

University of Dundee

DOCTOR OF PHILOSOPHY

**International Perspectives on Data Protection and its Relationship to Records Management
Recommendations for Emerging Practice in the West Indies**

Beckles, Cherri-Ann

Award date:
2014

Awarding institution:
University of Dundee

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

DOCTOR OF PHILOSOPHY

International Perspectives on Data
Protection and its Relationship to Records
Management

Recommendations for Emerging Practice in the West Indies

Cherri-Ann Beckles

2014

University of Dundee

Conditions for Use and Duplication

Copyright of this work belongs to the author unless otherwise identified in the body of the thesis. It is permitted to use and duplicate this work only for personal and non-commercial research, study or criticism/review. You must obtain prior written consent from the author for any other use. Any quotation from this thesis must be acknowledged using the normal academic conventions. It is not permitted to supply the whole or part of this thesis to any other person or to post the same on any website or other online location without the prior written consent of the author. Contact the Discovery team (discovery@dundee.ac.uk) with any queries about the use or acknowledgement of this work.



**THE UNIVERSITY OF DUNDEE
SCHOOL OF HUMANITIES**

SEPTEMBER 2014

***INTERNATIONAL PERSPECTIVES ON DATA PROTECTION AND ITS
RELATIONSHIP TO RECORDS MANAGEMENT: RECOMMENDATIONS FOR
EMERGING PRACTICE IN THE WEST INDIES***

CHERRI-ANN BECKLES

**Thesis submitted in the fulfilment of requirements of the
University of Dundee for the degree of Doctor of Philosophy**

TABLE OF CONTENTS

Acknowledgements	
Signed Declaration for Submission of Postgraduate Thesis	
Signed Statement by Supervisor	
Abstract	
Acronyms and Abbreviations	
INTRODUCTION	12
SECTION ONE	
<i>HISTORICAL CONTEXT AND BACKGROUND</i>	62
1. CHAPTER I	63
LITERATURE REVIEW	
1.1 Data Protection: Context, Origin and Development	
1.2 Data Protection and its Relationship to Records Management	
1.3 Conclusion	
2. CHAPTER 2	114
BACKGROUND TO THE WEST INDIES	
2.1 West Indies History - Early Period (17 th – 19 th Century)	
2.2 The Move towards Independence in the West Indies (1930s – 1960s)	
2.3 Post-Federal Attempts at Regional Integration	
2.4 West Indian Recordkeeping in Brief	
2.5 The West Indies: Law and Legal Systems	
2.6 Further Conclusions on the Literature	

SECTION TWO 147
MAIN FINDINGS

3. CHAPTER 3 149

INTERNATIONAL PERSPECTIVES ON DATA PROTECTION

3.1 Privacy/Data Protection ‘Models’

3.2 Data Protection in Germany

3.3 Data Protection in the United Kingdom

3.4 Privacy in the United States

3.5 Privacy in Canada

3.6 Privacy in Australia

3.7 Privacy in New Zealand

3.8 Conclusions

3.8.1 Assessing the ‘Models’

3.8.2 Assessing the Mechanics of the ‘Models’

SECTION THREE 222
CONCLUSIONS AND RECOMMENDATIONS

4. CHAPTER 4 223

**THE RELATIONSHIP BETWEEN DATA PROTECTION AND RECORDS
MANAGEMENT**

4.1 A New Records Management Approach for Data Protection - What Makes Personal
Records *Truly* Personal?

4.2 Implementing the ‘Life-story’ Approach in RM

4.3 The ‘Life-story’ Approach and Modern Records and Archives Theories

4.4 Key Records Management Concepts and Data Protection

4.5 Developing a Classification System for Personal Records

4.6 Other Key Considerations

4.7 Data Protection Terminology Relating to Records Management

- 4.8 Records Management Programmes and Data Protection
- 4.9 Developing Policies & Procedures in RM Programmes for DP
- 4.10 Key Records Management Mechanisms for Data Protection
- 4.11 Roles and Responsibilities for Data Protection: Who is Best Placed?
- 4.12 Data Protection and Archives Administration
- 4.13 Conclusion

5. CHAPTER 5

288

DATA PROTECTION AND RECORDS MANAGEMENT IN A DIGITAL WORLD

- 5.1 Being 'Remembered': The *Record's Life-story* in a Digital Age
- 5.2 Electronic Records and Data Protection
- 5.3 Electronic Personal Data and Security
- 5.4 'Cloud Computing' and Third Party Storage of Personal Data Across Borders
- 5.5 Identifying Electronic Records Types with Personal Data
- 5.6 The EU 'Right to be Forgotten': Principle vs. Practice
- 5.7 Conclusion

6. CHAPTER 6

312

DATA PROTECTION IN THE WEST INDIES: RECOMMENDATIONS FOR EMERGING PRACTICE

- 6.1 Why Data Protection: Key Drivers for Data Protection in the West Indies
- 6.2 The Challenge of Change: Main Obstacles to DP Implementation
- 6.3 Data Protection in the West Indies: An Integrated Approach?
- 6.4 Developing a West Indian Framework for Data Protection: Lessons Learnt
- 6.5 Recommendations to the West Indies

7. CHAPTER 7 352

CONCLUSIONS

7.1 Data Protection and Records Management: Where Are We Now?

7.2 Reflecting on the Thesis: Contribution to Knowledge

8. CHAPTER 8 361

FUTURE WORK

8.1 Addressing New Technologies and Concepts: Where Are We Going?

8.2 Enhancing Outreach and Educational Campaigns on Data Protection

8.3 Empowering Archivists and Records Managers to deal with Data Protection: The Role of the International Council on Archives (ICA)

7. BIBLIOGRAPHY 371

8. APPENDICES 397

Appendix 1 Semi-structure Interviews on the Relationship to Data Protection and Records Management

Appendix 2 Research Ethics Committee: Informed Consent for Interviews Form

Appendix 3 Timeline for Major Developments in Data Protection in the Selected Jurisdictions (1960 – 2012)

Appendix 4 Trajectory showing Impact of ICTs on Recordkeeping and Personal Data 1960-1980

Appendix 5 Timeline for British West Indies History (Post-Emancipation – Post-Independence)

Appendix 6 List of British West Indies Territories vs. CARICOM Territories

Appendix 7 Economic Partnership Agreement (EPA) Chapter 6, Title II, Protection of Personal Data

Appendix 8 General Privacy Principles from the Data Protection Act (2011) of Trinidad and Tobago

Appendix 9 Comments on Data Protection Policy/Bill from the Government Archivist of Trinidad and Tobago

Appendix 10 Extract from CARICOM Special Visa

A. List of Tables

- Table 1 Current Status of Archives Legislation vs. DP/Privacy Legislation (WI)
 Table 2 Data Protection in Selected Jurisdictions
 Table 3 Definitions of Personal Data in Selected Jurisdictions
 Table 4 Sample of Records Classification Schema with 'Flagged' Records Series for DP
 Table 5 Checklist to Meet Data Protection Requirements in RM Programmes
 Table 6 Activity Table for Archivists dealing with DP
 Table 7 Sample of Key Electronic Record Types with Personal Data

B. List of Diagrams

- Diagram 1 New Zealand Approach to Official vs. Personal Information
 Diagram 2 The Legal Effect of the EU Data Protection Directive
 Diagram 3 Elements of a Personal Record
 Diagram 4 Life-Cycle Management of Data Protection for RM
 Diagram 5 Frank Upward's Records Continuum and Personal Data
 Diagram 6 Levels of Privacy Protection for Organisational Records
 Diagram 7 The Passage of Recorded Personal Data into the Archives
 Diagram 8 Proposed Framework for Regional DP Regulation
 Diagram 9 Proposed Framework for Organisational DP Management

