. For civil proceedings, corporations have had to develop methods that work in each of the countries in which they do business. The relevance of

this research for practitioners in the field is the resulting database that can assist such professionals in their daily activities.

The third item for grounded theory is workability. In Chapter Four it was stated that the term “workability” implies that the theory “explains how a phenomenon is being addressed, solved, or managed” (Hamilton, 2011). The interviews demonstrate part of the hypotheses put forward in the introduction of Chapter Four. The approach to civil law in each country varies from the approach to criminal law because of the rights of the individual and privacy issues. The interviews illustrate how groups in both the civil and criminal camps are dealing with multijurisdictional digital evidence. For example, in the civil arena it is accomplished with established corporate policies. The Mutual Legal Assistance Treaties and extradition treaties exist for the criminal cases. As the technology makes more and more cases global, the need for more consistency in the international civil and the criminal arenas becomes apparent.

CHAPTER SIX - CONCLUSIONS AND NEXT STEPS

This dissertation set out to examine the digital forensics concepts in the form of three case studies – the United States, South Africa, and Namibia. Its purpose was to lay the foundation for the legal proceedings for digital investigations in a world that has multinational corporations, is increasingly digital in nature and can be litigious depending upon the cultures and the corporations involved. It also sought to examine the emergence and impact of e-discovery. It was established in Chapter Two that the three countries investigated can each be considered common law or at least a hybrid thereof. In the end, each relies upon case law when a law does not exist especially in the situation of new or evolving technology. This chapter begins with the original questions and hypotheses followed by the conclusions drawn from same. The first section examines the challenges faced as evidenced by the investigation, followed by what is needed in terms of training. Next, the impact of the emergence of e-discovery in the study is discussed. And finally, the future research and work that is needed are explored.

Conclusions and Resulting Grounded Theory

This investigation began with three primary questions: 1) what conditions have to be met if evidence collected in one's own country were to be tried in another; 2) what conditions have to be met for evidence collected elsewhere to be tried in one's own country; and 3) what professional qualifications are there for the digital forensic practitioner and how is that recognized externally?

Applying constant comparison to the case studies, the commonalities and variances between the three common law nations were sorted based on the data gathered. The study began by determining what laws existed at the international level that would affect the laws or creation of laws and treaties of the individual nations. The exploration of international laws showed that groups such as the Convention on Cybercrime exists and the new ISO Standard 27027:2012 has been created; however, the responsibility for device forensics lies with the individual nations to create local laws. In Chapter One, the prototype by Nance and Ryan for areas of study for items that may influence the legality of digital evidence was introduced. Using this as a preliminary guide, the investigation explored the rules of civil procedure, criminal procedure and rules of evidence for each country. It also examined the privacy laws, rules for computer misuse and abuse, hearsay, requirements for investigators and international cooperation. The comparisons allowed conclusions to be drawn as demonstrated in the next few pages. Below are the resulting items presented in Chapter Four:

1. Areas in which there are commonalities
 - a. Common law countries take similar approaches
 - b. There are similarities in the civil laws
 - c. There are similarities in the criminal laws
 - d. There are similarities in the evidence laws
 - i. Hearsay rules
 - e. Pivotal cases exist in each country which drive the laws

- f. There are similar cases in each country demonstrating that countries are dealing with the same or similar issues
2. Areas in which there are significant variances
 - a. There are significant differences in privacy laws
 - b. Despite much cooperation in criminal cases, courts are dissimilar in the sanctions applied or penalties
 - i. Cooperation in web defacement is not prevalent
 - ii. International cooperation in regards to financial hacking is very well established
3. Issues between states in the U.S. may be similar to differences in approaches across the countries.
4. The requirements for the digital forensic examiner will vary, but may currently rely upon the vendors on an international scale.
5. International cooperation exists, but improvements are needed

It was first assumed that common law nations respond to legalities in similar manners. This has certainly been borne out by examining the structure and legal histories of these three nations. With executive, judicial and legislative branches the flow of authority is approximately the same and allows a person to have some confidence that a similar law or structure will exist in another common law country. Each country also has a Bill of Rights that applies to the citizenry.

The next supposition was that Namibian and South African laws would track closely due to their prior history. In examining the laws that were carried forward in

Namibia to present day (from South West Africa to the Republic of Namibia) the assumption was supported. The Honorable Justice Mainga bore this out in his interview when he stated that for cases prior to independence the Namibian courts use South African case law. Further, in the post-independence era, they can use S.A. case law as needed. From a grounded theory perspective, this can be used when examining countries with similar histories – meaning former protectorates or occupied territories will share the same laws.

As was shown in Figure 4, the constant comparison phase would sort the data into commonalities and variances. The civil laws of the three countries examined are very similar in their scopes and effects. In 2006, the U.S. updated the Federal Rules of Civil Procedure (FRCP) to include items directly related to Electronically Stored Information (ESI). Both South Africa and Namibia accomplished the same items in their creation of the Electronic Communications and Transactions (ECT) Act 25 of 2002 and the Computer Misuse and Cybercrime Act. Therefore the hypothesis is correct that the civil laws will be the same.

Another commonality was in regards to criminal law. In the table below, a comparison of the U.S. Federal Rules of Criminal (FRCrP), South Africa's Criminal Procedures Act (CPA) Act 51 and Namibia's Act 25 of 2004 are shown. This illustrates how straightforward it is to compare the rules of common law countries at a fairly granular level to make the use of digital evidence across borders more fluid.

Table 7 -Comparison of Criminal Laws

Description	U.S. FRCrP	S.A. CPA 51	Namibian CPA Act 25 of 2004
Scope and definitions	41(a)	Section 1	Section 1
Who has authority to issue a warrant	41(b)	Section 21 (1)(a)	Section 21 (1)(a)
When a warrant may be issued	41(c)	Section 21	Section 21
When items may be seized without a search warrant	Case law	Section 22	Section 22
Search of an arrested person	Case law	Section 23	Section 23
Authority to enter premises in interest of national security	Case law / Patriot Act	Section 25	Section 25
Resisting arrest or search	Case law	Section 27	Section 27
The warrant must be issued to someone with authority to execute	41(e)	Section 21(2)	Section 21(2)
Motion to return property / wrongful search /compensation	41(g)	Section 28	Section 28

As can be seen, for several items in the United States, case law is relied upon because of when and how the laws were written. For example, in the U.S. a search warrant is issued for a person or premises, therefore a separate item was not created two centuries ago for the search of an arrested person. It has also been the practice of law enforcement to search the arrestee for weapons or evidence (Starbuck, 2012). However, as was shown in Chapters Two and Three, in the Gant case if the suspect has already been secured, the search of his vehicle was uncalled for. While inventory searches are standard when cars are impounded to protect both the individual's property and the police from possible harm, limitations do apply. In the recent Supreme Court ruling, even a strip

search of a suspect for a minor offense was upheld. Therefore, search of a suspect appears to always be allowable.

When items may be seized without a warrant and entering when in the good of national security are also covered in case law and other Acts, but not in the Federal Rules of Criminal Procedure. The table above is the start of the template created as part of this dissertation. By going down to the granular level, similarities between countries can be seen and mapped in a straightforward manner.

If it can be consistently shown to be true that common law nations have similar criminal laws and statutes, international cooperation in terms of digital evidence may be easier. In the case of cooperation in the interception of data transmissions to track down suspects this is already true. However, one must recall the statement made by the International Telecommunications Union that cooperation and regulations for interception of data is firmly in place, but the same cannot be said for device forensics (International Telecommunications Union, 2009). When examining the International Co-operation in Criminal Matters Act one can perhaps surmise that applying them to digital evidence is not too far afield. And the ratification of ISO Standard 27037:2012 on the collection and preservation of digital evidence will contribute to this end.

The comparison revealed that the evidence laws are similar or at least not dissimilar enough to cause issue in court. Both Namibia and South Africa share the Law of Evidence Amendment Act 45 of 1988. In it, evidence can be witnesses, real evidence or documents. The ECT Act 25 of 2002 corrected the term “document” to include those

created by a computer. The U.S. Federal Rules of Evidence (FRE) were not significantly impacted by the update to the FRCP done in 2006.

Hearsay rules and exceptions were similar among the three nations; however, it is unclear how much discretion is given to the courts when determining evidentiary weight. Hearsay in each nation is denied straightaway unless an exception applies. Because so much business is conducted via email, text messages, instant messages and other electronic-based forms of communication, separating “real computer evidence” from “hearsay computer evidence” remains an issue in each of the case studies.

The most striking variance involves privacy laws and the evidence illustrates that they vary sharply. Both South Africa and Namibia have privacy written into their constitution which includes privacy of communication and correspondence. An additional complication in the case of the U.S. is that privacy laws of each state can vary. Specifically, California and Montana along with other states have privacy written into their state constitutions. Such laws affect digital investigators within the U.S. and the privacy laws of other nations affect any investigations abroad.

The experts interviewed brought up key points. Ms. Scheuermann stated that the U.S. government expects the corporations to deal with the privacy issues in foreign locales. Many multinational companies now have global privacy departments to address such issues. Mr. Godfrey brought out the fact in one instance that even if it is company property, because an employee may have been using the corporate computer for limited personal use, privacy laws come into play. It can even have the effect of denying a foreign investigator from viewing the contents. It can be concluded that privacy will be

an issue that must be addressed. In the case of the company MegaUpload (as discussed in Chapter Two), the New Zealand High Court ruled that the search and seizure of items that were later shared with the FBI was unconstitutional (Jones, 2012). The FBI received the evidence from a legal entity – the New Zealand police - so even though the High Court has demanded the return of the evidence, it may be more a matter of courtesy than law that requires the return of same.

The next hypothesis is that variances between states in the U.S. would mirror what could be found when examining differences between countries. The differences in privacy laws, licensing of digital forensic investigators, computer crime, penalties associated with same, and the printing of ESI for court all are variances with the U.S. Six years ago Namibia required that all electronic evidence (ESI) be printed for presentation in court as well (Ludik, 2006). It might be advantageous to map countries to states in an attempt to see what would be the best approach to take if dealing with a case in that jurisdiction.

In the original questions it was put forth that there would be pivotal cases in each country that caused changes in laws or interpretation thereof. The investigation has certainly shown this to be true. In South Africa, the case of *Narlis v the South African Bank of Athens* in defining what a document was prompted a change in the definition of the term. Then later cases which showed the inaccuracy of the interpretations of that new definition urged the creation of the ECT Act 25 of 2002 for clarification (South African Law Reform Commission, 2010). The definition of “eavesdropping” as a result of the *Olmstead* case is very similar. The definition of theft of computer data as opposed to

merely copying it led to the creation of the Computer Fraud and Abuse Act . In the U.S., cases such as Enron caused the creation of Sarbanes-Oxley. It is also true that the sheer weight of circumstance has forced a change or a response. For example, the amount of e-discovery prompted the DOJ spell out to create guidelines for criminal e-discovery (Koblentz, 2012). In examining other nations, targeting such cases might be advantageous in understanding how items are interpreted.

Next it was assumed there would be similar cases in each country which demonstrated that each country was dealing with similar issues. While the cases themselves did not bear this out, the situations did. For example, hearsay is an issue in each of the three countries in regards to digital communications. Admissibility of evidence is of concern in any jurisdiction. However, because it has been shown in this investigation that the rules and/or laws of evidence are similar, that is not where the challenge lies.

Another hypothesis that emerged during the gathering and comparison of data was that countries would be dissimilar in sanctions and ramifications applied in computer crimes. The prime example of ramifications was in regards to extradition. The court in South Africa stated that if a citizen had merely defaced a website as opposed to embezzling money or wire fraud, they would not allow the extradition of that citizen. Each of the three nations in the study relies upon extradition treaties with reciprocity to turn suspects over to another nation. Justice Mainga stated that in many cases such as the man charged with rape in France, conditions would have to be met by the requesting country before the person would be turned over (Mainga, 2012). In that particular case,

the man had been convicted in absentia. That ruling had to be overturned before Namibia would proceed. Note that at the writing of this document, his case was still under appeal.

The last hypothesis is in regards to the digital forensics investigator. As Maat found in her survey, it is agreed that digital forensics is a highly specialized field (Maat, 2009). The original statement in chapter four was that the requirements would vary and most likely would be established by software vendors. This hypothesis cannot be answered definitively. The requirements for a digital forensics investigator vary state by state and country by country. As pointed out by Expert Four, it is also in a state of flux (G. Sorebo, private correspondence, 2012). Expert Two states that the requirements he sees are that the investigator must show what type of training he or she has had, what level of experience, how many declarations for court have he/she done and how many times have she/he appeared as an expert witness (R. Godfrey, private interview, 2012). Justice Mainga stated that he did rely on the experts to present the evidence. He also stressed that they prove they followed the standard procedure that exists (S. Mainga, private interview, 2012). Dr. Kessler cited a case in which a renowned forensics expert was challenged by the opposing counsel because he did not have a private investigator's license, shows how unreasoning situations can become (G. Kessler, private interview, 2012). In Ngomane's thesis, it was brought out that lack of experience by a digital forensic investigator could render evidence unusable for court (Ngomane & Horne, 2010). Dr. Ludik, in relating the case in Namibia, illustrated how inexperienced investigators allowed the suspect to alter the evidence by not following forensic

procedures (P. Ludik, private correspondence, 2012). Training and certification of digital forensics experts is paramount, but not one easily solved.

So the query becomes, can the original three questions posed in chapter one be answered based on this investigation? The answer to the first question can be analyzed from a variety of positions: Can data collected elsewhere be used in one's own court? Based on the response from Expert One, given the conditions that proper forensic procedures and precautions were used and documented the answer would be yes (S. Scheuermann, private correspondence, 2012). Ms. Scheuermann has evidence shipped physically or via the network for analysis. The agreements that exist for criminal cases such as the International Co-operation in Criminal Matters Act both in Namibia and South Africa along with the Mutual Legal Assistance Treaties of the U.S. spell out guidelines for acquiring foreign evidence. In the Criminal Procedures Act, Namibia and South Africa state how evidence from a foreign court will be admitted (South African Government, 1977). If conditions are met such as an affidavit that it was collected properly and to the authenticity of the evidence, then the answer is yes.

For the answer to the second question- if the case is being tried in one's own country what conditions must be met in the collection of evidence elsewhere to be presented here, one first must also look at the responses from the corporate experts. Expert Two has had two situations: 1) where the forensic drive image was shipped to him and 2) where he had to obtain the evidence in a foreign country, analyze in his own country and then present it before a foreign labor board. These scenarios would apply in civil cases and indicate that yes, the if evidence is collected properly and procedures

followed, the evidence can be used In criminal cases, again, the International Co-operation in Criminal Matters acts or similar legislation would dominate the discussion.

The third question focuses on the professional requirements for the digital forensic investigator. On an international level, how does one qualify the digital forensics investigator and how do you qualify them for use in another jurisdiction? In many instances, the only training venue is through the software vendors or through international law enforcement organizations. For example, the International Association of Computer Investigative Specialists (IACIS) provides certification but only to law enforcement and government employees. The civilian equivalent of IACIS is the International Society of Forensic Computer Examiners (ISFCE) and they also provide certification. The SANS Institute (SysAdmin, Audit, Network Security) also provide training and tests. So the question becomes who can take the exams and what does it qualify them to do? For example, people who are certified under a particular vendor may not have a thorough understanding of the underlying concepts or theory. And then it becomes a question of “how deep an understanding of the theory is needed to apply it effectively and accurately?” In the next section, the challenges relating to this are examined.