C. List of Images

- Image 1 Data Protection in Action at www.aujasus.wordpress.com/category/data-leak-prevention
 Image 2 Origin of the term 'data protection' – German at www.dreamstime.com
 Image 3 Photograph of London Delegation in 1953 compliments W.I. Federal Archives Centre
 Image 4 ICC Cricket World Cup 2007 Logo at www.cricketstar.net/cca/images/ICC%20quarterly_12%202005.pdf
 Image 5 The charming simplicity of Australia Data Protection at www.sangrea.net/free-cartoons/privacy-cartoons.html
 Image 6 Propaganda Poster – Big Brother is Watching (*US, 1984*) at www.typophile.com/node/82726
 Image 7 eH880 Secure Smart Card Terminal used in the German E-Health Programme at www.eh880.com/eh880.php
 Image 8 Data Breaches – Incident Types (UK)
 Image 9 Data Breach Maps at www.info@databreachmaps.com
 Image 10 Indiana University, Privacy of Medical Records at protect.iu.edu/privacy/cartoons
 Image 11 Cartoon on Privacy Impact Assessment at www.behance.net/gallery/Privacy-Cartoons/3754298
 Image 12 Internet Privacy at browertech.wordpress.com/category/internet-privacy
 Image 13 Diagram of Email Path from a POP Server at www.vimm.com/wp-content/uploads/2012/05/POP_diagram-email.jpg
 Image 14 Age Distribution on Social Networks & Online Communities at www.pingdom.com
 Image 15 Map of the West Indies and Central America (1910) at www.emersonkent.com/map_archive/central_america_1910.htm
 Image 16 Inauguration of the Caribbean Court of Justice (2001) at www.caribbeancourtofjustice.org
 Image 17 Google Glass at www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114

Acknowledgements

I wish to acknowledge the generous assistance of the Dean of the School of Humanities who enabled me to begin the course of study. This study would not have been possible without the support, guidance and encouragement of all the staff of the Centre for Archive and Information Studies at the University of Dundee, with special mention of the University Archivist, Mrs. Patricia Whatley and Records Manager/Compliance Officer, Mr. Alan Bell. I also would like to acknowledge Professor Jim Tomlinson and members of the various Thesis Monitoring Committees from the History Department for their guidance and for offering a wider perspective on the topic which enhanced my research findings. Additionally, I acknowledge the invaluable guidance of Professor Colin Reid who greatly assisted me in the final stages of the writing. I would like to thank the staff of The University of the West Indies (UWI) Archives and Records Management Programme, with special mention of the Campus Records Manager/Head Archivist Mrs. Sharon Alexander–Gooding and colleagues Dr. Stanley Griffin and Ms. Halcyon Wiltshire who supported my efforts and ensured that I completed the study in a timely manner. This appreciation I wish to extend to The UWI University Registrar, University Archivist and The UWI Cave Hill Campus Administrators who permitted me the required leave to conduct and complete my work. I would also like to thank Professor Alan Cobley, the then Coordinator of Graduate Studies at The UWI, Cave Hill Campus who would have offered me assistance in the initial stages with funding when needed.

Finally, I wish to extend my deepest thanks to my family, with special mention of my husband, Mr. Marvin Beckles, my mother Ms. Muriel Burton and my children Avani & Zoe Beckles for their unwavering support in every possible way.

Thank God!

Signed Declaration for Submission of Postgraduate Thesis

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Signature: _____

Date: _____

Signed Statement by Supervisor

I hereby declared that this submission has fulfilled the conditions of the relevant Ordinance and Regulations.

Signature: _____

Date: _____

Abstract

In the new millennium, West Indian territories began embarking on the introduction of information rights legislation such as Freedom of Information (FoI) and Data Protection. However, this type of legislation is proving challenging for West Indian nation states to implement. This thesis investigates the challenges faced by West Indian territories as it relates to the implementation of data protection legislation and explores the idea that these challenges are as a result of their historical background and developmental trajectory. Additionally, the thesis considers the implications of data protection for West Indian societies and a contextual account is undertaken to explain why data protection as a concept is misinterpreted, misunderstood or unknown by policy-makers and the citizenry at large.

Moreover, the study seeks to understand and explore whether the sub-standard management of records and information compared with internationally accepted standards, at all levels of West Indian society could be seen as a significant obstacle to the introduction of information rights legislation, in particular, the implementation, regulation and enforcement of data protection. The thesis analyses whether there is an irrefutable link between data protection and records management and if a sound records management environment would provide the required stability for the successful implementation of data protection at all levels.

In seeking to inform emerging practice in the West Indies, this is the first multi-disciplinary study that examines the provisions for data protection in select international jurisdictions from a records management perspective. The jurisdictions selected for examination are two European Union Member States, Germany and the United Kingdom as well as Canada, Australia and New Zealand where four distinct approaches for the implementation of data

protection have been identified. The study examines the core principles, policies, procedures and practices in these four models for data protection using a comparative approach. Thereafter, principally qualitative data is extrapolated towards the development of a framework for the implementation of data protection in the West Indies with a view of data protection's relationship to records management.

The thesis first interrogates how and why data protection emerged as a public issue across the selected jurisdictions in order to establish the main drivers in these societies. It examines the relationship between data protection and the management of records and information, particularly as it relates to the administration and use of the personal data of citizens by public and private agencies. It explores how new trends and advances in technology impact on data protection and records management in today's digital world. Using the data gathered, it identifies the main drivers and obstacles for the West Indies as they relate to data protection implementation and finally, what issues are expected to arise with the implementation of data protection and the management of records and information in future that would affect regions similar to the West Indies. Additionally, the comparative research makes a case for key solutions, mechanisms and strategies that would prepare professionals working with records and information for how to deal with data protection implementation in an increasingly technological environment in the West Indies.

Acronyms and Abbreviations

ACH	Association of Caribbean Archivists
ACP	African, Caribbean and Pacific States
CARBICA	Caribbean Branch of the International Council on Archives
CARICOM	Caribbean Community
CARIFORUM	Caribbean Forum of African, Caribbean and Pacific States
CARIFTA	Caribbean Free Trade Agreement
CCJ	Caribbean Court of Justice
CIA	Central Intelligence Agency
CSME	CARICOM Single Market and Economy
CTU	Caribbean Telecommunications Union
DoD	US Department of Defense
EU	European Union
FOI	Freedom of Information
HIPCAR	Project between CARICOM, CTU and ITU
IAPP	International Association of Privacy Professionals
ICC	International Cricket Council
ICA	International Council on Archives
IMF	International Monetary Fund
ITU	International Telecommunications Union
NSA	National Security Agency
OECS	Organisation of Eastern Caribbean States
RM	Records Management
UN	United Nations
UWI	The University of the West Indies
WTO	World Trade Organization

INTRODUCTION

'The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems'

U.S. Privacy Protection Study Commission 1977

'Data protection', a term arising from European nomenclature is informed by the broad value called 'privacy'.¹ Privacy conveys different meanings to varying groups of people based on their social, political, economic and historical background. Privacy is therefore highly subjective and its interpretation changes over time and space. Many English-speaking nations used the term 'privacy' to describe statutes that essentially perform the same functions as European data protection laws. The term 'privacy' and 'data protection' are at times used interchangeably, however, *data protection* refers more specifically to the group of policies and regulations designed to control the collection, storage, use and transmittal of personal information.² Data protection is the preferred term used in this thesis as this term has been chosen for use in legislation being introduced in the West Indies to date.

This study aims to contribute new and unique evidence of the relationship between data protection and records management. It investigates the emergence and development of data protection as a public policy within selected international jurisdictions from a records management perspective in order to inform emerging practice in the West Indies. In doing so, it identifies the main factors influencing the perceived need for data protection and explores its relationship to recordkeeping and the practice of records management with a view of contributing new knowledge on how this relationship can facilitate and support the

¹ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), pp. 12-13.

² Bennett, pp. 12-13.

successful implementation of data protection management in the West Indies region and beyond.

Thesis Statement and Research Questions

This section presents the thesis statement and central research questions that shaped the investigation of the topic. The thesis statement for this study is; *the West Indies needs to exploit the relationship between data protection and records management in order to successfully implement data protection legislation*. This statement gives rise to two central questions: 1) How does the relationship between data protection and records management affect what is needed to achieve effective data protection in the West Indies? and, 2) What lessons can be learnt for the specific context of West Indies from the selected international jurisdictions?

The sub-questions in the investigation that tackle the three main research themes, namely, the origin and development of data protection legislation, the relationship between data protection and records management and the recommendations for emerging practice in the West Indies, are:

Data Protection Legislation: Origins and Development

- Why, when and how did data protection/privacy arise in each jurisdiction?
- How is data protection and privacy defined?
- What are the underlying principles?
- What law(s) exists within each selected jurisdiction that deals with data protection and privacy?
- How is data protection/privacy legislation interpreted in each jurisdiction?
- Is there a single Data Protection Authority? (“One-stop shop”)
- What are the key mechanisms for enforcing the legislation at a regional, national and institutional level?

- In what ways is data protection policed in each jurisdiction?
- What are the strengths and weaknesses in data protection implementation?

The Relationship between Records Management and Data Protection

- How does data protection legislation impact on recordkeeping?
- How does data protection legislation relate to records management in principle and in practice?
- Who in the organisation deals with data protection as it relates to the organisational records and information?
- Is there a Code of Practice for data protection relevant to the work of the Records Managers and Archivists?
- If there is a code, does it require revision?
- How should Records Managers and Archivists comply with data protection?
- How do new trends and devices in the digital world which impact on recordkeeping affect data protection management?
- Are there direct ways in which records management could improve data protection management at an organisational level?
- Why is it necessary for collaboration between Records Managers and other professionals?

Recommendations for emerging practice in the West Indies

- What are the main obstacles which have resulted in slow adoption of data protection laws in the West Indies?
- What makes the West Indies unique as a region?
- Is there existing jurisprudence in the West Indies regarding the protection of personal information?
- What is the recordkeeping tradition(s) in the West Indies?
- How does this recordkeeping tradition impact on the implementation of data protection?
- Does the West Indies require the development of data protection regime?
- What are the main drivers for the West Indies?

- Is there a coordinated regional effort at regulating data protection?
- What lessons could be learnt from the EU, US, Canada/Australia, New Zealand models?
- Which privacy/data protection approach is most adaptable and suitable for the West Indies to emulate, if any?

Where the literature was not forthcoming, answers were gleaned from reports, newspapers, official websites and other internet sources as well as interviews, site visits and observation. The selection of sources will be discussed in the following section which deals with the research methodology and an assessment of the methodology will be undertaken.

Research Methodology

This section introduces and explains the research methodology used in the thesis that led to its findings and conclusions. The data collection and analysis is based predominately on qualitative sources which include a review of literature and other written sources as well as related images, extensive interviews, an on-line survey, site visits, observations and a brief internship. Most importantly, a review of privacy and data protection legislation and regulatory provisions from the selected jurisdictions was undertaken.

The Theme of Technology

Technological change is a recurring theme throughout the study. This thesis argues based on findings that dramatic societal changes due to revolutionary advances in technology caused an environment to evolve where the loss of control in the management of records and information increased risks of unwarranted disclosure. However, what is more important to this thesis is how technology influenced societal changes including changes in human and institutional behaviours as it relates to the creation, collection and use of records and information. As result of this focus on changes in human and institutional behaviours, it was decided that an examination of key literature on sociological findings in the period of the

1960s would provide critical background information. Therefore the theories examined, 'post-industrialism', 'information society' and 'the control revolution', were included in the study to provide insight into the context in which the need for data protection emerged.

In addition, this study sought to understand the main drivers for countries to begin implementing data protection at that point in history. The literature covering the topic of sociology in the first phase of data protection development strongly supports the argument that technology was the principal catalyst for change. The changes that took place heightened fears and concerns amongst citizens in information-driven societies with regard to how their personal data was being collected, stored and used by both public and private organisations.

Selection of Literature

Although the core discipline of study is records management, it was recognised at an early stage that an examination of key texts in other disciplines had to be undertaken in order to establish the context in which data protection as a policy arose. A search for texts on the topic of data protection/privacy was conducted and this resulted in the discovery of literature in disciplines such as law, political science, public policy and sociology. The search also revealed that there is very little written on the topic of data protection/privacy in the discipline of records management itself. Hence, an early conclusion was reached that this study had to examine the topic of data protection starting with disciplines outside records management to fully comprehend its depth.

The texts examined on the topic of data protection and discussed later in this chapter, quickly revealed that data protection as a public policy arose in the period of the 1960s. It was then necessary to examine the factors that led to this policy becoming increasingly

important at that point in history. There was also an underlying idea in the readings that the behaviour and expectations of citizens and organisations were changing in the 1960s. This led to an examination of key sociology texts written in the period of the 1960s in an attempt to understand why these societal changes were occurring.

The ideas in the literature were supported by newspaper articles of the period, mainly within the United Kingdom, which are made accessible through the University of Dundee Library, British Library, Newspaper Archives and The National Archives of the UK. The use of newspapers was particularly useful where the literature did not provide enough information about the concerns raised by citizens and the responses to threat to data protection/privacy. These articles provided evidence that citizens began to clamour for their personal data to be protected from misuse due to the increased usage of rapidly advancing technology.³

In the years to follow the rise of data protection/privacy as a public policy, the writings of a new generation of privacy advocates discussed later in this chapter were found to be useful in providing insight into their views as the causes for what they refer to as the 'threat to privacy'. Examining key text from recognised privacy advocates helped to shape the idea that solutions to this problem should be multi-disciplinary and a collaborative approach would be required. However, a strong case for the inclusion of records management in this discourse was still evident.

Privacy advocates are increasing in number and now have a firm standing as professionals through associations like the International Association of Privacy Professionals. In recent

³ See list of newspapers in the Bibliography at p. 380.

times, much of the writings on data protection in the field of privacy management can be found in online sources in the form of e-newsletters, blogs, e-journals, reports and articles.

The literature also led to the search for primary sources, mainly official reports from various government committees and private groups formed to review and provide solutions to what was considered a privacy problem across the selected jurisdictions. A search of the various governmental agencies responsible for data protection/privacy in the jurisdictions, e.g. Ministry of Justice, also led to the discovery of governmental reports. These reports, discussed in the literature review, confirm that the issue of data protection/privacy in records and information was seen as an area that needed to be addressed at the highest levels of society.