Challenges

One of the biggest challenges facing digital forensics does not have to do with the laws, the rules, international agreements or treaties. It does, however, have to do with people and proper training. An unanswered question in this investigation is the acceptability of the forensic investigator. Because the licensing and certifications of

digital forensics experts occurs at the state level, each state in the U.S. is free to have its own interpretation and requirements. As a result, the requirements vary state to state (Phillips & Nance, 2010). Educating those in the legal profession, including the paralegals, the attorneys, and the judges is also a challenge (Nance & Ryan, 2011). Mr. Godfrey stated that his best cases are when he spends time educating the paralegals and attorneys involved so that they understand what digital forensics is and how the information is obtained (R. Godfrey, personal interview, 2012). ISO Standard 27037:2012 has now established the skill sets needed by a Digital Evidence First Responder. It also

In his dissertation, Kessler concluded that the forensics expert must educate the judge as to what digital forensics is and how it is done. “The overriding educational theme that came out of this research is to remove the mystery about digital evidence” (Kessler, 2010). In speaking with others, even those in the IT field, responses such as “digital forensics is so cerebral” is common. People assume they cannot understand it. Proper education of the forensics investigators and teaching them how to convey the information to those in the legal profession is paramount.

In the U.S. there is the emergence of National Centers for Digital Forensic Academic Excellence (CDFAE) complete with learning objectives that can be mapped and assessed. This type of mapping could be a step towards establishing a national standard that could be used in both civil and criminal cases. Several pilot programs have already been accredited by the U.S. Department of Defense Cyber Crime Center including one at Anne Arundel Community College (“Honored for Forensics,” 2012). The work already done by the International Competition Network in assembling a

manual for digital evidence gathering and a methodology for search and seizure along with how to conduct raids covering over 90 international jurisdictions points to a solution (International Competition Network, 2010).

Implications and the Way Forward

In the case of digital crimes, there is much work left to be done. As discussed in the previous section, education and training of more digital forensics examiners in all nations is needed. Mr. Godfrey stated – “We cannot afford to have digital forensics investigators in every country in which we are operating” (Godfrey, 2012). In nations such as South Africa and Namibia education begins with courses such as those offered at University of Cape Town and the Polytechnic of Namibia.

The database that has been created as part of this dissertation investigation should be expanded upon, further populated, and perhaps maintained as an open source or similarly maintained and updated project. The tables that have been used throughout this dissertation are the compilation of data that exists in books, on websites, etc., but not in an electronic format that is easily updated or accessible. For example, one has to go to one website to find that state’s criminal laws and then click back and forth for each state. The same is true for state privacy laws and computer crime laws. Consider how much easier and more efficient it would be if that information were in one database that could be easily queried. This could be done not only for the case studies in this research, but for other countries as well. The Appendices at the end of this document details the database that could be put on the web and updated by a team or multiple teams for use globally.

It would be advantageous to create the mapping of the criminal laws and their relevant sections as was done in Table 6 along with similar mapping of the rules of evidence, rules of civil procedure, etc. for common law countries. And based on the conclusions drawn in Section A of this chapter, most common law countries should have similar constructs for their civil and criminal proceedings. The mapping of countries to individual states of the U.S. that have similar laws could aid in presenting a case or administering an electronic evidence case with ties abroad.

The focus of this paper has been narrow to arrive at the grounded theory. The next step would be to apply the same logic to the European Union and perhaps involve the Convention on Cybercrime. The other focus of the paper has been common law countries. The investigation and analysis of a similar nature should be done with civil law countries such as Japan, France and Norway who do not employ case law to address laws that do not currently exist such as when dealing with new technology. The most challenging would likely be countries such as China with a mixture of civil and socialist law. Other nations may be ruled by religious law or combinations of religious, civil, or socialist. Whether they have similar constructs or areas in which agreements or parallels are easily ascertained is a topic for future research.

A concern that international students studying in the U.S. have is that learning the laws that affect cases in the U.S. will not be of any use when they return home. By proving that the primary difference is in the privacy laws along with the fact that countries such as South Africa and Namibia use case law from the U.S. or Canada or

others if it does not exist in their country indicates higher similarities than most assume (Mainga, 2012). And that their education abroad is beneficial.

Privacy of the individual will continue to play a significant role in dealing with digital evidence. While countries such as Namibia and South Africa have privacy of communications built into their constitutions, the interpretation of definitions by the legal profession remains a challenge. The recent events around the Electronic Communications Privacy Act in the U.S. expose several loopholes regarding email and email drafts. A large section regarding privacy has been left out of this investigation and that is the privacy of medical records. The push to place medical records online in the U.S. was introduced in Chapter Two, but what effect will that have on digital forensics examinations and privacy? What happens to international worker's records?

The cloud (introduced in Chapter Two) offers yet another level of complexity when discussing jurisdiction. When discussing the Internet, the cloud can exist as a public, private, community or hybrid deployment. People who use conveniences such as Gmail, DropBox or GoogleDocs are using the cloud. Since the cloud crosses multiple jurisdictions, not only in the locality sense but in the global sense of the word, how will each country approach this issue? The cloud providers may have server farms in more than one country and have an obligation to abide by the laws of each country. As has already been experienced by companies with branches in various countries conducting digital investigations, the laws and accepted procedures vary (Phillips et al, 2014). Is the jurisdiction determined on where the company or suspect is located? Or do you apply the South African law if it has an effect in the Republic?

Live Forensics is going to grow in importance as a result of the cloud. Until the last few years, digital forensics has relied upon taking a forensic image of a “dead” machine or one that has been powered off. Taking a server offline to take a forensic image is impractical in many instances. For example, if a small credit union were to take its primary server offline for the amount of time needed to make a forensic image, their clientele would be unable to access much of their information.

The issue concerning live forensics is twofold: 1) the data may be changing as the evidence is being gathered and 2) the evidence gathering act in itself may alter the evidence. This violates one of the fundamental premises of forensic science – that the results can be reproduced. Also, since many of the servers are virtual machines, reliance upon snapshots (Shende, 2010) poses the issue of how often the snapshots are taken and that they may only be good for the last fifteen minutes. Live forensics, especially in a dynamic environment such as the network cloud, cannot be reproduced or at least not in the way currently viewed at the time of this writing.

In each country the legal systems use hyper-refined criteria to pursue or justify their actions. The definition of the term “document” in South Africa and now the definition of “stored communications” in the U.S. indicate that new technology and changing lifestyles are challenging the interpretation of many laws and acts. As the citizens of the world become more and more global in nature, a better understanding of how to address the evidence on cellphones, tablets, cloud based storage, corporate email and mobile devices remains an issue. The database that has been created as a result of this dissertation includes tables containing of countries, federal / country laws and statutes,

federal rule sections or subsections, state laws, states / provinces and case law. The granularity of the mapping will be a benefit to those in the field.

In closing, this investigation has achieved much of what it started out to accomplish. By lifting the veil on what is and is not true regarding what, work can begin on the dilemmas listed above. The limitations on the results of this research are time and the rapid pace at which technology advances. Countries that don't have a handle on this should take heed. As the field of digital forensics grows, the digital forensic professionals will find themselves in a similar predicament as real estate agents find themselves in which they cannot give legal advice, but they had best know it to carry out their job.

“Sometimes the questions are complicated and the answers are simple.”

— *Dr. Seuss*

REFERENCES

- ACLU. (2012). ACLU Sues DC Police Officer. *ACLU of the Nations Capitol*. Retrieved September 10, 2012, from <http://aclu-nca.org/docket/aclu-sues-dc-police-officer-for-stealing-citizen%E2%80%99s-smartphone-memory-card>
- Angwin, J. (2012). FBI v Google - The legal fight to unlock smartphones. *Wall Street Journal*. Retrieved October 10, 2012, from <http://online.wsj.com/article/SB10001424052702303644004577524790015525450.html>
- BBC News. (2012). South Africa Profile. *BBC News*. Retrieved on 9 April 2012, from <http://www.bbc.co.uk/news/world-africa-14094918>
- Beebe, R. M., & Senkewicz, R. M. (2001). *Lands of Promise and Despair; Chronicles of early California, 1535-1846*. Santa Clara: Santa Clara University.
- Birks, M., & Mills, J. (2010). *Grounded Theory: A Practical Guide* (pp. 1-14). London: Sage Publications.
- Brenner, S. (2010). Passwords and the 5th Amendment Privilege. Retrieved on 12 June 2011, from <http://cyb3rcrim3.blogspot.com/2010/04/passwords-and-5th-amendment-privilege.html>
- Brown, J. (2012). Oregon court finds cell phone not closed container. *CyberCrime Review*. Retrieved March 6, 2013, from <http://www.cybercrimereview.com/2012/01/court-finds-camera-not-closed-container.html>
- Burd, S. D., Seazzu, A. F., & Jones, D. (2011). Bridging Differences in Digital Forensics for Law Enforcement and National Security. *Proceedings of the 44th Hawaii International Conference on System Sciences - 2011*.
- CESPAM. (2007). CESPAM EXECUTIVE TRAINING PROGRAMME: Combating Cybercrime in the SADC Region Report on the Seminar held in Cape Town, South Africa 23. *Seminar*.
- California Legislature. (n.d.). California Constitution. Retrieved 19 August 2012, from <http://www.leginfo.ca.gov/const-toc.html>
- California v. Acevedo. 500 U.S. 565 (U.S. Supreme Court. 1991).

- Casey, E. (2011). *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet* (3rd ed., p. 807). Waltham, MA: Elsevier.
- Cassim, F. (2010). Addressing the Challenges posed by Cybercrime : a South African Perspective. *Journal of International Commercial Law*, 5(3), 118-123.
- Charles Katz v. U.S. 389 U.S. 347, (U.S. Supreme Court 1967).
- Ciocchetti, C. (2001). Monitoring Employee Email - Efficient Workplaces vs. Employee Privacy. *Duke Law and Technology Review*, 0026.
- Coates, S. (2005). Rader Gets 175 Years for BTK Slayings. *The Washington Post*. Retrieved 16 February 2011, from <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/18/AR2005081800201.html>
- Cohen, A., & Lender, D. (2012). *Electronic Discovery Law and Practice* (2nd ed.). New York: Wolters Kluwer Law & Business.
- Constitution of the Republic of Namibia. (1990).
- Corner, S. (2011). Australia wants to join European cybercrime convention. Retrieved 25 February 2011, from <http://www.itwire.com/it-policy-news/regulation/45260-australia-wants-to-join-european-cybercrime-convention>
- Council of Europe. (2001). Convention on Cybercrime. *European Treaty Series*, (185).
- Cyanre. (2013). Cyanre: the Computer Forensics Lab. Retrieved 14 March 2013, from <http://www.cyanre.co.za/>
- Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (U.S. Supreme Court, 1993)
- DHS/Office for Civil Rights and Civil Liberties. (2012). Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Retrieved July 6, 2012, from <http://www.it.ojp.gov/default.aspx?area=privacy&page=1284>
- Department of Justice - Republic of South Africa. (2011). International Legal Relations. Retrieved July 22, 2012, from <http://www.justice.gov.za/docs/emlatreaties.htm>
- Donato APONTE-NAVEDO, et al., Plaintiffs v. NALCO CHEMICAL COMPANY, et al., Defendants. 268 F.R.D. 31 (United States District Court, D. Puerto Rico, 2010).
- Donn Olson v. Michael Reynolds. (2012).

- EDRM LLC. (2011a). Collection Guide - The EDRM. Retrieved 29 January 2012, from <http://www.edrm.net/resources/guides/edrm-framework-guides/collection>
- EDRM LLC. (2011b). Information Governance Reference Model (IGRM). Retrieved 29 January 2012, from <http://www.edrm.net/resources/guides/igrm>
- ENFSI Working Group Forensic IT. (2006). *GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY v. Practice* (pp. 1-28).
- Esselaar, S., Gillwald, A., Moyo, M., & Naidoo, K. (2010). South African ICT Sector Performance Review 2009/2010. *Towards Evidence-based ICT Policy and Regulation Volume Two, Policy Paper 6, 2010*.
- Family Health International. (2005). *Qualitative Research Methods* (p. Module 1). Retrieved 26 June 2012, from <http://www.fhi360.org/sites/default/files/media/documents/Qualitative%20Research%20Methods%20-%20A%20Data%20Collector%27s%20Field%20Guide.pdf>
- Farlex Inc. (2005). Common Law. Retrieved July 24, 2012, from <http://legal-dictionary.thefreedictionary.com/Common+law>
- Faust, E. (1955). History of Human Parasitic Infection. *Public Health Reports (1896 - 1970)*, 70, 10.
- Federal Evidence Review. (2012). 1975 FRE Original Enactment Legislative History Page. Retrieved July 6, 2012, from <http://federalevidence.com/node/574>
- Federal Judicial Center. (n.d.). *Olmstead v. United States: The Constitutional Challenges of Prohibition Enforcement — Historical Background and Documents*. Retrieved July 1, 2012, from http://www.fjc.gov/history/home.nsf/page/tu_olmstead_narrative.html
- FindLaw. (1969). *Chimel v. California*. Retrieved July 3, 2012, from <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=395&page=752>
- FindLaw. (2012). State Computer Crimes Laws. Retrieved July 3, 2012, from <http://law.findlaw.com/state-laws/computer-crimes/>
- Florida v. Wells. 495 U.S. 1 (U.S. Supreme Court. 1990).

- Frieden, J., & Murray, L. (2011). THE ADMISSIBILITY OF ELECTRONIC EVIDENCE UNDER THE FEDERAL RULES OF EVIDENCE. *Richmond Journal of Law and Technology*, XVII(2). Retrieved 5 March 2012, from <http://jolt.richmond.edu/v17i2/article5.pdf>
- Gangalaramsamy, N. (2010). CyberSecurity in Africa. Retrieved February 17, 2011, from <http://www.docstoc.com/docs/42694998/Cyber-Security-in-Africa-%28Law-Enforcement%29-Mauritius>
- Garrie, D. B., Armstrong, M. J., Adler, E., Burdett, W. R., & Routt, T. J. (2002). Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act. *LegalThinkTank.com*, 1-41.
- Gillers, S. (2004). Multijurisdictional Practice of Law: Merging Theory with Practice. *The Bar Examiner*.
- Goeiman, F. (2012). Kobi Extradition Hearings Resume. *The Namibian Sun*. Retrieved September 10, 2012, from <http://www.namibiansun.com/content/national-news/kobi-extradition-hearing-resumes>
- Grobler, M. (2010). Digital Forensics Standards: International Progress. *Proceedings of the South African Information Security Multi-Conference*.
- Grobler, M., & Dlamini, I. (2010). MANAGING DIGITAL EVIDENCE – THE GOVERNANCE OF DIGITAL FORENSICS. *Council for Scientific and Industrial Research*.
- Gross, G. (2012). Supreme Court Justices question surveillance secrecy.pdf. *ComputerWorld*.
- Guidelines. (n.d.). How to write a case study, 1-7, Retrieved on 14 October 2012, from <http://www.gttp.org/docs/HowToWriteAGoodCase.pdf>
- Guynn, J. (2012). Petraeus case triggers concerns about Americans' online privacy. *Los Angeles Times*. Retrieved November 16, 2012, from <http://www.latimes.com/business/technology/la-fi-tn-petraeus-online-privacy-20121114,0,2491543.story>
- Hamilton, A. B. (2011). Spotlight on Women Cyberseminar Series What is GroundedTheory , Anyway ? *VA Womens Health Research Network*.
- Hansen, M. (2006). How the Cops Caught BTK. *ABAJournal.com*. Retrieved 14 March 2011, from http://www.abajournal.com/magazine/article/how_the_cops_caught_btk/

- Henry, R. (2011). UNPREDICTABLE AND INCONSISTENT: NEVADA'S EXPERT WITNESS STANDARD AFTER HIGGS V. STATE. *Nevada Law Journal*, 0-27.
- Hershensohn, J. (2005). I.T. FORENSICS: THE COLLECTION AND PRESENTATION OF DIGITAL EVIDENCE.
- Honored for Forensics. (2012). *The Baltimore Sun*. Retrieved November 15, 2012, from http://articles.baltimoresun.com/2012-08-02/news/bs-ar-edbriefs-0805-20120801_1_cybersecurity-studies-program-defense-cyber-crime-center-digital-forensics-academic-excellence
- Hughes, A. (2009). The Fifth Amendment and Sebastien Boucher. *Information Forensics*. Retrieved 25 March 2012, from <http://infoforensics.vidocrazor.com/2009/02/27/the-fifth-ammendment-and-sebastien-boucher-beyond-knee-jerk-response/>
- Illinois v. Lafayette. 462 U.S. 640 (U.S. Supreme Court. 1983).
- International Competition Network. (2009a). Chapter 1: Searches, Raids and Inspections. *Anti-Cartel Enforcement Manual*, (May). Retrieved 4 December 2012, from <http://www.internationalcompetitionnetwork.org/>
- International Competition Network. (2009b). ICN Factsheet and Key Messages.
- International Competition Network. (2010). Chapter 3: Digital Evidence Gathering. *Anti-Cartel Enforcement Manual*, (March). Retrieved 4 December 2012, from <http://www.internationalcompetitionnetwork.org/>
- International Organization for Standards. (2012). Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence, working document only
- International Organization on Computer Evidence. (2000). G8 Proposed Principles For The Procedures Relating To Digital Evidence, (March 1998), 1998.
- International Organization on Computer Evidence. (2002). IOCE Training and KSAs. *IOCE Training and KSAs, 1.0*(May), 1-8.
- International Records Management. (2002). Evidence-Based Governance in the Electronic Age Case Study - Legal and Judicial Records and Information Systems in South Africa.
- International Telecommunications Union. (2009). Understanding Cybercrime: A Guide for Developing Countries.

- Internet Law Treatise. (2010). Privacy: Searching and Seizing Computers. Retrieved July 23, 2012, from http://ilt.eff.org/index.php/Privacy:_Searching_and_Seizing_Computers
- ISO/IEC 27037 ISO / IEC 27037:2012(E) Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence (2012).
- Jones, B. (2012). Megaupload Search Warrants Ruled Illegal by High Court. Retrieved June 28, 2012, from <http://torrentfreak.com/megaupload-search-warrants-ruled-illegal-by-high-court-120628/>
- Josephy, A. (1994). *500 Nations - An Illustrated History of North American Indians*. New York.
- Joymungul, S. P. (2008). Digital Forensics –Challenges in Solving Cyber Crimes in African Countries. Johannesburg, S.A.: Cyber Crime Summit 2008.
- Kadlec, D., Weisskopf, M., & Zagorin, A. e. (2002, Jan 13). *Enron: Who's Accountable?* Retrieved Nov 20, 2011, from Time Magazine: <http://www.time.com/time/printout/0,8816,1001636,00.html>
- Kanita, W. S. (2008). NAMIBIAN ECT BILL & COMPUTER BREACHES. *School of IT*. Windhoek Namibia: Polytechnic.
- Kerr, O. S. (2005). SEARCH WARRANTS IN AN ERA OF DIGITAL EVIDENCE. *Mississippi Law Journal*, 75.
- Kessler, G. C. (2008). Purpose of P. I. Licensure. *CDFSL*.
- Kessler, G. C. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. *Graduate School of Computer and Information Sciences*. Nova Southeastern University.
- Kleiman, D. (n.d.). Digital Forensics: DFCB and the ABA Resolution. Retrieved 14 October 2012, from <http://www.computerforensicsexaminer.com/computer-forensics-expert-florida-miami-palm-beach-lauderdale-dave-kleiman-forensic-training-files/Digital%20Forensics%20DFCB%20and%20the%20ABA%20Resolution.pdf>
- Koblentz, E. (2012). DOJ Lays Down the Law on Criminal Evidence. Retrieved 20 November 2012, from <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202542777740&slreturn=1>

- Kravets, D. (2012). House Approves Sweeping , Warrantless Electronic Spy Powers. *Wired Magazine*. Retrieved Dec. 12, 2012, from <http://www.wired.com/threatlevel/2012/09/house-approves-spy-bill/>
- Laura Zubulake v UBS Warburg LLC, UBS Warburg, and UBS AG. 229 F.R.D. 422 (S.D.N.Y. 2004).
- Laws.com. (2011). Easy Guide to Understanding ENRON Scandal Summary. Retrieved 30 September 2012, from <http://finance.laws.com/enron-scandal-summary>
- Legal Assistance Reform Centre. (2010). NAMLEX - INDEX TO THE LAWS OF NAMIBIA. Windhoek.
- Legal Information Institute. (2009). Arizona v. Gant. Retrieved 14 October 2012, from <http://www.law.cornell.edu/supct/html/07-542.ZO.html>
- Lekala, A. R. (2011). E-mail Communication for Provisional Sentence Summons. *Journal of International Commercial Law and Technology*, 6(3), 145-150.
- Liptak, A. (2012). Supreme Court Ruling Allows Strip Search for Any Arrest. *The New York Times* 2. Retrieved November 1, 2012, from http://www.nytimes.com/2012/04/03/us/justices-approve-strip-searches-for-any-offense.html?pagewanted=all&_r=0
- Maat, S. (2009). CYBER CRIME A COMPARATIVE LAW ANALYSIS. *Communications*.
- Mason, E. (2009). HIGHLY USEFUL TIPS FOR CASE STUDY DISSERTATION. Retrieved 14 January 2013, from <http://www.articlesbase.com/college-and-university-articles/highly-useful-tips-for-case-study-dissertation-1492680.html>
- Mason, S. (2008). *International Electronic Evidence*. London: British Institute of International and Comparative Law.
- Mason, S. (2010). *Electronic Evidence*. (S. Mason, Ed.). LexisNexis, Butterworths.
- McRoy, R. G. (n.d.). Qualitative Research. Retrieved February 11, 2013, from www.uncp.edu/home/marson/qualitative_research.html
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*.

- Menges, W. (2012). Extradition request on 1991 rape charge. *The Namibian Sun*. Retrieved October 10, 2012, from [http://www.namibian.com.na/index.php?id=28&tx_ttnews\[tt_news\]=94467&no_cache=1](http://www.namibian.com.na/index.php?id=28&tx_ttnews[tt_news]=94467&no_cache=1)
- Meyers, M., & Rogers, M. (2004). Computer Forensics: The Need for Standardization and Certification. *International Journal of Digital Evidence*, 3(2).
- Mirchin, D. (2011). Israeli privacy update. *The Privacy Advisor - IAPP*. Retrieved 14 December 2011, from https://www.privacyassociation.org/publications/2011_12_05_israeli_privacy_update_landmark_case_establishes_guidelines_for
- Montana Legislature. (2011). Montana Code Annotated. Retrieved 16 October 2012, from http://leg.mt.gov/bills/mca_toc/index.htm
- Myfundi.co.za. (2011). The History of South African Law. *Myfundi - Your Online Encyclopedia*. Retrieved 24 June 2012, from http://myfundi.co.za/e/History_of_the_South_African_Law#European_ius_commune_or_common_law
- NIST. (2001). General Test Methodology for Computer Forensic Tools. (U.S. Department of Commerce, Ed.).
- NIST. (2010). *Computer Forensics Tool Testing Program*. Retrieved April 1, 2011, from NIST - Information Technology Laboratory: <http://www.cftt.nist.gov/>
- Namibian Parliament. (1995). Foreign Courts Evidence Act. *Government Gazette*, (2).
- Namibian Parliament. (2003). THE COMPUTER MISUSE AND CYBERCRIME ACT 2003.
- Namibian Parliament. (2004). The Criminal Procedure Act, (25).
- Nance, K., & Ryan, D. (2011). Legal Aspects of Digital Forensics: A Research Agenda. *44th Hawaii International Conference on System Sciences*.
- Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations* (Fourth., p. 682). Boston, MA: Course Technology, Cengage Learning.

- New York Criminal Law and Procedure. (2009). Inventory Searches: The Factual Predicate. Retrieved July 7, 2012, from <http://www.nycrimblog.com/nycrim/2009/01/inventory-searches-the-factual-predicate.html>
- Ngak, C. (2012). Email privacy : What Petraeus needed to know. *CBSNews.com*. Retrieved November 16, 2012, from http://www.cbsnews.com/8301-205_162-57549755/email-privacy-what-petraeus-needed-to-know/
- Ngomane, A. R., & Horne, J. S. (2010). *The Use of Electronic Evidence in Forensic Investigation*. Pretoria, S.A.: University of South Africa.
- Office of the Prime Minister. (1996) Namibian Extradition Act.
- Office of the Prime Minister. (2000). International Co-operation in Criminal Matters Act 9 of 2000. *Government Gazette of the Republic of Namibia*.
- Office of the Prime Minister. (2010a). Use of Electronic Transactions and Communications Bill.
- Office of the Prime Minister. (2010b). Public Notice on ECT Bill.
- Overly, M. (2004). *Overly on Electronic Evidence in California* (p. 436). West, a Thomson Company.
- Parliament of South Africa. (2002). ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 of 2002. Retrieved 4 March 2011, from <http://pol.mcm.co.za/html/govdocs/legislation/2002/act25.html>
- Phillips, A., & Nance, K. (2010). Computer Forensics Investigators or Private Investigators: Who is Investigating the Drive. *Systematic Approaches to Digital Forensic Engineering*. Oakland, CA: IEEE/SADFE.
- Phillips, A., Godfrey, G., Steuart C., Brown, C. (2014). *E-Discovery: An Introduction to Digital Evidence*, Cengage Publishing, Boston MA ISBN 9781111310646
- Pistorius, T. (n.d.). SYMPOSIUM DRAFT USE OF ELECTRONIC TRANSACTIONS AND COMMUNICATIONS BILL FOR NAMIBIA. Retrieved 19 April 2012, from http://209.88.21.36/opencms/export/sites/default/grnnet/OPM/downloadable_resources/201009Use_of_ETC_Act_part_I.pdf
- Privacy International. (2004). Silenced South Africa. Retrieved 28 September 2012, from [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-103781](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103781)

Rathmell, L., & Valeri, A. (2002). *Handbook of Legislative Procedures of Computer and Network Misuse in E.U. Countries*. UK: Rand Europe.

Republic of South Africa. (1999). *CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA*.

Robbins Religious and Civil Law Collection. (n.d.). *The Common Law and Civil Law Traditions*. *School of Law, University of California at Berkeley*. Retrieved July 1, 2012, from <http://www.law.berkeley.edu/library/robbins/CommonLawCivilLawTraditions.html>

Romero, S., & Atlas, R. (2002). *Worldcom's Collapse: The Overview; Worldcom Files for Bankruptcy; Largest U.S. Case*. *New York Times*. Retrieved 23 June 2012, from <http://www.nytimes.com/2002/07/22/us/worldcom-s-collapse-the-overview-worldcom-files-for-bankruptcy-largest-us-case.html>

Rothstein, B., Hedges, R., & Wiggins, E. (2007). *Managing Discovery of Electronic Information: A Pocket Guide for Judges*. (F. J. Center, Ed.).

Rustad, M. (2009). *Internet law* (p. 457). St. Paul, MN: West - Thomson Reuters.

S v Mashiyi And Another 2002. 2 SACR 387 (South Africa 2002).

S v Mdlongwa 2010. (2) SACR 419 (SCA) (South Africa, 2010).

S v Ndiki And Others 2008. (2) SACR 252 (Ck) (South Africa, 2008).

S v Teek. (1) NR 127 (SC) (Namibian Supreme Court, 2009).

S v. Koralev and Another 2006. (2) SACR 298 (N) (South Africa, 2006)

Schatz, B. (2007). *Digital Evidence: Representation and Assurance*. *Information Technology*. Queensland University of Technology.

Schroeder, S. (2012). *The Lure*. Boston, MA: Course Technology, Cengage Learning.

Sedona Conference. (2011). *The Sedona Conference*. Retrieved March 15, 2011, from The Sedona Conference: <http://www.thesedonaconference.org/>

Sedona Conference. (2007). *The Sedona Principles: 2nd Edition Best Practices, Recommendations and Principles for Addressing Electronic Document Production*.

- Shende, J. (2010). Live Forensics and the Cloud – Part 1: Exploring the effects of Cloud Computing on Digital Forensics. Retrieved 15 February 2013, from <http://cloudcomputing.sys-con.com/node/1547944>
- Sorebo, G. (2009). Remote Electronic Discovery. *Digital Evidence and Electronic Signature Law Review*, (Nbr 6).
- South African Government. (1977). Criminal Procedures Act.
- South African Government. (2003). Criminal Procedures Act 51 of 1977 amended 2003.
- South African Law Reform Commission. (2010, June 30). Project 26: Review of the Law of Evidence. *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues*. South Africa: ISBN 978-0-621-389226-5.
- South Dakota v. Opperman. 428 U.S. 364 (U.S. Supreme Court, 1976).
- Stander, A., Johnston, K., Town, C., & Africa, S. (2007). The Need for and Contents of a Course in Forensic Information Systems & Computer Science at the University of Cape Town. *Issues in Informing Science and Information Technology*, 4.
- Starbuck, J. L. (2012). Redefining Searches Incident to Arrest : Gant’s Effect on Chimel. *Penn State Law Review*, 1692(2009), 1253-1280.
- Steven Warshak v. United States of America. Case 06-4092, (U.S. Court of Appeals, 6th Circuit 2007).
- Steven Warshak v. United States of America., Case 06-4092, (U.S. Court of Appeals, 6th Circuit 2008).
- Stork, D. C. (2011). M-banking the Unbanked. Retrieved 10 November 2011, from <http://www.ResearchICTAfrica.net>.
- Supreme Court of Namibia. (2007). Retrieved October 31, 2012, from <http://www.superiorcourts.org.na/supreme/default.asp>
- Supreme Court of Ohio. (2009). Warrantless Search of Cell Phone Data Barred Unless Necessary for Officer’s Safety or to Preserve Evidence. Retrieved 3 March 2013, from <http://www.supremecourt.ohio.gov/rod/docs/pdf/0/2009/2009-Ohio-6426.pdf>
- Swartz v. Indongo and Others, (A 334/2011) [2012] NAHC (Namibian High Court, 2012)
- U.S. DOJ Joint Electronic Technology Working Group. (2012). Introduction to Recommendations for ESI Discovery in Federal Criminal Cases.