Ultimately, the study's initial intent to explore whether there is a significant relationship between data protection and records management was validated. The thesis went further to examine whether records management is compulsory and inescapable in protecting the personal information of citizens in the changing environment described by sociologists, legal experts, political scientists and privacy advocates. The study recognises that one discipline alone cannot provide all the answers or even knows all the questions to be asked when dealing with data protection/privacy. The literature review is therefore an attempt to distil the main ideas that influenced the conclusions and recommendations in this complex and multifaceted study.

Main Literature

The main sociological theorists examined include Alain Touraine's text, *The Self Production of Society*,⁴ Alvin Toffler's text, *Creating a New Civilization: The Politics of the Third Wave*,⁵

⁴ Alain Touraine, *The Self-Production of Society* (Chicago, 1997).

Frank Webster's work, *Theories on the Information Society*⁶ with references made to futurist writings and sayings of Herman Kahn. However, it was the writings of notable sociologist Daniel Bell in his seminal work on the 'post-industrial society' entitled, *The Coming of Post-Industrial Society: A Venture into Social Forecasting*⁷ that has been used extensively in the background of the study. Bell's writings best explain and describe the impact of the shift to information-based economies and how the collection and use of records and information became the new 'engine' of societies. Additionally, the theory of the 'control revolution', a term coined and explained by James Beniger in his work, *The Control Revolution: Technological and Economic Origins of the Information Society*,⁸ is also useful in understanding societal shifts in the early period of data protection development. It helped to shape the argument that modern societies became dependent on technology to control workers in organisations as well as the populace. This idea is explored fully in Chapter 1 of the thesis.

The study also reflects on the writings of Alan Westin, who is referred to as the 'pioneer of privacy' by privacy experts. In his 1967 work entitled, *Privacy and Freedom*,⁹ Westin provides extensive insight into the threat to privacy as a result of growing technology. In subsequent articles, such as *Social and Political Dimensions on Privacy*,¹⁰ he chronicles the steadily growing privacy concerns from what he refers to as the 'privacy baseline' in the period of the 1940s up until the 'post-9/11' period in 2002. His writings support the argument in the study that public trust in government and business began to decline in modern, societies due to how technology began to be utilised. For example, in 2013,

⁵ Alvin Toffler, *Creating a New Civilization: The Politics of the Third Wave* (Nashville, 1995).

⁶ Frank Webster, *Theories on the Information Society* 4th ed. (London, 2014).

⁷ Daniel Bell, *The Coming of Post-Industrial Society: A Venture into Social Forecasting* (New York, 1976).

⁸ James Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Boston, 1986).

⁹ Alan Westin, *Privacy and Freedom* (London, 1970).

¹⁰ Alan Westin, 'Social and Political Dimensions', *Journal of Social Issues*, Vol. 59, No. 2, 2003.

Reuters reported that a poll showed that 73% of US citizens distrust the US government due to its spying activities along with its other actions and decisions.¹¹ This idea is bolstered by writings of James Rule in his work, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*,¹² which deals with issues of the politics of privacy and discusses whether privacy is in peril in the digital world due to intrusive surveillance devices and software.

However, it is political scientist, Colin Bennett who has done extensive writing in the area of privacy protection and surveillance technologies. His work is recognised and cited by Westin. Bennett's key text that bears relevance to this study is *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*.¹³ In this book, Bennett provides a history of the development of privacy but goes further by comparing and contrasting two differing data protection regimes, Europe and the United States highlighting commonalities and divergences in the two approaches. This study discusses four global models for data protection and so Bennett's text provides significant insight into two of these four models. The study effectively demonstrates that the approaches of Europe and the United States are furthest apart in terms of compatibility hence the introduction of a 'Safe Harbor Agreement' was necessary and will be discussed in the literature review.¹⁴

Literature on Records Management and Archival Studies

It was imperative to this study to conduct a review of literature on archives and records management in order to understand these disciplines in principle and practice and how they

¹¹ Reuters, *Three quarters of Americans distrust the government* at rt.com/usa/government-trust-americans-poll-172. Accessed on 24 April 2014.

¹² James Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Missouri, 1981).

¹³ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992).

¹⁴ Literature review, p. 62.

relate to data protection. In seeking to provide evidence that there is an irrefutable relationship between records management and data protection, a number of key matters had to be examined. Records management has also been influenced by significant technological changes. The discipline arose in the same period as data protection due to societal changes. At the 'heart' of both pursuits is the issue of loss of control and both are responses to dealing with regaining control of records and information.

One of the first issues that had to be examined in the study is defining the term 'record'. This definition has changed over time and the concept of a record has become wider ranging in the digital world. For example, the traditional view of what is a record in the European tradition of diplomatics and archival studies has predominantly been written documents. However, in technologically driven societies since the 1960s, records include data (structured and unstructured) captured in databases, electronic mail, instant messages, closed circuit television footage, digital camera images and entries on social media sites. In addition, in today's socially driven societies, the creation and dissemination of personal information is happening in unprecedented ways as individuals are more empowered to create and share information about them and the technology is becoming increasingly intrusive.

An examination of notable works used in the discipline of records and information management and the related, older discipline of archival studies provided the basis for understanding societal changes that impact on recordkeeping. The main texts used include Laura Miller's recent study, *Archives Principles and Practices*;¹⁵ Robek et al *Information and Records Management: Document-based Information Systems*;¹⁶ Ira Penn et al, *Records*

¹⁵ Laura Miller, *Archives Principles and Practices* (London, 2010).

¹⁶ Mary F. Robek et al, *Information and Records Management: Document-Based Information Systems* 4th Edition (California, 1995).

Management Handbook,¹⁷ Ricks, Swafford & Gow's work, *Information and Image Management: A Records Systems Approach*.¹⁸ The writings of Luciana Duranti, *Diplomatics: New Uses for an Old Science*¹⁹ and Geoffrey Yeo's article, *Records and Representations* also provided sound insight into the elements and characteristics of records from the beginnings of archival studies to the present.²⁰ Yeo's subsequent article, *Concepts of Records (2): Prototypes and Boundary Objects* builds on the complex concept of what is a record using the sociological notion of 'boundary objects' to demonstrate how the same records have different meanings to different groups, communities or individuals.²¹

Other articles were used in this study to understand key concepts in records management including the Australian concept of the Records Continuum.²² This thesis asserts that the responsibility of data protection management is one of the functions inherently being carried out by archivists and records managers within organisations. Records management remains very relevant in dealing with data protection because the core concepts and practices that underpin the discipline, intentionally or unintentionally, safeguard records and information regardless of format and technological change. In light of this reasoning, the study incorporates or further embeds data protection activities into the core concepts, both in the stages of traditional 'life-cycle' or 'cradle-to-grave' management of records²³ as well as Frank Upward's *Records Continuum Concept* which is described in an article, 'Structuring the Records Continuum Part 1 & 2'.²⁴ Sue McKemmish's *Yesterday, Today and*

¹⁷ Ira Penn, et al, *Records Management Handbook*, 2nd ed. (Vermont, 1994).

¹⁸ Ricks, Swafford and Gow, *Information and Image Management: A Records Systems Approach* (Ohio, 1992).

¹⁹ Luciana Duranti, 'Diplomatics: New Uses for an Old Science', *Achivara* 28 at journals.sfu.ca/archivar.

²⁰ Geoffrey Yeo, *Records and Representations*, Paper presented at the Conference on the Philosophy of Archive, Edinburgh, Scotland, 10 April 2008.

²¹ Geoffrey Yeo, 'Concepts of Record (2): Prototypes and Boundary Objects', *American Archivist* 70/2 (Fall/Winter 2007), pp. 315-343.