- U.S. House of Representatives. (1975). U.S. Federal Rules of Evidence.
- U.S. House of Representatives. (2010). FEDERAL RULES OF CIVIL PROCEDURE.
- U.S. House of Representatives. (n.d.). Computer Fraud and Abuse Act. Retrieved from [http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_\(CFAA\)](http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA))
- U.N. Secretariat. (2010). *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*. Twelfth United Nations Congress on Crime Prevention and Criminal Justice.
- U.S. State Department. (1997). Mutual Legal Assistance in Criminal Matters Treaties. Retrieved July 7, 2012, from <http://library.findlaw.com/1997/Dec/1/127851.html>
- U.S. CERT. (2008). Computer Forensics, government document.
- U.S. Code, Title 18, Part II, Chapter 209 - Extradition (2006).
- U.S. Department of Health and Human Services. (2011). Understanding Health Information Privacy. Retrieved 30 November 2011, from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>
- U.S. Department of Justice. (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Retrieved Dec 10, 2010, from Computer Crime and Intellectual Property Section, US DOJ: <http://www.justice.gov/criminal/cybercrime/ssmanual/index.html>
- U.S. Department of Justice. (2010). Electronic Communications Privacy Act of 1986. Retrieved 17 May 2012, from <http://it.ojp.gov/default.aspx?area=privacy&page=1285>
- U.S. National Archives. (2013). The Bill of Rights. *The Charters of Freedom*. Retrieved March 5, 2013, from http://www.archives.gov/exhibits/charters/bill_of_rights.html
- U.S. Supreme Court. (2010). FEDERAL RULES OF CRIMINAL PROCEDURE. (THE HOUSE OF REPRESENTATIVES, Ed.). Washington DC.
- U.S. v. Jones. 615 F. 3d 544 (U.S. Supreme Court, 2011).
- U.S. v John Doe. 11-12268 & 11-15421 (U.S. Circuit Court of Appeals 11th Cr. 2012).
- UNECE - United Nations Economic Commission for Europe. (n.d.). Retrieved 5 December 2012, from <http://www.unece.org/cefact/edifact/welcome.html>

- USLegal.com. (2001). Inventory Search Law and Legal Definition.
- United Nations (1999) UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.
- United Nations Commission on International Trade. (2006). UNCITRAL Model Law on International Commercial Arbitration With amendments as adopted in 2006.
- United States Courts. (2012). Federal Courts. Retrieved November 2, 2012, from <http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/FederalCourtsInAmericanGovernment.aspx>
- United States v. Karo. 468 U.S. 705 (U.S. Supreme Court. 1984).
- United States v. Knotts. 460 U.S. 276 (U.S. Supreme Court. 1983).
- Valenzuela, D., & Shrivastava, P. (n.d.). Interview as a Method for Qualitative Research. *Qualitative Research*. Retrieved 21 November 2012, from <http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf>
- VenBrux, L. N. (2009). French Data Protection Authority Issues Guidelines on Pre-Trial Discovery. (C, Ed.) *Privacy and Security Law*. The Bureau of National Affairs.
- Vijayan, J. (2009). Court ruling limits electronic searches. Retrieved June 25, 2012, from http://www.computerworld.com/s/article/9137209/Court_ruling_limits_electronic_searches
- Waters, R. (2011). Privacy, technology, and the law. *DFI News*. DFI News. Retrieved June 25, 2012 from www.dfinews.com
- Watney, M. (2009). Admissibility of Electronic Evidence in Criminal Proceedings : An Outline of the South African Legal Position. *Journal of Information, Law and Technology*, 2009(May), 1-13.
- Whittaker, Z. (2013). Justice Dept. to Congress: We want greater email, Facebook, Twitter snooping powers. *ZDNet*. Retrieved March 20, 2013, from <http://www.zdnet.com/justice-dept-to-congress-we-want-greater-email-facebook-twitter-snooping-powers-7000012786/>
- Yannella, P., & Rein, A. (2009). Canada, Australia, and United Kingdom Adopt U.S.-Style Electronic Discovery. *Privacy and Data Security Law Journal*, (June), 538-544.

Zatyko, K. (2007). Commentary: Defining Digital Forensics. Retrieved 3 October 2011, from *Forensic Magazine* <http://forensicmag.com>.

APPENDIX A

DATABASE DESIGN

In the course of this investigation, the ability to be able to map the laws of each nation at a granular level emerged. A database template was created to demonstrate the way the laws of nations interlace. The ability to be able to quickly look up a country, its laws, existing case law, relevant to another country when dealing with digital evidence is a useful tool. Currently the information exists, but it is scattered and not available at this level of detail.

The database allows one to see just how the laws/rules in each country link together. Table 7²⁴ illustrates a comparison of the criminal laws of each case study. The notion of such granularity appeals to the ease with which one could relate the laws in various countries. Multijurisdictional companies, crimes and lawsuits would benefit from being able to quickly see if the laws were compatible and potentially pinpoint potential issues that could be avoided.

Several law firms in the U.S. and Australia currently host databases with case law that can be updated by others and this would follow that model. The initial entries are for the countries examined in this research. To populate it for several hundred countries would take the input of students in the field, IT staff and legal professionals. When presented to the South King County Chapter of the Washington State Paralegal

²⁴ Table 7 can be found in Chapter 6

Association (WSPA)²⁵, the response was immediate and positive. Their suggestion was to begin populating the database with Canadian and Mexican data.

Database Design

The purpose of this database was to create a resource at a level of granularity that will aid digital investigators and legal counsel when dealing with cases involving digital evidence. To accomplish this end, it is essential to start at the country level and work down to case law. Figure A1 illustrates the original concept of the database. The base table would contain the countries. As was shown in Chapter 2, each case study had laws at the federal level which contained some subsections. Each nation also has states or provinces. Of the case studies, only the United States has laws that vary per state. However, other nations share this characteristic; therefore the state laws need to be represented. And finally, because this research focuses on common law nations, case law is a critical piece.

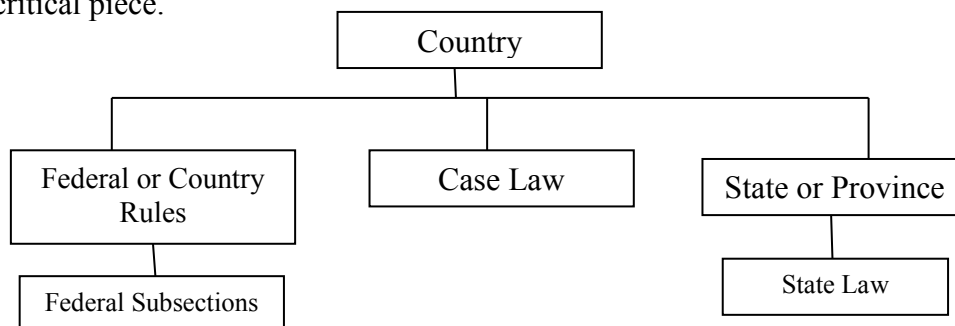


Figure A1 - Conceptual Drawing

²⁵ The Washington State Paralegal Association consists of nine geographic chapters. The South King County Chapter includes the cities of Kent, Auburn, Federal Way and Des Moines, WA.

The Entity Relationship Diagram in Figure A2 (shown on the next page) gives an overall view of the final design. The Country table has a one-to-many relationship to the Federal or Country Rules table, the State/Province table and the Case Law table. The Federal or Country Rules table has a one-to-many relationship to the State Rules table to enable mapping of the state laws to the federal laws. The Federal Rule Sections and Subsections table contains a foreign key from the Federal or Country Rules table. Note the foreign keys contained in the various tables to decrease data redundancy. Two additional tables – the Rule Type and Common Search Criteria tables – were created to expedite comparisons and searches.

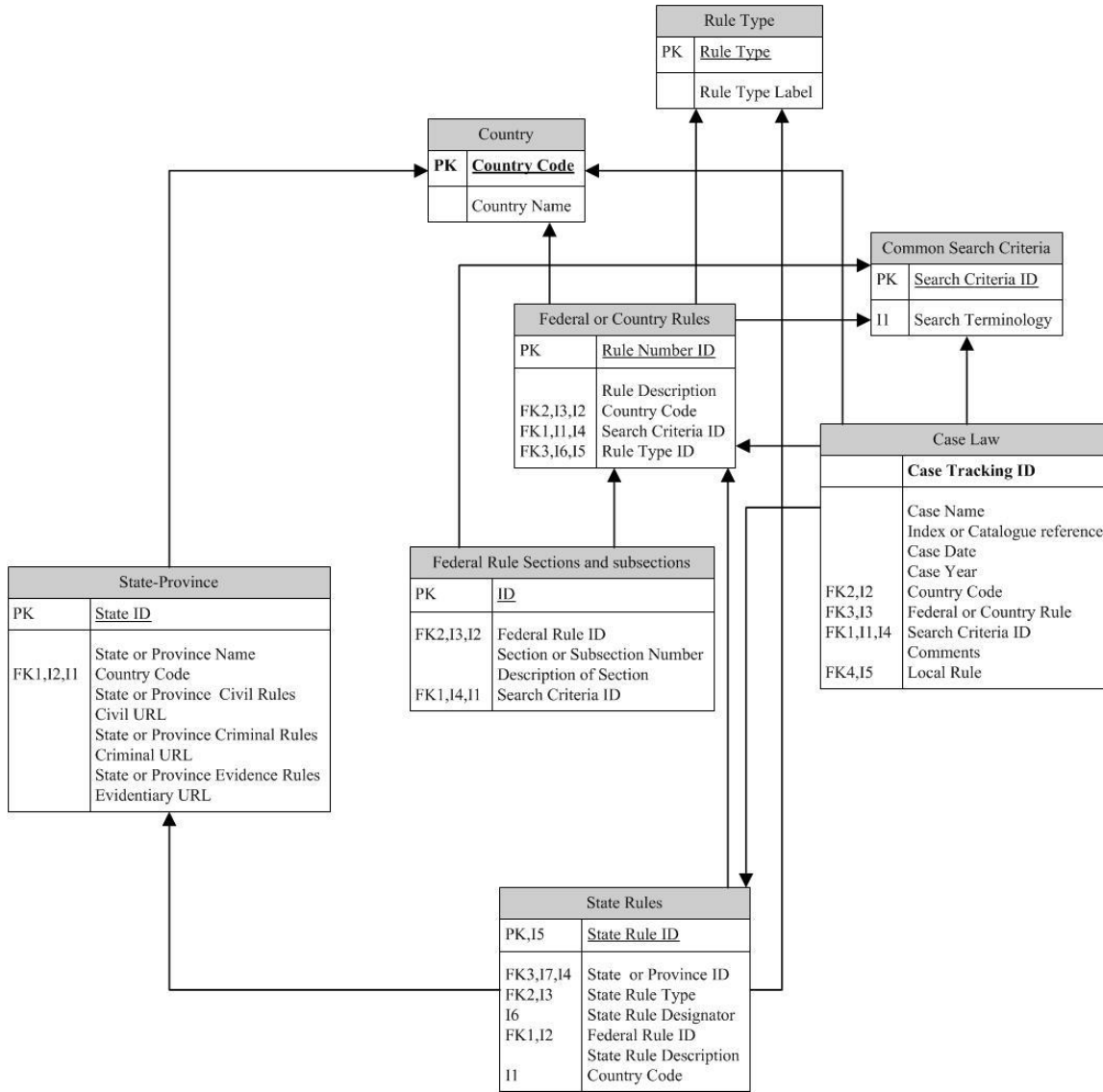


Figure A2 – Entity-Relationship Diagram

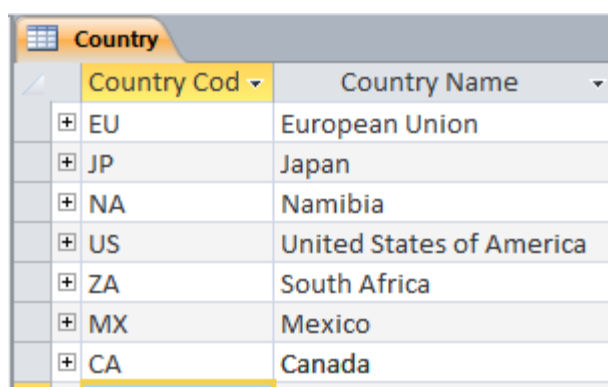
Table Descriptions and Design

To accomplish the goal of being able to access and compare the data at a granular level, the database begins at the country or federal level as was shown in the conceptual model. The Country table consists of two fields based upon ISO standard 3166 for country names and codes as shown in Table A1 (International Organization for Standards, 2012). Table A2 gives a sample of the populated Country table. For ease of reference, the table and corresponding screenshot of the populated table are grouped together below. Note that only a limited number of countries are entered in addition to the case studies.

Table A1- Country Table

Field Name	Type	Size	Description
Country Code	Text	2	Official abbreviation of country
Country Name	Text	100	Name of country

Table A2 - Country Table Data



The screenshot shows a database table named 'Country' with two columns: 'Country Cod' and 'Country Name'. The data rows are as follows:

Country Cod	Country Name
EU	European Union
JP	Japan
NA	Namibia
US	United States of America
ZA	South Africa
MX	Mexico
CA	Canada

As each country in this research has laws at the federal level, the next table created is labeled Federal or Country rules. This table consists of five fields beginning with the Rule Number ID which is the standard acronym used in that country for the rule or law as can be seen in Table A3. The third field is a foreign key from the Country Table.

The Rule Description field contains the full name of the rule for that country. For example, the Federal Rules of Civil Procedure would be spelled out here and the Rule Number ID would be “FRCP”.

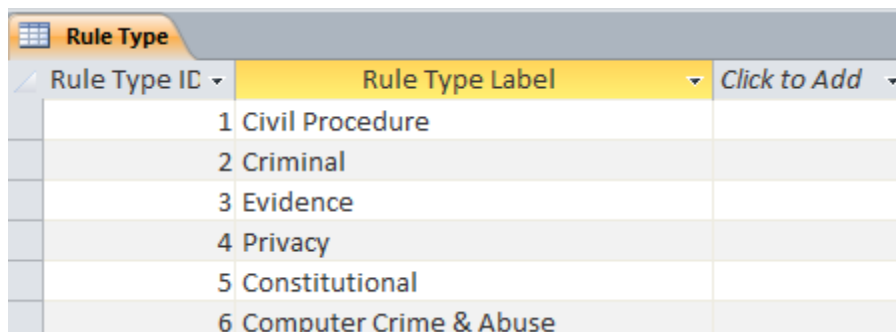
Table A3 - Federal or Country Rules

Field Name	Type	Size	Description
Rule Number ID	Text	20	Abbreviation
Rule Description	Text	255	Full Name of Rule
Country Code	Text	2	Foreign key from Country table
Common Search Term ID	Long Integer	4	Foreign key from Common Search Terms table
Rule Type ID	Integer	4	Foreign key from Rule Type table

Within the development of the database, it became apparent that searching the database would not be an easy task for someone unfamiliar with each country. One objective of the template is to make such an effort straightforward. To accomplish this, two tables were created – the Common Search Terms and Rule Type tables. Modifiability is a function of grounded theory. The creation of such tables is an example of how this database prototype can be modified as items come to the fore or change.

Table A4 - Rule Type

Field Name	Type	Size	Description
Rule Type ID	Long Integer	4	Auto numbered field
Rule Type Label	Text	25	Short description of rule type

Table A5 - Populated Rule Type Table


Rule Type ID	Rule Type Label	Click to Add
1	Civil Procedure	
2	Criminal	
3	Evidence	
4	Privacy	
5	Constitutional	
6	Computer Crime & Abuse	

Table A4 shows the makeup of the Rule Type table. It allows the data to be grouped according to the primary commonalities – specifically civil, criminal, and evidence laws – and the variances – including privacy, computer crime and abuse and constitutional laws. Table A5 shows the populated Rule Type table.

The Common Search Terms table is equally straightforward in design consisting of two fields – a key term ID which is a simple auto number field and the search terms that are common between the various laws (see Table A6). In populating the database, one needs to consider the topic or field of the search. For example, search of an arrested person, privacy in regards to communication, along with privacy in general are things one would parse the data for. A full discussion of how this table was developed can be found in Chapter Three. Table 2 in that section illustrates the conceptualization of the table. Table A7 is a screen capture of the populated table. The full table can be found in Appendix B. The selection of some items is specific to countries, such as a case that meets the Katz requirements²⁶. Such items are useful when dealing with states or

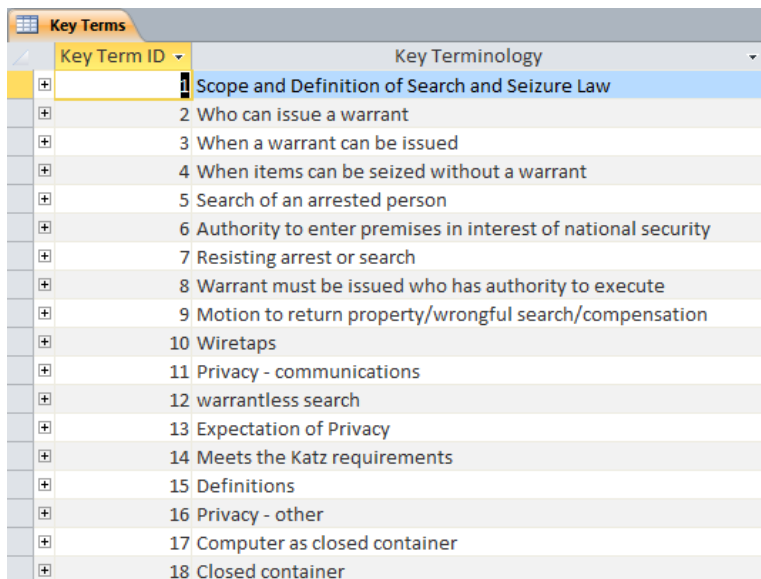
²⁶ The *Katz* case was discussed in Chapter Two and established two items with regards to privacy – 1) expectation of privacy and 2) is the expectation reasonable?

provinces. Advances in technology presented challenges to each nation as they struggled to adjust terminology to existing definitions such as the word “document” in South Africa thirty years ago. In Chapter Two, the case of *S v. Ndiki* is discussed in detail. Briefly, the term “document” was defined legally as something created by a human. Therefore machine generated documents such as bank statements were not admissible in court. As a result, the common search term “definitions” was included.