²² See 3.2 in Chapter 3.

²³ Description by ARMA International found at www.arma.org.

²⁴ Frank Upward, 'Structuring the Records Continuum Part 1 & 2', *Archives and Manuscripts* 24 & 25 (Monash, 1996-1997).

Tomorrow: A Continuum of Responsibility further explains the concept of the continuum as providing a framework for the management of records to be shared by all records professionals without the artificial separation of roles.²⁵ The idea that both archivists and records managers should be at the fore in the quest to safeguard personal data in records within their care is explored in Chapter 4.

Terry Cook and Joan Schwartz's article, *Archives, Records and Power: The Making of Modern Memory* was considered to explain the power of archivists in shaping society's history and collective memory.²⁶ The thesis argues that records, particularly personal records, are powerful. They are used to control the lives of people in ways that affect their standard of living, their ownership of property, their overall treatment in society, their access to rights, how they are remembered, their reputation and their dignity. Personal records control one's existence in society at large. This idea is fully supported by writings of Eric Ketelaar in the article *Archival Temples, Archival Prisons: Modes of Power and Protection*²⁷ and Verne Harris', *The Archival Sliver: Power, Memory, and Archives in South Africa* which show how authorities use records to control the lives of people; in some cases, to regulate and support citizens and in other cases, to dominate and control citizens.²⁸

However, very little is written to reinforce one of the key points made in the thesis that inherent in archives and records management is the concept that data, in particular confidential and private data, must be protected in order to protect the lives of people.

Menzi Behrnd-Klodt's, *Privacy & Confidentiality Perspectives: Archivists & Archival Records*

²⁵ Sue McKemish, *Yesterday, Today and Tomorrow: A Continuum of Responsibility*, Article in the Proceedings of the Records Management Association of Australia 14th National Convention, Perth, September 1997.

²⁶ Terry Cook and Joan Schwartz, *Archives, Records and Power: The Making of Modern Memory*, *Archival Science* Vol. 2, Issue 1-2.

²⁷ Eric Ketelaar, 'Archival Temples, Archival Prisons: Modes of Power and Protection', *Archival Science* 2: 221–238, (2002).

²⁸ Verne Harris, 'The Archival Sliver: Power, Memory, and Archives in South Africa', *Archival Science* 2: 63–86, (2002).

represents the only full text in the discipline of records and archives management that makes a clear link between the role of archives and records in privacy protection.²⁹ This text most comprehensively discusses why privacy issues need to be addressed within archival institutions. However, while this text looks at the philosophical and ethical reasons for managing privacy in archives, it does not adequately address privacy in the active and semi-active phases of records management. Therefore, this study is the first one in the discipline of records and information management studies to give a wider perspective on the issue of privacy and European data protection while addressing why and how to deal with these issues in records management as well as archives management programmes.

Another useful and related study in the form of a research project funded by the Arts and Humanities Research Council and conducted by the Department of Information Studies at the University College London (UCL) examines the role of the records manager when dealing with Freedom of Information (FoI) legislation. This project, led by Professor of Archives and Records Management Elizabeth Shepherd, asserts that records managers have a part to play in compliance with FoI in public authorities. It also examines how FoI legislation impacts on records management services in a similar way to how this study examines how data protection relates to records management. It makes the case that professionals should work together 'to deliver more credible and reliable records and data to citizens'.³⁰ Correspondingly, this study supports the view that ensuring data protection compliance at an institutional level should take an integrated approach involving all stakeholders or functionaries that interact with personal data. This view is explored in Chapter 4.

²⁹ Menzi Behrnd-Klodt, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005).

³⁰ Elizabeth Shepherd, Alice Stevenson and Andrew Flinn, 'The Impact of Freedom of Information and Records Use in Local Government: A Literature Review', *Journal of the Society of Archivists* Vol. 30, Issue 2 (2009).

Literature on West Indian History

It was decided that to truly understand the complexities of the West Indian region as it stands today, a review of literature in West Indian history would need to be undertaken. Further, this study examines whether these complexities in West Indian history and development have in some way affected the implementation of data protection in the present time. The development of the topic cannot be properly explored without examining this area. It was then necessary to examine the historical, social and political developments which could mainly be found in British West Indies historiography. Some other writings in disciplines such as law, political science and economics were taken into account. The historical trajectory of the region provides answers as to why there are obstacles to implementing information rights legislation and why it is critical to the region's competitiveness and economic growth for it to overcome those obstacles in today's global environment. However, it was discovered at an early stage in the study that the historical literature, in the main, covers the period of the early settlement of the colonies, the slave trade and the plantation economy, the abolition of slavery and the immediate post-emancipation period. This meant that a heavy reliance on other sources would be necessary to understand post-independence (post-1960s) history.

The notable Caribbean history texts that speak to the existence and legacy of colonialism in the West Indies include Richard B. Sheridan's *Sugar and Slavery: An Economic History of British West Indies 1623-1775*;³¹ William A. Green's *British Slave Emancipation: The Sugar Colonies and the Great Experiment 1830-1865*;³² Richard Dunn's *Sugar and Slaves: The Rise*

³¹ Richard B. Sheridan, *Sugar and Slavery: An Economic History of British West Indies 1623-1775* (Kingston, 1994).

³² W.A Green, *British Slave Emancipation: The Sugar Colonies and the Great Experiment 1830-1865* (Oxford, 1976).

of the Planter Class in the English West Indies 1624-1713;³³ Elsa Goveia's *A Study of the Historiography of the British West Indies to the end of the Nineteenth Century*;³⁴ Roy Augier's *Before and After 1865: Education, Politics and Regionalism in the Caribbean*;³⁵ Hilary Beckles and Verene Shepherd's *Caribbean Freedom: Economy and Society from Emancipation to the Present*;³⁶ Bridget Brereton's *Social Life in the Caribbean 1838-1938*³⁷ and Eric Williams' *From Columbus to Castro: The History of the Caribbean 1492-1969*.³⁸ Collectively, these texts unearth the factors that shape West Indian society, culture and identity.

Although there are new and upcoming historians, some of whom are members of the present-day, research-driven Association of Caribbean Historians (ACH) and are making notable contributions to West Indian historiography, a review of the literature reveals that there is still a dearth of writing on the post-independence period (post-1960s) of the West Indies, the period of interest in this thesis. In addition, the history has not adequately addressed the administrative and related legal aspects of West Indian society. Founding member of the Association of Caribbean Historians (ACH) and Emeritus Professor of History, Sir Woodville Marshall states that, 'West Indian historians simply do not see the appeal [at this time] in extensive writing about the development of administrative structures in Caribbean societies'.³⁹

³³ Richard Dunn, *Sugar and Slaves: The Rise of the Planter Class in the English West Indies 1624-1713* (Williamsburg, 1972).

³⁴ Elsa Goveia, *A Study of the Historiography of the British West Indies to the end of the Nineteenth Century* (Washington, 1956).

³⁵ Roy Augier, *Before and After 1865: Education, Politics and Regionalism in the Caribbean* (Kingston, 1998).

³⁶ Beckles, Hilary and Shepherd, Verene, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996).

³⁷ Bridget Brereton's *Social Life in the Caribbean 1838-1938* (London, 1985).

³⁸ Eric Williams, *From Columbus to Castro: The History of the Caribbean 1492-1969* (New York, 1970).

³⁹ Based on interview with an Emeritus Professor of History at The University of the West Indies, Sir Woodville Marshall.