Table A6- Key Terms

Field Name	Type	Size	Description
Key Term ID	Long Integer	4	Auto number
Key Terminology	Text	60	Brief description of common items searched

Table A7- Populated Key Terms Table



Key Term ID	Key Terminology
1	Scope and Definition of Search and Seizure Law
2	Who can issue a warrant
3	When a warrant can be issued
4	When items can be seized without a warrant
5	Search of an arrested person
6	Authority to enter premises in interest of national security
7	Resisting arrest or search
8	Warrant must be issued who has authority to execute
9	Motion to return property/wrongful search/compensation
10	Wiretaps
11	Privacy - communications
12	warrantless search
13	Expectation of Privacy
14	Meets the Katz requirements
15	Definitions
16	Privacy - other
17	Computer as closed container
18	Closed container

Once the two supporting tables were populated, the Federal or Country Rule table as shown in Table A8 was populated. Determination of which common search term to link to the rule provided a clearer understanding of how the country’s laws are related.

Table A8 - Populated Federal or Country Rule Table

Federal or Country Rules					
Rule Number ID	Rule Description	Coun	Rule Type ID	Search Criteria ID	
4th Amendment	regarding unreasonable search and seizure	US	Constitutional	Scope and Definition	
5th Amendment	self incrimination	US	Constitutional	Self Incrimination	
Act 22 of 2003	Computer Misuse and CyberCrime Act	NA	Computer Crime &		
Act 57 of 1983	Computer Evidence Act 57	ZA	Computer Crime &		
Act 9 of 2000	International Co-operation in Criminal Matters	ZA	Criminal		
CFAA	Computer Fraud and Abuse Act	US	Computer Crime &		
CPA	Criminal Procedures Act 51	ZA	Criminal		
CPA 25	Criminal Procedures Act 25	NA	Criminal		
ECPA	Electronic Communications Privacy Act	US	Privacy	Privacy - communicat	
ECT Act of 2002	Electronic Communications Act 25 of 2002	ZA	Privacy	Privacy - communicat	
FRCP 16	Pretrial Conference - ESI may be in contents	US	Civil Procedure		
FRCP 26		US	Civil Procedure		
FRCP 26(f)	Meet and Confer	US	Civil Procedure		
FRCP 33	Interrogatories - option to produce business re	US	Civil Procedure		
FRCP 34	May specify form of ESI	US	Civil Procedure		
FRCP 37 (e)	Safe Harbor for routine good faith operation o	US	Civil Procedure		
FRCrP 41	Search and Seizure Rules	US	Criminal		
FRE 1002	Contents of Writings, Recordings and Photogra	US	Evidence		
FRE 1003	Contents of Writings, Recordings and Photogra	US	Evidence		
FRE 103	Rulings on Evidence	US	Evidence		
FRE 104	Preliminary questions such as whether or not	US	Evidence		
FRE 105	Limited Admissibility	US	Evidence		
FRE 106	Remainder of or Related Writings or Recorded	US	Evidence		
FRE 401	Relevancy and its Limits	US	Evidence		

Table A9 shows the states or provinces in which the State ID and Name are based on the same ISO code as the Country table. Note that under the ISO code, states are typically preceded by the country code, a hyphen or other separator, followed by the state acronym which can be up to three characters (International Organization for Standards, 2012). For example, the state of California is represented by US-CA. This limits the confusion if two different countries have states or provinces with the same name or acronym. This table also contains the name and URL link for the civil, criminal and rules of evidence for the state or province if they differ from the country. The foreign key field in the table points back to the Country Code.

Table A9 – State-Province Table

Field Name	Type	Size	Description
State ID	Text	6	Abbreviation of State or Province per ISO 3166
State or Province Name	Text	255	Maximum length due to some specific items that name organizations within regions
Country Code	Text	2	Foreign key from Country Table
State or Province Civil Rules	Text	255	Description of civil rules or official name given
Civil URL	Hyperlink		URL to state civil laws
State or Province Criminal Rules	Text	255	Description of criminal rules or official name given
Criminal URL	Hyperlink		URL to state criminal laws
State or Province Rules of Evidence	Text	255	Description of rules of evidence or official name given
Evidentiary Link	Hyperlink		URL to state rules of evidence

In populating the tables, items of interest appeared, such as Mississippi having rules of civil procedure for ESI which predates the 2006 changes to the FRCP. The database entries illustrate which states have not added amendments to their civil procedures as a result of the 2006 FRCP amendments (Cohen & Lender, 2012). Also many states rely upon federal statutes and case law and as a result, do not have laws specific to their jurisdiction. These are currently left blank. In the future a designation such as “no such rule or law” or “see federal rules” or “not applicable” may be deemed appropriate to minimize confusion by the user.

Table A10 - Populated State-Province Table

Country	State-Province		Country Cod	State or Province Civil Rules	Civil URL
State ID	State or Prov	Country Cod	State or Province Civil Rules	Civil URL	
US-CA	California	US	Code of Civil Procedure, effective 2009 similar		
US-CO	Colorado	US	none of FRCP amendments		
US-CT	Connecticut	US	Practice Book, Superior Court		
US-DC	District of Colu	US	none of the 2006 FRCP amendments		
US-DE	Delaware	US	none of the 2006 FRCP amendments		
US-FL	Florida	US	Rules for the Complex Business Litigation Divis		
US-GA	Georgia	US	none of the 2006 FRCP amendments		
US-HI	Hawaii	US	none of the 2006 FRCP amendments		
US-ID	Idaho	US	Rules of Civil Procedure effective 2006 - mode		
US-IL	Illinois	US	Supreme Court Rules - 1996, acknowledges ESI	www.state.il.us/court/SupremeCc	
US-IN	Indiana	US	Rules of Trial Procedure. In 2008, similar to 200	www.in.gov/judiciary/rules/trial_j	
US-IO	Iowa	US	Rules of Civil Procedure	www.legis.state.ia.us/DOCS/ACO/	
US-KS	Kansas	US	effective 2008, similar to 2006 FRCP	http://kansasstatutes.lesterama.o	
US-KY	Kentucky	US	none of the 2006 FRCP amendments		
US-LA	Louisiana	US	2009 follows 2006 FRCP amendments - except i	www.legis.state.la.us/billdata/str	
US-MA	Massachusetts	US	Rules of Civil Procedure - done in 2008, but do	www.massreports.com/courtrules	
US-MD	Maryland	US	2008 - similar to 2006 FRCP amendments; Rules	www.courts.state.md.us/rules/roc	
US-ME	Maine	US	Rules of Civil Procedure; effective 2008 based	www.courts.state.me.us/rules_for	
US-MI	Michigan	US	Court Rules; effective 2009 based on 2006 FRCP	http://courts.michigan.gov/suprer	
US-MN	Minnesota	US	2007 adopted 2006 FRCP amendments with me	www.mncourts.gov/documents/O	
US-MO	Missouri	US	None of the 2006 FRCP amendments		
US-MS	Mississippi	US	2003, predates 2006 FRCP; Rules of Civil Proce	www.mssc.state.ms.us/rules/msr	
US-MT	Montana	US			

For the states that have their own specific rules of civil, criminal and evidence, an additional table was added entitled State Rules table. This table consists of seven fields which are shown in Table A11 and populated in Table A12. This is where more relations between tables and multiple lookups occur. Because there are so many states with similar rule numbers, an auto number was used as the key field, State Rule ID, to be able to set up a one-to-many relationship to the State or Province table. The next field allows the data entry person to distinguish between civil, criminal, or evidentiary rules. The State Rule Designator field data would be the specific name used by the state or province for the rule. Mapping is enhanced with the next key by providing a link to the Federal or Country Rules table. The State Rule field is used to describe the functionality of that rule. Finally a foreign key to the Country is provided. Once scripts and/or queries are developed to enhance the database, this may be redundant, but is included for now.

Table A11 - State Rules Table

Field Name	Type	Size	Description
State Rule ID	Long Integer	4	Auto number
State or Province ID	Text	6	Foreign key from State or Province table
State Rule Type	Long Integer	4	Foreign key from the Rule Type table
State Rule Designator	Text	30	Per the state or province
Federal Rule ID	Text	20	Foreign key from the Federal or Country rules table
State Rule Description	Text	255	Description if needed
Country Code	Text	2	Foreign key to Country table

Table A12- Populated State Rules Table

State Rule ID	State	State Rule Type	State Rule Designator	Federal Rule ID	State Rule Description
61	US-LA	Civ	1460	FRCP 33	
62	US-LA	Civ	1461	FRCP 34	lists ESI
63	US-LA	Civ	1462	FRCP 34	can specify format
64	US-LA	Civ	1471	FRCP 37 (e)	
65	US-LA	Civ	1424(D)	Misc	inadvertant waiver
66	US-LA	Civ	1354	Misc	subpoena
67	US-MA	Civ	26(b)(5)	Misc	requires production of a privilege log for anyo
68	US-MD	Civ	2-504.1	FRCP 16	
69	US-MD	Civ	2-402(b)	FRCP 26	
70	US-MD	Civ	2-504	FRCP 26(f)	contents of scheduling order may contain prov
71	US-MD	Civ	2-421	FRCP 33	
72	US-MD	Civ	2-422	FRCP 34	
73	US-MD	Civ	2-433(b)	FRCP 37 (e)	
74	US-MD	Civ	2-402(e)(3)	Misc	inadvertent disclosure
75	US-MD	Civ	2-424	Misc	admission of ESI
76	US-MD	Civ	2-510	Misc	subpoena
77	US-ME	Civ	16	FRCP 16	
78	US-ME	Civ	26	FRCP 26	
79	US-ME	Civ	33	FRCP 33	
80	US-ME	Civ	34	FRCP 34	
81	US-ME	Civ	37	FRCP 37 (e)	
82	US-MI	Civ	2.401	FRCP 16	
83	US-MI	Civ	2.302(18)(6)	FRCP 26	
84	US-MI	Civ	2.301	FRCP 34	
85	US-MI	Civ	2.313(E)	FRCP 37 (e)	
86	US-MI	Civ	2.302	Misc	inadvertent waiver

After entering in several cases, it was decided that a further granularity as mentioned in the main dissertation was needed. A table for sections and subsections of the Federal or Country laws was created as shown in Table A13 and populated in A14.

This allows for situations such as in the FRE 41 with various sections that refer to warrants, arrests, etc.

Table A13 - Federal Rules Subsection

Field Name	Type	Size	Description
ID	Long Integer	4	Auto number
Federal Rule ID	Text	20	Foreign key from Federal Rules table
Section or Subsection Number	Text	50	Section or subsection
Description of Section	Text	255	
Common Search Term ID	Long Integer	4	Foreign key from Common Search Terms table

Table A14 - Populated Federal Rules Subsections

ID	Federal Rule ID	Section or St	Description of Section	Key Term ID
1	FRCrP 41	41(a)	Scope and definitions	Scope and Definition of Search and
2	FRCrP 41	41(b)	Who has the authority to issue a warrant	Who can issue a warrant
3	FRCrP 41	41 (c)	When a warrant may be issued	When a warrant can be issued
4	FRCrP 41	41(d)	The warrant must be issued to someone with author	Warrant must be issued who has au
5	FRCrP 41	41(g)	Motion to return property	Motion to return property/wrongft
6	CPA	Section 21	Articles to be seized under a Search Warrant	Search of an arrested person
7	CPA	Section 22	When items may be seized without a search warrant	When items can be seized without
8	CPA	Section 23	Search of an arrested person	Search of an arrested person
9	CPA	Section 25	Authority to enter premises in interest of national se	

The final table to be created was the Case Law table. In addressing new technology such as digital law, case law is relied upon heavily in common law nations. This table allows a person to look up cases in which laws were applied or argued. The design is shown in Table A15. The tracking ID is unique to the database and has no relevance elsewhere. The case name and catalogue number follow the convention of the countries in the database. However, *plaintiff v. defendant*, is used in the database as opposed to “*vs. or v*”. Depending upon the literature, the exact date of the ruling may be available, but not always. As a result, the year and exact date are both included in the

database. The Federal Rules and Common Search terms are included in the table as shown in Table A16. In the future it may be required to add an additional layer to this as more than one law or regulation may apply to a case. Recall that modifiability is a quality of grounded theory. Note that a memo field is provided for a brief description.

Table A15 - Case Law Table

Name	Type	Size	Description
Case Tracking ID	Long Integer	4	Auto number
Case Name	Text	255	In the form of Plaintiff v. Defendant
Index or Catalogue reference	Text	100	Accepted catalogue number
Case Date	Date/Time	8	If full date available
Case Year	Long Integer	4	Year
Country ID	Text	2	Foreign key from the Country table
Federal or Country Rule	Text	20	Applicable Federal or Country rule via lookup
Common Search Terms ID	Long Integer	4	Foreign key from the Common Search Terms table
Local Rule	Long Integer	4	Potential additional table
Comments	Memo	-	

Table A16 - Populated Case Law Table

Case	Case Name	Index or Catalogue	Case Date	Case Year	Country	Federal or C	Key Terms ID	Comments
	Donn Olson v. Michael Reynolds	No. 11-227	6/27/2012	2012	US			Daubert stande
44	S v. Mashiyi and Another			2002	SA		Definitions	Some documen
45	Narlis v. South African Bank of Att			1976	NA		Definitions cre	Documents cre
46	S v. Koralev and Another	2006 (2) SACR 298 (N		2006	SA		Third party searches	2006 (2) SACR 2
47	S v. Mdlongwa							Qualifications
48	S v. Ndiki and Others	2008 (2) SACR 252 (C	11/13/2006	2006	SA			computer gene
5	Chimel v. California	395 U.S. 752	6/23/1969	1969	US	4th Amendme	Search of an arrested person	Search of an ar
6	Arizona v. Gant	216 Ariz. 1, 162 P. 3d	4/21/2009	2009	US	4th Amendme		driving with su
1	Katz v. United States	389 U.S. 347	10/17/1967	1967	US	4th Amendme	Wiretaps	Wiretap Act as
9	United States v Jacobsen	466 U.S. 109, 113		1984	US	4th Amendme	When a warrant can be issued	interception of
10	Berger v. New York	388 U.S. 41, 59-60		1967	US	4th Amendme		
11	Illinois v. Andreas	463 U.S. 765, 771		1983	US	4th Amendme	Warrantless search	exception to a
12	Payton v. New York	445 U.S. 573, 589-90		1980	US	4th Amendme		Expectation of
13	Kyllo v. United States	533 U.S. 27, 34-35		2001	US	4th Amendme	Specialized technology use	Use of thermal
14	United States v. Ross	456 U.S. 798, 822-23		1982	US	4th Amendme		Opaque contai
15	United States v. Heckenkamp	482 F.3d 1142, 1146		2007	US	4th Amendme		9th Circuit cour
16	United States v. Buckner	473 F.3d 551, 554 n.2		2007	US	4th Amendme		4th Circuit cour
17	United States v. Lifshitz	369 F.3d 173, 190		2004	US	4th Amendme		2nd Circuit, ex
18	United States v. Al-Marri	230 F. Supp. 2d 535,		2002	US	4th Amendme	Computer as closed container	S.D.N.Y. compu
19	United States v. Reyes	922 F.Supp. 818, 822		1996	US	4th Amendme	Expectation of privacy in a person	S.D.N.Y. reaso
20	United States v. Lynch	908 F.Supp. 284, 287		1995	US	4th Amendme	Expectation of privacy in a person	D.V.I. reasona
21	United States v. Andrus	483 F.3d 711, 718		2007	US	4th Amendme	Expectation of privacy in a person	10th Circuit, pe
22	United States v. Runyan	275 F.3d 449, 464-65		2001	US	4th Amendme	Email privacy	5th Circuit. The

User Interface

The primary objective of this database is to create a user friendly environment for professionals in the field. It needs to be easy to update and query. In this section, the user interfaces are presented. Figure A3 shows the Navigation Area for the data. It can also be used to browse the database.

The Microsoft Access database application was used to create the prototype. The user interfaces, queries and reports presented here are specific to that application. However, the tables can be easily modified for other platforms such as MySQL, SQL Server or Oracle. The MS Access Navigation form relies upon tabs. The primary forms that can be seen on the tab headings are Country, State-Province, Federal or Country Rules, Federal Rule Sections and subsections, Common Search Terms, Rule Type and Case Law as shown in Figure A3.

State Rule ID	State Rule Title	State Rule Designator	Federal Rule ID	State Rule Designator
1	Civil Procedure 16(b)(N)		FRCP 16	
2	Civil Procedure 26(b)(2)(B)		FRCP 26	
3	Civil Procedure 26(f)(3)		FRCP 26(f)	

Figure A3 - Database Navigation Menu

The Federal and Country Rules form shown in Figure A4 allows one to browse each country and their corresponding laws. Note the rule description, subsections and Common Search Criteria area. Each of these items contributes to the ability to search the database.

Federal or Country Rules

Rule Number ID: CPA
 Rule Description: Criminal Procedures Act 51
 Country Code: ZA
 Search Criteria:

ID	Federal Rule ID	Section or Subsection Number	Description of Section
6	CPA	Section 21	Articles to be seized under a Search
7	CPA	Section 22	When items may be seized witho
8	CPA	Section 23	Search of an arrested person
9	CPA	Section 25	Authority to enter premises in int
10	CPA	Section 27	Resisting arrest or search
11	CPA	Section 28	Wrongful search and award of dar
* (New)	CPA		

Record: 1 of 6 | No Filter | Search

Figure A4 - Federal or Country Rules Form

Countries may have multiple jurisdictions in them; it is further complicated by the fact that in countries such as the U.S. and Canada each state or province may have different civil laws or statutes. Nations such as Namibia have multiple jurisdictions, but the laws are the same as the federal laws in each province. The State-Province Form reflects this complication as shown in Figure A5. In addition to entering the state names, the related civil and criminal laws can be entered while in the sub-form, the state or province laws can be mapped to the federal laws. Accessing this information is essential

when a case is first being tried at the state level or if the investigation begins in one state and moves to another.

The screenshot shows a web form titled "State-Province". The form contains the following fields:

- State ID: US-KS
- State or Province Name: Kansas
- Country Code: United States of America (dropdown menu)
- State or Province Civil Rules: effective 2008, similar to 2006 FRCP
- Civil URL: <http://kansasstatutes.lesterama.org/Chapter>
- State or Province Criminal Rules: (empty field)
- Criminal URL: (empty field)
- State or Province Evidence Rules: (empty field)
- Evidentiary URL: (empty field)

Below the form is a table with the following data:

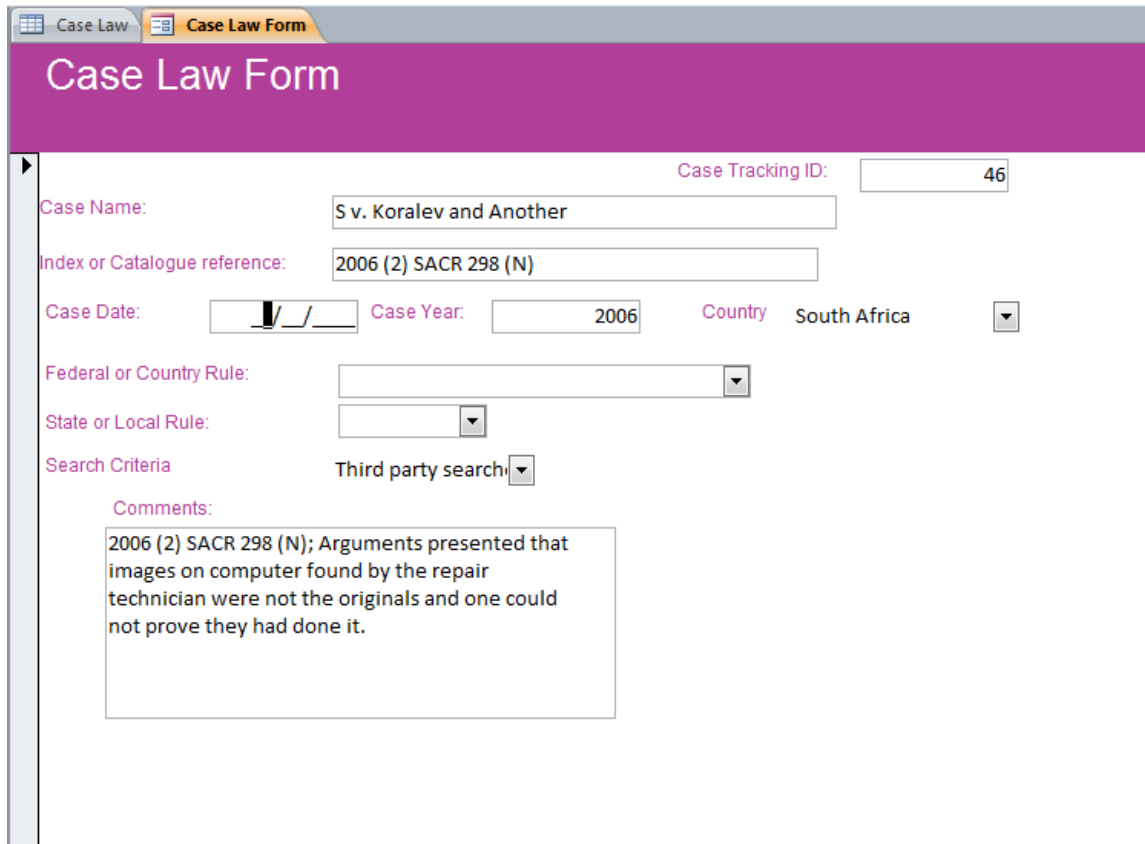
State Rule ID	State Rule Title	State Rule Designator	Federal Rule ID	State Rule Description
53	Civil Procedure	60-216	FRCP 16	
54	Civil Procedure	60-226(b)(2)(B)	FRCP 26	
55	Civil Procedure	60-233	FRCP 33	
56	Civil Procedure	60-234	FRCP 34	
57	Civil Procedure	60-237	FRCP 37 (e)	
58	Civil Procedure	60-245	Misc	subpoena

At the bottom of the table, there is a pagination control showing "Record: 1 of 6" and a search bar.

Figure A5 - State-Province Form

Once the provinces or states and their relevant laws are entered, the user can look up or enter the case law. As has been established, common law nations rely upon case law when dealing with new technology or situations in which the law has not yet been created. The Case Law²⁷ form shown next illustrates how the cases are linked to the country, the appropriate law and key search terms.

²⁷ The full Case Law table can be found in Appendix B



Case Law Form

Case Tracking ID: 46

Case Name: S v. Koralev and Another

Index or Catalogue reference: 2006 (2) SACR 298 (N)

Case Date: / / Case Year: 2006 Country: South Africa

Federal or Country Rule: [Dropdown]

State or Local Rule: [Dropdown]

Search Criteria: Third party search [Dropdown]

Comments:
2006 (2) SACR 298 (N); Arguments presented that images on computer found by the repair technician were not the originals and one could not prove they had done it.

Figure A6 - Case Law Form

Queries and Reports

Queries are used in databases to search for terms or combinations thereof. As mentioned previously, the tables Common Search Criteria and Rule Types were added to assist in querying the database. Queries can be created for easy lookup and to generate associated reports. The tables created in the template can be easily expanded to bring all of the information together into an easy lookup for experts and novices. Figure A7 shows a query by example (QBE) grid, which is native to MS Access, to search for evidence rules in the U.S. and South Africa. Figure A8 shows the result of the query. The generated SQL statement is:

```

SELECT Country.[Country Code], Country.[Country Name], [Federal or Country
Rules].[Rule Number ID], [Federal or Country Rules].[Rule Description], [Rule
Type].[Rule Type ID], [Rule Type].[Rule Type Label]
FROM [Rule Type] INNER JOIN (Country INNER JOIN [Federal or Country
Rules] ON Country.[Country Code] = [Federal or Country Rules].[Country
Code]) ON [Rule Type].[Rule Type ID] = [Federal or Country Rules].[Rule Type
ID]
WHERE (((Country.[Country Code]="US") AND (([Rule Type].[Rule Type
ID]=3))) OR (((Country.[Country Code]="ZA") AND (([Rule Type].[Rule Type
ID]=3)));
    
```

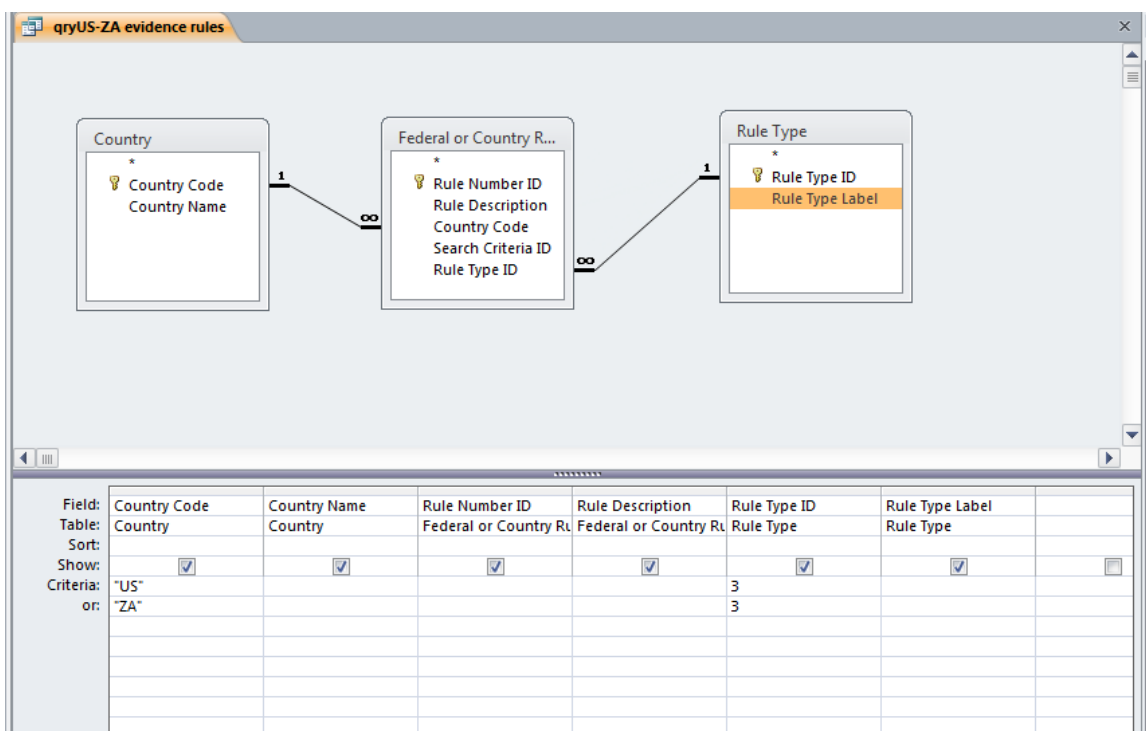


Figure A7 - QBE grid

Table A17- Query Results

qryUS-ZA evidence rules					
Country Cod	Country Name	Rule Number ID	Rule Description	Rule Type ID	Rule Type Label
US	United States of America	FRE 1002	Contents of Writings, Recordings and Photographs	3	Evidence
US	United States of America	FRE 1003	Contents of Writings, Recordings and Photographs	3	Evidence
US	United States of America	FRE 103	Rulings on Evidence	3	Evidence
US	United States of America	FRE 104	Preliminary questions such as whether or not	3	Evidence
US	United States of America	FRE 105	Limited Admissibility	3	Evidence
US	United States of America	FRE 106	Remainder of or Related Writings or Recorded	3	Evidence
US	United States of America	FRE 401	Relevancy and its Limits	3	Evidence
US	United States of America	FRE 402	Relevancy and Its Limits	3	Evidence
US	United States of America	FRE 701		3	Evidence
US	United States of America	FRE 702	Expert Testimony	3	Evidence
US	United States of America	FRE 703	Bases for the Opinion of Expert Testimony	3	Evidence
US	United States of America	FRE 802	Hearsay exclusion	3	Evidence
US	United States of America	FRE 803	Hearsay exceptions	3	Evidence
US	United States of America	FRE 804	Hearsay Exceptions	3	Evidence
US	United States of America	Sarbanes-Oxley	publicly traded corporations required to have	3	Evidence
US	United States of America	SCA	Stored Communications Act	3	Evidence
ZA	South Africa	ZA - Act 45 of 1988	Law of Evidence Amendment	3	Evidence

Reports can be produced as a result of the queries for use in research or other types of communication. Figure A8 shows a report generated from the query results shown in Table A17. The ability to perform custom queries will allow IT and legal practitioners to better evaluate what may be needed based on the country or countries involved.

Country		
Country Name		
United States of America		
Rule Type Label	Rule Number ID	Rule Description
Evidence	FRE 702	Expert Testimony
	FRE 1003	Contents of Writings, Recordings and Photograph
	FRE 103	Rulings on Evidence
	FRE 104	Preliminary questions such as whether or not a w
	FRE 105	Limited Admissibility
	FRE 106	Remainder of or Related Writings or Recorded St
	FRE 401	Relevancy and its Limits
	FRE 1002	Contents of Writings, Recordings and Photograph
	FRE 701	
	FRE 703	Bases for the Opinion of Expert Testimony
	FRE 802	Hearsay exclusion
	FRE 803	Hearsay exceptions

Figure A8 - Resulting Report

Improvements and Projected Use

Grounded theory has modifiability as a fundamental principle. The prototype created in this research was designed as a relational database model so that as new correlations emerge, they can be easily added. As mentioned at the beginning of this Appendix, this database will require many hands to be fully populated with the data of all the common law nations of the world. Once fully implemented for a web environment, the database could then be put on a production server and accessible to others. The South King County Chapter of the Washington State Paralegal Association is interested in the project and will be able to assist in adding more countries. Other groups may also be interested in doing the research and data input needed to accomplish this. The most pressing concern would be validating the accuracy of the data entered.

This prototype, as discussed in Chapter Six, demonstrates that this level of granularity can be achieved with most common law nations. It also illustrates that the way the nations address digital law and digital evidence can be mapped to each other. This enables professionals in cases in which digital evidence crosses national boundaries to quickly ascertain what laws in their country or other may apply.