The text by J. H. Parry et al entitled, *A Short History of the West Indies*, could be considered the work which comprehensively covered the broadest timeframe on West Indian history.⁴⁰ Hence this text is used to explain the West Indies long and complex history in the most succinct way. The writings of Roy Augier in *Before and After 1865: Education, Politics and Regionalism in the Caribbean* are the most enlightening on the impact of the colonial system on the formation of administrative structures that developed amongst the territories. Most importantly, his writings although focused on Jamaica, could be applied to the situation that arose in the other British territories in the immediate post-independence period.⁴¹ The region was left to carry on a type of administrative style that was not fully understood by the new working class made up predominantly of the descendants of former slaves and peasant workers. Many required skills and knowledge were not passed on and had to be acquired in universities outside of the region. In the case of records and information management as a discipline and profession, this situation remains so up until today.

This study makes the case for sound records management as providing the right foundation for information rights including data protection. Information rights cannot be upheld where there is no proper records and information management environment for the simple reason that if records and information cannot be found as a result of poor classification systems or are indiscriminately damaged and destroyed and are not stored securely; it does not bode well for administering legislation such as freedom of information or data protection. In other words, accountability and transparency are lost in this type of *ad hoc* environment. Unfortunately, many territories in the region continue to grapple with the effects of poor record-keeping and the lack of proper records management systems and expertise.⁴²

⁴⁰ Parry, J.H., *A Short History of the West Indies* 4th ed. (Oxford, 1987).

⁴¹ Roy Augier, *Before and After 1865: Education, Politics and Regionalism in the Caribbean* (Kingston, 1998).

⁴² Based on experience gathered as a trained archivist and a regional records and information management consultant from 2003 – present.

In further examining the legacy of the colonial system, Eric Williams' economic history *Capitalism and Slavery*,⁴³ which focuses on the abolition of slavery and is recognised among West Indian historians as one of the greatest pieces of historical writing on the region was utilised in the study. The differing view of Williams A. Green's *British Slave Emancipation: The Sugar Colonies and the Great Experiment 1830-1865*⁴⁴ was considered for a wider perspective. These texts support the argument that a 'vacuum' of knowledge and skills was left behind as it relates to the governance of the region when the colonial powers shifted focus from economic gains derived from the region's plantation economy.

The most relevant text on the impact of the colonial system on record-keeping in the West Indies to date is the writings of Jeannette Bastian in her work, *Owning Memory: How the Caribbean Community Lost its Archives and Found its History*.⁴⁵ Although Bastian's work addresses the Danish West Indies, the situation was very similar in the British West Indies. No other writings adequately address the reasons for the poor creation and management of records in the region in the post-independence period. She speaks of the 'voiceless-ness' of the colonised who are under-represented in the records and the tensions between the written and oral traditions. The records in these societies serve the purpose of maintaining the status quo of one group being dominant over another and do not adequately reflect the true histories of all groups of people within the society. The thesis discusses the implications of this for the treatment and use of personal records in the West Indies in Chapter 5. Finally, the report from the 1965 Conference of Historians on Caribbean Archives at the Mona Campus in Jamaica offers a reliable representation of the status of recordkeeping in the

⁴³ Eric Williams, *Capitalism and Slavery* (Cambridge, 2004).

⁴⁴ Williams A. Green's *British Slave Emancipation: The Sugar Colonies and the Great Experiment 1830-1865* (Oxford, 1991).

⁴⁵ Jeannette Bastian, *Owning Memory: How the Caribbean Community Lost its Archives and Found its History* (Westport, 2003).

Caribbean at that time. This report was compiled based on papers from historians with an interest in archival materials and some expatriate archivists employed to coordinate the first attempts at establishing archival institutions across the region including the French, Dutch and Spanish West Indies. However, with the absence of substantial research and writing on recordkeeping and archives since then, there is a heavy reliance on interviews in this study which will be discussed in a following section.

This thesis represents the first attempt to link the history and legacy of the colonial system in West Indian territories to the management of its records and information including those containing personal information. Essentially one of the main arguments of the thesis is that in these slave societies, where a large proportion of the population were slaves, personal information on individuals, which mainly took the form of slave registers, was not protected. Slaves were considered the property or chattel of the planter class and the concepts of human rights in general and the 'right to privacy' were not recognised or upheld until long after emancipation well into the post-independence period.⁴⁶

The writings of noted political scientist Gordon K. Lewis including in his work, *The Growth of the Modern West Indies* were considered.⁴⁷ This text, first published in the 1960s, examines the political and social make-up of individual territories and provides insight into the dynamics of the region in a unique style. It aided with understanding the factors influencing why the Federation 'experiment' failed and the challenges of independence. The work of Cynthia Barrow-Giles, *Introduction to Caribbean Politics*, gave a succinct account of political systems and developments in the region's post-independence period including attempts at

⁴⁶ The information is fully explained in Chapter 5 when dealing with the obstacles to implementation of data protection in the West Indies.

⁴⁷ Gordon K. Lewis, *The Growth of the Modern West Indies* (Kingston, 2004).

integration.⁴⁸ Caribbean economist George L. Beckford in his book, *Persistent Poverty: Underdevelopment in Plantation Economy of the Third World*⁴⁹ and Norman Girvan in his article entitled, *The Quest for Regional Integration in the Caribbean – Successes and Challenges*⁵⁰ both offer perspectives on the economic realities faced by the region since independence and how these impact on its attempts at regional integration. The study is concerned with the question of regional integration as it explores the most suitable approach that should be taken to developing a framework for data protection implementation.

Finally, another aspect of regional development that needed to be explored is the development of Caribbean law and legal systems. The study seeks to understand whether the existing legal tradition in the region would allow for successful implementation of data protection. Three main authors were used towards this end. Fred Phillips' *Commonwealth Caribbean Constitutional Law*,⁵¹ Rose-Marie Bell Antoine's *Commonwealth Caribbean Law and Legal Systems*⁵² and Albert Fiadjoe's *Commonwealth Caribbean Public Law*⁵³ provided valuable information about the influences, history and development of the legal tradition of the region. They demonstrate that the region has developed its own localised style of administering law in spite of its origin in the common law tradition. This in itself would have implications for implementing information rights legislation such as data protection and will be discussed in Chapter 5.

⁴⁸ Cynthia Barrow-Giles, *Introduction to Caribbean Politics* (Kingston, 2002).

⁴⁹ George L. Beckford, *Persistent Poverty: Underdevelopment in the Plantation Economies of the Third World* (Kingston, 2000).

⁵⁰ Norman Girvan, *The Quest for Regional Integration in the Caribbean – Successes and Challenges*

⁵¹ Fred Phillips, *Commonwealth Caribbean Constitutional Law* (London, 2002).

⁵² Rose-Marie Bell Antoine, *Commonwealth Caribbean: Law and Legal Systems* 2nd ed. (New York, 2008).

⁵³ Albert Fiadjoe, *Commonwealth Caribbean Public Law* (New York, 2008).

Other Sources of Writing

The subjects of privacy and data protection are very dynamic and topical areas of discussion in today's digital world. As global citizens become more aware of how their privacy is under threat, debates and discussions are happening on a weekly, if not daily basis in several parts of the world evidenced by international news reports in all forms of media as well as television and radio talk shows. In order to keep abreast of the trends and debates on privacy and data protection, it was necessary to examine other sources of writing including journals, newsletters, reports, professional magazines, brochures, television and radio news reports and newspapers in print and online. These sources were useful to track changes in the perception of privacy and data protection over time among the citizenry, professional groups and privacy advocates. Additionally, in today's digital age, information which was once made available in traditional print format is now widely disseminated online. A substantial amount of current information was gleaned from the Internet in the form of websites, blogs, Listservs (electronic mailing lists), daily posts, wikis and social media sites.⁵⁴ In these cases, the information was taken from reliable and well-informed sources in established professional groups/associations or relevant public offices.