APPENDIX B – POPULATED TABLES**Table B1 - Country Table**

Country Code	Country Name
CA	Canada
EU	European Union
JP	Japan
MX	Mexico
NA	Namibia
US	United States of America
ZA	South Africa

Table B2 – State-Province Table

State ID	State or Province Name	Country Code	State or Province Civil Rules	Civil URL	State or Province Criminal Rules	Criminal URL	State or Province Evidence Rules
NA-CA	Caprivi	NA		-		-	
NA-ER	Erongo	NA		-		-	
NA-HA	Hardap	NA		-		-	
NA-KA	Karas	NA		-		-	
NA-KH	Khomas	NA		-		-	
NA-KU	Kumene	NA		-		-	
NA-OD	Otjozondjupa	NA		-		-	
NA-OH	Omaheke	NA		-		-	
NA-OK	Okavango	NA		-		-	
NA-ON	Oshana	NA		-		-	
NA-OS	Omusati	NA		-		-	
NA-OT	Oshikoto	NA		-		-	
NA-OW	Ohangwena	NA		-		-	
US-AK	Alaska	US	Alaska rules of civil procedure	http://www.courts.alaska.gov/civ.htm	Alaska Rules of Criminal Procedure	http://courts.alaska.gov/crpro.htm	Alaska Rules of Evidence
US-AL	Alabama	US	AL Rules of Civil Procedure - effective 2/10, same as FRCP	-		-	
US-AR	Arkansas	US	http://courts.arkansas.gov/rules/rules_civ_procedures/index.cfm	-		-	

Table continued on next page

State – Province Table (page 2 of 5)

State ID	State or Province Name	Country Code	State or Province Civil Rules	Civil URL	State or Province Criminal Rules	Criminal URL	State or Province Evidence Rules
US-AZ	Arizona	US	in 2008, e-discovery rules similar to 2006 FRCP				
US-CA	California	US	Code of Civil Procedure, effective 2009 similar to FRCP 2006	-		-	
US-CO	Colorado	US	none of FRCP amendments	-		-	
US-CT	Connecticut	US	Practice Book, Superior Court	-		-	
US-DC	District of Columbia	US	none of the 2006 FRCP amendments	-		-	
US-DE	Delaware	US	none of the 2006 FRCP amendments	-		-	
US-FL	Florida	US	Rules for the Complex Business Litigation Division of the 13th Judicial Circuit in Tampa	-		-	
US-GA	Georgia	US	none of the 2006 FRCP amendments	-		-	
US-HI	Hawaii	US	none of the 2006 FRCP amendments	-		-	
US-ID	Idaho	US	Rules of Civil Procedure effective 2006 - modeled on 2006 FRCP and Texas Rules of civil procedure	-		-	
US-IL	Illinois	US	Supreme Court Rules - 1996, acknowledges ESI but requires that it be printed to be produced in court	www.state.il.us/court/SupremeCourt/Rules/Art_II/		-	
US-IN	Indiana	US	Rules of Trial Procedure. In 2008, similar to 2006 FRCP amendments	www.in.gov/judiciary/rules/trial_proc/index.html		-	

State – Province Table (page 3 of 5)

State ID	State or Province Name	Country Code	State or Province Civil Rules	Civil URL	State or Province Criminal Rules	Criminal URL	State or Province Evidence Rules
US-IO	Iowa	US	Rules of Civil Procedure	www.legis.state.ia.us/DOCS/ACO/CR/LINC/06-04-2010.chapter.1.pdf		-	
US-KS	Kansas	US	effective 2008, similar to 2006 FRCP	http://kansasstatutes.lesterama.org/Chapter_60/Article_2/		-	
US-KY	Kentucky	US	none of the 2006 FRCP amendments	-		-	
US-LA	Louisiana	US	2009 follows 2006 FRCP amendments - except meet and confer optional; Under Code of Civil Procedure	www.legis.state.la.us/billdata/streamdocument.asp?did=447007		-	
US-MA	Massachusetts	US	Rules of Civil Procedure - done in 2008, but does not fully address e-discovery	www.massreports.com/courtrules/civil.htn		-	
US-MD	Maryland	US	2008 - similar to 2006 FRCP amendments; Rules of Civil Procedure	www.courts.state.md.us/rules/rodocs/ro158.pdf		-	
US-ME	Maine	US	Rules of Civil Procedure; effective 2008 based on 2006 FRCP amendments	www.courts.state.me.us/rules_forms_fees/rules/MRCivPAmend7-08.pdf		-	
US-MI	Michigan	US	Court Rules; effective 2009 based on 2006 FRCP	http://courts.michigan.gov/supremecourt/Resources/Administrative/2007-24-12-16-08.pdf		-	

Table continued on next page

State – Province Table (page 4 of 5)

State ID	State or Province Name	Country Code	State or Province Civil Rules	Civil URL	State or Province Criminal Rules	Criminal URL	State or Province Evidence Rules
US-MN	Minnesota	US	2007 adopted 2006 FRCP amendments with meet and confer optional; Rules of Civil Procedure	www.mncourts.gov/documents/O/Public/Rules_effective_7-1-2007.pdf		-	
US-MO	Missouri	US	None of the 2006 FRCP amendments	-		-	
US-MS	Mississippi	US	2003, predates 2006 FRCP; Rules of Civil Procedure	www.mssc.state.ms.us/rules/msrulesofcourt/rules_of_civil_procedure.pdf		-	
US-MT	Montana	US		-		-	
US-NC	North Carolina	US		-		-	
US-NE	Nebraska	US		-		-	
US-NH	New Hampshire	US		-		-	
US-NJ	New Jersey	US		-		-	
US-NM	New Mexico	US		-		-	
US-NV	Nevada	US	None of the 2006 FRCP amendments	-		-	
US-NY	New York	US		-		-	
US-OH	Ohio	US		-		-	
US-OK	Oklahoma	US	None of the 2006 FRCP amendments	-		-	
US-OR	Oregon	US	None of the 2006 FRCP amendments	-		-	
US-PA	Pennsylvania	US	None of the 2006 FRCP amendments	-		-	
US-RI	Rhode Island	US	None of the 2006 FRCP amendments	-		-	

Table continued on next page

State – Province Table (page 5 of 5)

State ID	State or Province Name	Country Code	State or Province Civil Rules	Civil URL	State or Province Criminal Rules	Criminal URL	State or Province Evidence Rules
US-SC	South Carolina	US	None of the 2006 FRCP amendments	-		-	
US-SD	South Dakota	US	None of the 2006 FRCP amendments	-		-	
US-TN	Tennessee	US		-		-	
US-TX	Texas	US		-		-	
US-UT	Utah	US		-		-	
US-VA	Virginia	US		-		-	
US-VT	Vermont	US		-		-	
US-WA	Washington	US	None of the 2006 FRCP amendments	-		-	
US-WI	Wisconsin	US	None of the 2006 FRCP amendments	-		-	
US-WV	West Virginia	US	None of the 2006 FRCP amendments	-		-	
US-WY	Wyoming	US		-		-	
ZA-EC	Eastern Cape	ZA		-		-	
ZA-FS	Free State	ZA		-		-	
ZA-GT	Gauteng	ZA		-		-	
ZA-LP	Limpopo	ZA		-		-	
ZA-MP	Mpumalanga	ZA		-		-	
ZA-NC	Northern Cape	ZA		-		-	
ZA-NL	KwaZulu-Natal	ZA		-		-	
ZA-NW	North West	ZA		-		-	
ZA-WC	Western Cape	ZA		-		-	

Table B3 - Federal or Country Rules

Rule Number ID	Rule Description	Country Code	Rule Type ID	Search Criteria ID
4th Amendment	Regarding unreasonable search and seizure	US	Constitutional	Scope and Definition of Search and Seizure Law
5 th Amendment	Self-incrimination	US	Constitutional	Self-incrimination
Act 22 of 2003	Computer Misuse and CyberCrime Act	NA	Computer Crime & Abuse	
Act 57 of 1983	Computer Evidence Act 57	ZA	Computer Crime & Abuse	
Act 9 of 2000	International Co-operation in Criminal Matters Act	ZA	Criminal	
CFAA	Computer Fraud and Abuse Act	US	Computer Crime & Abuse	
CPA	Criminal Procedures Act 51	ZA	Criminal	
CPA 25	Criminal Procedures Act 25	NA	Criminal	
ECPA	Electronic Communications Privacy Act	US	Privacy	Privacy – communications
ECT Act of 2002	Electronic Communications Act 25 of 2002	ZA	Privacy	Privacy – communications
FRCP 16	Pretrial Conference – ESI may be in contents	US	Civil Procedure	
FRCP 26		US	Civil Procedure	
FRCP 26(f)	Meet and Confer	US	Civil Procedure	

Table continued on next page

Federal or Country Rules (page 2 of 3)

Rule Number ID	Rule Description	Country Code	Rule Type ID	Search Criteria ID
FRCP 33	Interrogatories - option to produce business records	US	Civil Procedure	
FRCP 34	May specify form of ESI	US	Civil Procedure	
FRCP 37 (e)	Safe Harbor for routine good faith operation of ESI	US	Civil Procedure	
FRCrP 41	Search and Seizure Rules	US	Criminal	
FRE 1002	Contents of Writings, Recordings and Photographs	US	Evidence	
FRE 1003	Contents of Writings, Recordings and Photographs	US	Evidence	
FRE 103	Rulings on Evidence	US	Evidence	
FRE 104	Preliminary questions such as whether or not a witness is qualified	US	Evidence	
FRE 105	Limited Admissibility	US	Evidence	
FRE 106	Remainder of or Related Writings or Recorded Statements	US	Evidence	
FRE 401	Relevancy and its Limits	US	Evidence	
FRE 402	Relevancy and Its Limits	US	Evidence	
FRE 701		US	Evidence	
FRE 702	Expert Testimony	US	Evidence	
FRE 703	Bases for the Opinion of Expert Testimony	US	Evidence	
FRE 802	Hearsay exclusion	US	Evidence	
FRE 803	Hearsay exceptions	US	Evidence	
FRE 804	Hearsay Exceptions	US	Evidence	

Table continued on next page

Federal or Country Rules (page 3 of 3)

Rule Number ID	Rule Description	Country Code	Rule Type ID	Search Criteria ID
Misc	Subpoena or inadvertent disclosure or Cost Shifting or Sanctions	US	Civil Procedure	
NA - Act 25 of 1965	Civil Proceedings Evidence Act	NA	Civil Procedure	
NA - Act 45 of 1988	Law of Evidence Amendment	NA	Evidence	
Sarbanes-Oxley	publicly traded corporations required to have financial transparency	US	Evidence	
SCA	Stored Communications Act	US	Evidence	Privacy - communications
Section 12	Chapter 1, Section 12 of the Constitution of S.A., Freedom of the individual	ZA	Constitutional	
Section 14	Chapter 1, Section 14 of the Constitution of the Republic of South Africa	ZA	Constitutional	Privacy - communications
ZA - Act 25 of 1965	Civil Proceedings Evidence Act	ZA	Computer Crime & Abuse	
ZA - Act 45 of 1988	Law of Evidence Amendment	ZA	Evidence	

Table B4 - Federal Rule Sections or Subsections

ID	Federal Rule ID	Section or Subsection Number	Description of Section	Search Criteria ID
1	FRCrP 41	41(a)	Scope and definitions	Scope and Definition of Search and Seizure Law
2	FRCrP 41	41(b)	Who has the authority to issue a warrant	Who can issue a warrant
3	FRCrP 41	41 (c)	When a warrant may be issued	When a warrant can be issued
4	FRCrP 41	41(d)	The warrant must be issued to someone with authority to execute	Warrant must be issued who has authority to execute
5	FRCrP 41	41(g)	Motion to return property	Motion to return property/wrongful search/compensation
6	CPA	Section 21	Articles to be seized under a Search Warrant	Search of an arrested person
7	CPA	Section 22	When items may be seized without a search warrant	When items can be seized without a warrant
8	CPA	Section 23	Search of an arrested person	Search of an arrested person
9	CPA	Section 25	Authority to enter premises in interest of national security	
10	CPA	Section 27	Resisting arrest or search	
11	CPA	Section 28	Wrongful search and award of damages	Motion to return property/wrongful search/compensation

Table B5 - State Rules

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
1	US-AK	Civil Procedure	16(b)(N)	FRCP 16		United States of America
2	US-AK	Civil Procedure	26(b)(2)(B)	FRCP 26		United States of America
3	US-AK	Civil Procedure	26(f)(3)	FRCP 26(f)		United States of America
4	US-AK	Civil Procedure	33(d)	FRCP 33		United States of America
5	US-AK	Civil Procedure	37(i)	FRCP 37 (e)		United States of America
6	US-AK	Civil Procedure	45		Subpoena	United States of America
7	US-AL	Civil Procedure	16(b)(5)	FRCP 16		United States of America
8	US-AL	Civil Procedure	16(b)(6)	FRCP 16		United States of America
9	US-AL	Civil Procedure	26(b)(2)	FRCP 26		United States of America
10	US-AL	Civil Procedure	26	FRCP 26	not mandatory	United States of America

Table continued on next page

State Rules (page 2 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
11	US-AL	Civil Procedure	33(c)	FRCP 33		United States of America
12	US-AL	Civil Procedure	34(a)	FRCP 34		United States of America
13	US-AL	Civil Procedure	37(g)	FRCP 37 (e)		United States of America
14	US-AL	Civil Procedure	26(b)(6)(G)		inadvertent waiver	United States of America
15	US-AR	Civil Procedure	26.1 adopted by AR S. Crt	FRCP 16		United States of America
16	US-AR	Civil Procedure	26(b)(5)	Misc		United States of America
17	US-AZ	Civil Procedure	16	FRCP 16		United States of America
18	US-AZ	Civil Procedure	26(b) and 26.1	FRCP 26		United States of America
19	US-AZ	Civil Procedure	33(c)	FRCP 33		United States of America
20	US-AZ	Civil Procedure	34	FRCP 34		United States of America
21	US-AZ	Civil Procedure	37(g)	FRCP 37 (e)		United States of America

Table continued on next page

State Rules (page 3 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
22	US-AZ	Civil Procedure	45	Misc	state rules of evidence 502 Attorney Client Privilege	United States of America
23	US-CA	Civil Procedure	2031.060(e) and 2031.310	FRCP 26		United States of America
24	US-CA	Civil Procedure	Civil Rules of Court 3.724	FRCP 26(f)		United States of America
25	US-CA	Civil Procedure	2031.030 and 2031.280	FRCP 34		United States of America
26	US-CA	Civil Procedure	2031.060(i)	FRCP 37 (e)		United States of America
27	US-CA	Civil Procedure	2031.285(a) and 2031.060(e)	Misc	inadvertent disclosure and cost shifting respectively	United States of America
28	US-CT	Civil Procedure	13-9(d)	FRCP 26	must have showing of good cause if ESI needed in alternative format	United States of America
29	US-FL	Civil Procedure	7.10.1	FRCP 26		United States of America
30	US-FL	Civil Procedure	7.10.2	FRCP 34		United States of America
31	US-FL	Civil Procedure	7.10.3	FRCP 37 (e)		United States of America
32	US-FL	Civil Procedure	7.10.4	Misc	similar to FRCP	United States of America

Table continued on next page

State Rules (page 4 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
33	US-ID	Civil Procedure	33(d)	FRCP 33		United States of America
34	US-ID	Civil Procedure	34(b)	FRCP 34		United States of America
35	US-ID	Civil Procedure	45(b)	Misc	subpoena for ESI	United States of America
36	US-ID	Civil Procedure	37(a)(4)	Misc	discretionary cost-shifting by Court	United States of America
37	US-ID	Civil Procedure				United States of America
38	US-ID	Civil Procedure				United States of America
39	US-II	Civil Procedure	201	FRCP 34	definition of documents includes retrievable information in computer storage	United States of America
40	US-II	Civil Procedure	214	FRCP 34	produce ESI as kept in original course of business but ESI must be printed	United States of America
41	US-IN	Civil Procedure	26	FRCP 26		United States of America
42	US-IN	Civil Procedure	34	FRCP 34		United States of America
43	US-IN	Civil Procedure	37(e)	FRCP 37 (e)		United States of America

Table continued on next page

State Rules (page 5 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
44	US-IO	Civil Procedure	1.602	FRCP 16		United States of America
45	US-IO	Civil Procedure	1.504	FRCP 26		United States of America
46	US-IO	Civil Procedure	1.507	FRCP 26(f)		United States of America
47	US-IO	Civil Procedure	1.509	FRCP 33		United States of America
48	US-IO	Civil Procedure	1.503	FRCP 34	documents include ESI	United States of America
49	US-IO	Civil Procedure	1.512	FRCP 34		United States of America
50	US-IO	Civil Procedure	1.517(6)	FRCP 37 (e)		United States of America
51	US-IO	Civil Procedure	1.701	Misc	subpoena	United States of America
52	US-IO	Civil Procedure	Rules of evidence 5.502	Misc	regarding privileged documents	United States of America
53	US-KS	Civil Procedure	60-216	FRCP 16		United States of America
54	US-KS	Civil Procedure	60-226(b)(2)(B)	FRCP 26		United States of America

Table continued on next page

State Rules (page 6 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
55	US-KS	Civil Procedure	60-233	FRCP 33		United States of America
56	US-KS	Civil Procedure	60-234	FRCP 34		United States of America
57	US-KS	Civil Procedure	60-237	FRCP 37 (e)		United States of America
58	US-KS	Civil Procedure	60-245	Misc	subpoena	United States of America
59	US-LA	Civil Procedure	1551	FRCP 16		United States of America
60	US-LA	Civil Procedure	1462(E)	FRCP 26		United States of America
61	US-LA	Civil Procedure	1460	FRCP 33		United States of America
62	US-LA	Civil Procedure	1461	FRCP 34	lists ESI	United States of America
63	US-LA	Civil Procedure	1462	FRCP 34	can specify format	United States of America
64	US-LA	Civil Procedure	1471	FRCP 37 (e)		United States of America
65	US-LA	Civil Procedure	1424(D)	Misc	inadvertent waiver	United States of America

Table continued on next page

State Rules (page 7 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
66	US-LA	Civil Procedure	1354	Misc	subpoena	United States of America
67	US-MA	Civil Procedure	26(b)(5)	Misc	requires production of a privilege log for anyone who makes a claim of privilege in response to a discovery request	United States of America
68	US-MD	Civil Procedure	2-504.1	FRCP 16		United States of America
69	US-MD	Civil Procedure	2-402(b)	FRCP 26		United States of America
70	US-MD	Civil Procedure	2-504	FRCP 26(f)	contents of scheduling order may contain provisions for ESI	United States of America
71	US-MD	Civil Procedure	2-421	FRCP 33		United States of America
72	US-MD	Civil Procedure	2-422	FRCP 34		United States of America
73	US-MD	Civil Procedure	2-433(b)	FRCP 37 (e)		United States of America
74	US-MD	Civil Procedure	2-402(e)(3)	Misc	inadvertent disclosure	United States of America
75	US-MD	Civil Procedure	2-424	Misc	admission of ESI	United States of America

Table continued on next page

State Rules (page 8 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
76	US-MD	Civil Procedure	2-510	Misc	subpoena	United States of America
77	US-ME	Civil Procedure	16	FRCP 16		United States of America
78	US-ME	Civil Procedure	26	FRCP 26		United States of America
79	US-ME	Civil Procedure	33	FRCP 33		United States of America
80	US-ME	Civil Procedure	34	FRCP 34		United States of America
81	US-ME	Civil Procedure	37	FRCP 37 (e)		United States of America
82	US-MI	Civil Procedure	2.401	FRCP 16		United States of America
83	US-MI	Civil Procedure	2.302(18)(6)	FRCP 26		United States of America
84	US-MI	Civil Procedure	2.301	FRCP 34		United States of America
85	US-MI	Civil Procedure	2.313(E)	FRCP 37 (e)		United States of America
86	US-MI	Civil Procedure	2.302	Misc	inadvertent waiver	United States of America

Table continued on next page

State Rules (page 9 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
87	US-MI	Civil Procedure	2.313	Misc	sanctions	United States of America
88	US-MI	Civil Procedure	2.506	Misc	subpoenas	United States of America
89	US-MN	Civil Procedure	16	FRCP 16		United States of America
90	US-MN	Civil Procedure	26.02(b)(2)	FRCP 26		United States of America
91	US-MN	Civil Procedure	26.06	FRCP 26(f)	not mandatory	United States of America
92	US-MN	Civil Procedure	33	FRCP 33		United States of America
93	US-MN	Civil Procedure	34.02	FRCP 34		United States of America
94	US-MN	Civil Procedure	37.05	FRCP 37 (e)		United States of America
95	US-MN	Civil Procedure	26.02(f)(2)	Misc	inadvertent waiver	United States of America
96	US-MN	Civil Procedure	45	Misc	subpoena	United States of America
97	US-MS	Civil Procedure	26(b)(5)	FRCP 26		United States of America

Table continued on next page

State Rules (page 10 of 10)

State Rule ID	State or Province ID	State Rule Type ID	State Rule Designator	Federal Rule ID	State Rule Description	Country Code
98	US-MS	Civil Procedure	37€	Misc	cost shifting for discovery abuses	United States of America

Table B6 - Case Law

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
4	Donn Olson v. Michael Reynolds	No. 11-227	6 /27/2012	2012	United States of America			Daubert standard	
44	S v. Mashiyi and Another			2002	South Africa		Definitions	Some documents were scanned which were admissible. Documents were defined as being created by a person. Computer generated bank statements were inadmissible	
45	Narlis v. South African Bank of Athens			1976	Namibia		Definitions	Documents created by a computer were inadmissible	

Table continued on next page

Case Law (page 2 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
46	S v. Koralev and Another	2006 (2) SACR 298 (N)		2006	South Africa		Third party searches	2006 (2) SACR 298 (N); Arguments presented that images on computer found by the repair technician were not the originals and one could not prove they had done it.	
47	S v. Mdlongwa							Qualifications of the investigator	
48	S v. Ndiki and Others	2008 (2) SACR 252 (CK)	11/13/2006	2006	South Africa			computer generated documents and hearsay	
49	Minister of Safety and Security v Liddell			2002	South Africa		Motion to return property/wrongful search/compensation	the defendant was awarded R20,000 for wrongful search and seizure, imprisonment and defamation of character	
5	Chimel v. California	395 U.S. 752	6/23/1969	1969	United States of America	4th Amendment	Search of an arrested person	Search of an arrested person	

Table continued on next page

Case Law (page 3 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
6	Arizona v. Gant	216 Ariz. 1, 162 P. 3d 640	4 /21/2009	2009	United States of America	4th Amendment		Driving with suspended license, search of vehicle produced cocaine and a gun. He moved to have the evidence thrown out. It was granted.	
1	Katz v. United States	389 U.S. 347	10/17/1967	1967	United States of America	4th Amendment	Wiretaps	Wiretap Act as well	
9	United States v. Jacobsen	466 U.S. 109, 113		1984	United States of America	4th Amendment	When a warrant can be issued	Interception of Intangible communications as a seizure.	
10	Berger v. New York	388 U.S. 41, 59-60		1967	United States of America	4th Amendment			
11	Illinois v. Andreas	463 U.S. 765, 771		1983	United States of America	4th Amendment	Warrantless search	exception to a warrantless search	

Table continued on next page

Case Law (page 4 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
12	Payton v. New York	445 U.S. 573, 589-90		1980	United States of America	4th Amendment		Expectation of privacy in ones home	
13	Kyllo v. United States	533 U.S. 27, 34-35		2001	United States of America	4th Amendment	Specialized technology use	Use of thermal imaging - new technology	
14	United States v. Ross	456 U.S. 798, 822-23		1982	United States of America	4th Amendment		Opaque container	
15	United States v. Heckenkamp	482 F.3d 1142, 1146		2007	United States of America	4th Amendment		9th Circuit court regarding reasonable expectation of privacy in a personal computer	
16	United States v. Buckner	473 F.3d 551, 554 n.2		2007	United States of America	4th Amendment		4th Circuit court, reasonable expectation of privacy of personal computers	

Table continued on next page

Case Law (page 5 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
17	United States v. Lifshitz	369 F.3d 173, 190		2004	United States of America	4th Amendment		2nd Circuit, expectation of privacy in their home computers	
18	United States v. Al-Marri	230 F. Supp. 2d 535, 541		2002	United States of America	4th Amendment	Computer as closed container	S.D.N.Y. computers should be treated as closed containers	
19	United States v. Reyes	922 F.Supp, 818, 822-33		1996	United States of America	4th Amendment	Expectation of privacy in a personal computer	S.D.N.Y. reasonable expectation of privacy for data on a pager	
20	United States v. Lynch	908 F.Supp. 284, 287		1995	United States of America	4th Amendment	Expectation of privacy in a personal computer	D.V.I. reasonable expectation of privacy of data on a pager	

Table continued on next page

Case Law (page 6 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
21	United States v. Andrus	483 F.3d 711, 718		2007	United States of America	4th Amendment	Expectation of privacy in a personal computer	10th Circuit, personal computer as a repository for most personal information one does not intend to share with others	
22	United States v. Runyan	275 F.3d 449, 464-65		2001	United States of America	4th Amendment	Email privacy	5th Circuit. The computer, floppies and zip disks had initially been searched by the estranged wife. The court upheld that the police had not exceeded what had already been begun by the third party	
23	United States v. Walser	275 F.3d 981, 986		2001	United States of America	4th Amendment	Computer as closed container	5th Circuit, police did not exceed the search	
24	United States v. Stults	N0. 08-3183	5 /13/2009	2009	United States of America	4th Amendment	Expectation of privacy in a personal computer	8th Circuit, no expectation of privacy when shared in a peer to peer network	

Table continued on next page

Case Law (page 7 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
25	United States v. Gorshkov	WL 1024026		2001	United States of America	4th Amendment	Expectation of privacy in a personal computer	Defendant did not have a reasonable expectation of privacy from an agent looking over his shoulder	
26	United States v. Horowitz	806 F.2d 1222		1986	United States of America	4th Amendment		No expectation of email privacy once received by the other party. They can use as they wish	
27	Guest v. Leis	255 F.3d 325, 333		2001	United States of America	4th Amendment	Email privacy	6th Circuit, lost legitimate expectation of privacy once it reaches the recipient, analogous to a letter	

Table continued on next page

Case Law (page 8 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
28	United States v. Jacobsen	466 U.S. 109, 113		1984	United States of America	4th Amendment	Third party searches	No 4th Amendment violation if a party of their own accord searches and turns over to law enforcement provided they are not acting as an agent of law enforcement	
29	United States v. Grimes	244 F.3d 375, 383		2001	United States of America	4th Amendment	Third party searches	Searches by repairmen prior to contacting law enforcement are private searches and do not violate the 4th Amendment	
30	United States v. Grant	434 F. Supp. 2d 735, 744-45		2006	United States of America	4th Amendment	Third party searches	D. Nebraska search by technician does not violate 4th Amendment	

Table continued on next page

Case Law (page 9 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
31	United States v. Bermudez	2006 WL 3197181	6 /30/2006	2006	United States of America	4th Amendment	Specialized technology use	S.D. Ind. June 30, 2006 - court rejected the Kyllo argument because cell phone signals are knowingly used by a third party - the phone company	
32	United States v. Long	425 F.3d 482, 487		2005	United States of America	4th Amendment	Specialized technology use	7th Circuit, the use of the Encase software did not exceed scope of consent to search laptop	
33	United States v. Anderson	2007 WL 1121319	4 /16/2007	2007	United States of America	4th Amendment	Third party searches	N.D. Ind. - court argued technicians had the actual and apparent authority to consent to search of a computer	
34	United States v. Barth	26 F. Supp. 2d 929, 938		1998	United States of America	4th Amendment	Third party searches	W.D. Tex. - repairman lacked authority because given the hard drive for a specific purpose	

Table continued on next page

Case Law (page 10 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
35	United States v. Chadwick	433 U.S. 1, 15		1977	United States of America	4th Amendment	Search of an arrested person	officers impermissibly searched footlocker seized incident to arrest when they took it away from the scene and did it a significant time later	
36	United States v. Brookes	2005 WL 1940124, at *3	6 /16/2005	2005	United States of America	4th Amendment	Computer as closed container	approved search of pager incident to arrest	
37	United States v. Finley	477 F.3d 250, 259-60		2007	United States of America	4th Amendment	Computer as closed container	approved search of cell phone incident to arrest	
39	Horton v. California	496 U.S. 128, 136		1990	United States of America	4th Amendment	Plain view doctrine	incriminating evidence immediately apparent which allows police to seize the computer	

Table continued on next page

Case Law (page 11 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
40	United States v. Wong	334 F.3d 831, 838		2003	United States of America	4th Amendment	Plain view doctrine	The original search was for graphics regarding a murder. When the child pornography was discovered, the plain view doctrine applied	
41	United States v. Herndon	501 F.3d 683, 693		2007	United States of America	4th Amendment	Plain view doctrine	6th Circuit, computer seized after probation officer showed the child porn on parolees computer	
42	United States v. Maxwell	45 M.J. 406, 422		1996	United States of America	4th Amendment	Plain view doctrine	C.A.A.F, 1996 - computer files opened by agents were not in plain view	
43	United States v. Villarreal	963 F.2d 770, 776		1992	United States of America	4th Amendment	Plain view doctrine	5th Circuit, a label on a container is not an invitation to search	

Table continued on next page

Case Law (page 12 of 12)

Case Tracking ID	Case Name	Index or Catalogue reference	Case Date	Case Year	Country Code	Federal or Country Rule	Search Criteria ID	Comments	Local Rule
7	U.S. v. Kirschner	2010 WL 1257355		2010	United States of America	5th Amendment		Giving of his encrypted computer's password with limited immunity. He refused.	
2	Daubert v. Merrell Dow Pharmaceuticals	509 U.S. 579 (1993)	6 /28/1993	1993	United States of America	FRE 702		Daubert Standard	
3	U.S. v. Sharron Grinnage	No. 10-3494.	6 /29/2012	2012	United States of America	FRE 702		Challenged that a pretrial Daubert hearing was not held for a new DNA methodology for sparse evidence.	

Table B7- Rule Type

Rule Type ID	Rule Type Label
1	Civil Procedure
2	Criminal
3	Evidence
4	Privacy
5	Constitutional
6	Computer Crime & Abuse

Table B8 - Common Search Criteria

Search Criteria ID	Search Terminology
1	Scope and Definition of Search and Seizure Law
2	Who can issue a warrant
3	When a warrant can be issued
4	When items can be seized without a warrant
5	Search of an arrested person
6	Authority to enter premises in interest of national security
7	Resisting arrest or search
8	Warrant must be issued who has authority to execute
9	Motion to return property/wrongful search/compensation
10	Wiretaps
11	Privacy - communications
12	Warrantless search
13	Expectation of Privacy
14	Meets the Katz requirements
15	Definitions
16	Privacy - other
17	Computer as closed container
18	Closed container
19	Private searches
20	Specialized technology use
21	Expectation of privacy in a personal computer
23	Third party searches
24	Exceeding scope of the warrant
25	Email privacy
26	Plain view doctrine
27	Self-Incrimination
28	Right to a speedy trial
29	Resisting Arrest or Search
30	National Security exception
31	Self-Incrimination

APPENDIX C – COPYRIGHT PERMISSIONS

Permission to use Figures 2 and 3

Hi Amelia,

You can use maps from here as its open source and free which i have dedicated to world community.

www.mapsopensource.com/namibia.html

Select the required map from here and can use it for any purpose. Please give courtesy or credit to mapopensource.

Regards

Emapsworld.com

Mapsopensource.com