Personal Experience and Observations

As a result of the dearth of information about the status of record-keeping in the West Indies, the author has had to include her personal experience and observations made throughout her career in archives and records management. The author has worked in the heritage sector since 1995, served as a trained Government archivist, regional university archivist and regional consultant in archives and records management since 2003. She has had brief stints at archives and records management offices at the University College

⁵⁴ These sources helped to inform the case studies in the data protection models in Chapter 3 and the discussion on data protection in the digital world in Chapter 5.

London (UCL) and the University of London, Institute of Education. In addition, she has served as President in a local (Barbados) records management association and is a sessional lecturer in a Certificate in Records Management course and the Masters in Heritage Studies programme at The University of the West Indies since 2004. She currently serves as the Communications Officer for the Caribbean Branch of the International Council on Archives (CARBICA), a member of the United Nations Educational, Scientific and Cultural Organisation (UNESCO) Memory of the World Committee - Barbados Commission and has been nominated to serve on the Executive Committee of the International Council on Archives, Section for University and Research Institutions (SUV) Archives in 2014. The experience and knowledge gained during her career as well as interviews with other professionals provided much needed insight into the realities of record-keeping in the West Indies region in light of the lack of written sources. This career experience also informs Chapter 3 of the study where the relationship between data protection and records management is explored.

Interviews

One of the principal means of gathering data in the study was to conduct interviews. Twenty-nine semi-structured interviews, both formal and informal in nature, were conducted as part of the research for the thesis across the selected jurisdictions. Formal interviews occurred when the interviewee agreed to be interviewed in advance. These interviewees signed the Informed Consent Form of the University of Dundee, Research Ethics Committee and agreed to be recorded by use of a digital Dictaphone.⁵⁵ Interview questions were designed and approved through the ethical approval process provided by the University of Dundee. The anonymity of interviewees who signed the agreement is protected. In two instances, a few adaptations were made to these forms by the

⁵⁵ See Appendix 1 Informed Consent Forms, p. 400.

interviewees. Informal interviews were conversations which took place when opportunities arose for discussion with individuals who have knowledge of the subject. In these cases, the interviewee was informed about the study and reason for the discussion but did not sign the Informed Consent Form. These informal interviews although unplanned enhanced the data collection process. The author sought to treat information derived from both formal and informal interviews in a manner that would not reveal unnecessary personal information about interviewees in keeping with data protection principles.

The interviews were captured as stored recordings from the digital Dictaphone and in handwritten notes which are in part of the collection of data held by the author. The recordings and notes were used in this study but will not be shared or re-used for a purpose beyond this study without the consent of the interviewees. Some direct quotes are included in the work while preserving the anonymity of the interviewee, particularly in cases where the Informed Consent Form was signed. The selection of interviewees is discussed in the following section.

Selection of Interviewees

The interviewees were selected based on the main theme under investigation, that is, the relationship between records management and data protection. This was closely followed by the selection of experts in the legal world who interface with data protection and privacy within their respective regime. The author chose to use semi-structured interviews to glean as much information as possible from interviewees. Two sets of semi-structured interviews were designed: 1) to target professionals working in the field of records and archives management dealing with data protection/privacy, principally archivists and records

managers in the selected jurisdictions⁵⁶ 2) To assess the current state of data protection in the West Indies.⁵⁷ The author also targeted four Freedom of Information (Fol) officers in the UK who interact with data protection to understand how data protection interfaces with Fol legislation. In some cases, targeted individuals directed the interviewer to other professionals within their organisations who they felt could add to the data. This helped to enrich the data collection experience. An assessment of interviews is conducted in the following section.

The author visited four countries in three jurisdictions in order to conduct face-to-face interviews namely, the UK and Germany as part of the European Union; Canada and the US. The lack of funding and constraints with time prevented the author from visiting Australia and New Zealand. She also attempted to conduct interviews wherever possible in the West Indies namely, Barbados, Jamaica, Trinidad and Tobago, St. Lucia, Dominica and Guyana. Where face-to-face interviews were not possible, other means such as the telephone and email were utilised. This resulted in seventeen interviews (sixteen formal and one informal) in the selected jurisdictions and twelve interviews (four formal and eight informal)⁵⁸ in the West Indies region. The main challenge encountered with interviews was as a result of some individuals stating that they did not know enough about data protection and its relationship to records management to carry out a meaningful interview. Other targeted interviewees could not be reached. Although the author did not get to interview all of the individuals targeted in the selected jurisdictions and the West Indies,⁵⁹ the information gleaned from the twenty-nine interviews conducted formed a good basis for reaching conclusions in the study.

⁵⁶ See Appendix 2 PhD Semi-structured interview - Jurisdictions, p. 397.

⁵⁷ See Appendix 2 PhD Semi-structured Interview – West Indies, p. 398.

⁵⁸ One interviewee, Sir Shridath Ramphal, was interviewed twice, formally and informally by telephone.

⁵⁹ The author aimed to target twenty individuals in the jurisdictions and fifteen in the West Indies.

Online Survey

In addition, an online survey was designed based on the semi-structured interview questions using the University of Bristol Online Survey (BOS). This survey was launched for two months at the end of the year 2012 and closed on 1st January 2013.⁶⁰ The survey was distributed to the mailing list of the members of the Scottish Higher Education Information Practitioners (SHEIP) using a University of Dundee contact.⁶¹ There were only four respondents to the online survey and so the information was inconclusive. However, the survey still proved useful to the data collection because two of the respondents agreed to be interviewed. One face-to-face interview was conducted and one telephone interview was conducted. One of the interviewees works at a large-sized (upwards of 10,000 students) Scottish university and the other at a mid-sized Scottish university. Both interviews provided insight into the challenges faced with implementing data protection management within the specific sector of higher education institutions (HEIs) in Scotland.

Interviews in PhD Internship

The internship at Tate Britain provided invaluable first-hand experience on how to deal with data protection at an organisational level. The author was allowed to fully participate in staff general meetings as well as FoI Committee groups meetings. This provided first-hand experience with how data protection and FoI is dealt with at an organisational level. The interviews conducted at the Tate helped to provide information absent in the literature as it relates to the implications for privacy/data protection in practice. Most importantly, they revealed that information managers and other professionals are at present not fully equipped to deal with data protection in the digital world.

⁶⁰ University of Bristol, *Bristol On-line Surveys* at www.survey.bris.ac.uk. Accessed on 10 September 2014.

⁶¹ There were approximately twenty members of Scottish Higher Education Information Practitioners (SHEIP) at the end of 2012.

Legal authorities and legal experts that agreed to be involved, particularly in the UK and the West Indies which were more accessible to the author, were interviewed to garner information on the provisions or lack of provisions for data protection as well as to establish the effectiveness and challenges with these provisions. In the West Indies, interviews also targeted heads of regional bodies in order to assess their viewpoint or position on the topic of data protection implementation. An attempt was made to interview the Secretary-General of CARICOM at the CARICOM Headquarters in Guyana for further insight into the plans for implementing data protection legislation and harmonising the regional privacy regime. That attempt was unsuccessful.

Among some of the key persons interviewed in the region who agreed to have a formal and/or informal interview were the then Secretary-General of the Organisation of the Eastern Caribbean States (OECS), Ms. Len Ishmael along with her Legal Counsel and the former Secretary-General of Commonwealth Secretariat who was also one of the founding members of The West Indies Federation and the Caribbean Community, Sir Shridath Ramphal. The author conducted both formal and informal interviews with Sir Shridath Ramphal.⁶² These interviews were enlightening as they revealed the history and development of regional administrative structures and the current perception and stance of regional bodies on the thrust to implement data protection. An informal interview on the topic was also conducted with a legal consultant to CARICOM, Dr. Kusha Haraksingh. These interviews were used in the study to identify the obstacles and the reasons why the region should seek to address the issue of data protection and related information rights in the soonest possible time frame.⁶³

⁶² Sir Shridath agreed to disclose his identity in both types of interviews.

⁶³ See Chapter 6 for full discussion on drivers for data protection in the West Indies, p. 312.

It was very informative conducting an informal interview with the former Information Commissioner of the UK, Richard Thomas and a formal interview with the Assistant Information Commissioner for Scotland, Ken MacDonald.⁶⁴ These experts provided much insight into the provisions for enforcement and management of data protection across the UK. Richard Thomas spoke highly of the need for records professionals to be involved in the process of data protection management which is in keeping with one of the recommendations in the study. Some Freedom of Information (Fol) Officers at The National Archives of the UK (TNA) were interviewed and these interviews strongly suggested that freedom of information and data protection should be considered and implemented in tandem. These pieces of information rights legislation are 'two sides of the same coin'.⁶⁵ Where Fol focuses on 'openness' or transparency, this should be balanced with protecting personal data. Therefore, the right measures should be taken to meet both requirements at an organisational level.⁶⁶ Additionally, key administrators working in regional organisations as well as university administrators in the UK were interviewed face-to-face and in an on-line survey to give a broader perspective of the data protection issues faced by organisations at a sectoral level. Finally, the author attended an International Association of Privacy Professionals Conference in London in 2013 where she attended sessions and networked with global privacy professionals conducting informal interviews and sharing ideas.

Privacy/ Data Protection Legislation

The study required an examination of data protection and privacy legislation in the selected jurisdictions of the Member States of the European Union, the United Kingdom and

⁶⁴ Ken MacDonald agreed to disclose his identity in his capacity as Assistant ICO for Scotland.

⁶⁵ Interview at The National Archives in 2010.

⁶⁶ See Chapter 4 for a full description of mechanisms to use in records and information management programme

Germany; the United States, which has several pieces of legislation that cover various aspects of privacy at a sectoral level; Australia, Canada and New Zealand. Trinidad and Tobago's Data Protection Act was reviewed as one territory in the West Indies with a fully-fledged Act. Legislation in a digital world is very accessible and was found on the websites of Government agencies responsible for the implementation of privacy/data protection legislation such as various Ministries of Justice and/or the offices of the Information/Privacy Commissioners. The study compares and contrasts some of the key provisions such as definitions for 'personal data'.⁶⁷ References to legislation utilised by the thesis may be found in the bibliography.

Diagrams and Tables

Diagrams and tables were created and designed by the author to illustrate various points or arguments in the study as well as provide visual aids for understanding cases made or recommendations and solutions given throughout the chapters. The diagrams and tables have been inserted into the thesis in the areas closest to the information that they relate to. Some may be found as appendices. In cases where a diagram or table was adapted by the author, the author of the original work is indicated in the references.

Images

Images are included at various points in the thesis to enhance the writing but mainly to provide insight into the minds of the populace on the subject of privacy and data protection through editorial or political cartoonists within the selected jurisdictions. In some cases, they reinforce points made in the chapters and in other instances they highlight a popular view on the reality of dealing with privacy and data protection in everyday life. References to the source of images may be found in the footnotes.

⁶⁷ See Chapter 3, p, 149.

To conclude, the data collected during the course of this multi-disciplinary study was critical in supporting the three key arguments of the study, 1) data protection arose as a public issue as a result of rapid technological advances which led to changes in society and human behaviours; 2) there is an irrefutable relationship between data protection and records management that should be explored and enhanced; and, 3) the West Indies should seek to implement data protection in a sound records management environment on a regional scale to protect its citizens and to remain relevant and competitive in the digital world.

Assessment of the Methodology

The varied methodology enabled the author to gain a good understanding of relevant information and concepts, however, some aspects were more successful than others. The topic of the thesis required an understanding of a range of subjects to properly address the central research questions. The author greatly benefitted from exploring a range of literature that related to the theme of data protection which helped to shape the ideas for this multifaceted study.

A search of literature on the theme of data protection revealed that many of the texts were predominately descriptive and did not offer sufficient analysis to explain why data protection came into being as a public policy. However, this literature did indicate that there were societal changes that occurred in the period of the 1960s which led to the search for sociology texts to investigate what those changes were and how they influenced the emergence of data protection as a policy. The sociological texts in turn led to the key proponents of new concepts and ideas about the changes and behaviours in society at that point in history. The use of seminal sociological texts provided the background needed to

understand the context in which data protection emerged.⁶⁸ Extracting the main ideas from an overview of these texts provided the context within which more specific developments could be placed.

Other branches of literature had their own strengths and limitations for this study. Research into legal texts provided information on the provisions of the legislation in various jurisdictions but did not reflect the relationship between the legislation and other disciplines. However, legal texts gave the author a sound understanding of the differing approaches taken with data protection/privacy laws across the selected jurisdictions. The literature in records management that deal with privacy/data protection did not adequately cover information about the relationship between data protection and records management. This immediately indicated that there was a gap here which this study could help to fill.

As it relates to the West Indies, the literature did not prove useful in providing background on either the context or the current status of data protection in the region. The literature however gave the author a good understanding of the possible obstacles and reasons for slow progress in the West Indies as it relates to data protection legislation by providing information about the historical context of the former colonies and their struggles since independence.

Finally, some of the literature on data protection across the disciplines examined was dated because the area of data protection is constantly evolving and so the author had to rely more heavily on official Internet sources and interviews for current information.

⁶⁸ These seminal works are presented in the Literature Review, p. 62.

Internet sources were exceptionally useful to this study as the topic of data protection is very dynamic with changes to the provisions occurring with frequency in some jurisdictions. The author started by examining official websites of Information/Privacy Commissioners to get up-to-date information on legislation, reports and case studies. By looking at these websites, the author began to be exposed to up-to-date information on any changes to the law, guidelines and codes as well as case studies and the situation with breaches within the selected jurisdictions. Other sites searched were those of legal offices that deal with data protection, privacy advocates and their professional bodies. The websites of privacy advocates and professional bodies gave a great deal of insight into current practices that relate to data protection/privacy in both public and private organisations and changes in the provisions in some jurisdictions. On-line newspapers proved very helpful with providing the views of citizens as it relates to privacy/data protection as well as news items that dealt with breaches and other aspects of the topic.

Conducting interviews was the most challenging area of investigation but one of the most fruitful methods. The ideal of face-to-face interviews was not possible in many instances but where they did take place, they were very useful and informative. Although some respondents contacted felt that they were not suited to the topic, they were helpful in referring the interviewers to other persons who they felt were more versed in the area and were willing to assist. In these instances, the best available methods were to conduct interviews by telephone or by email, especially in cases where the geographic location of the jurisdiction rendered it impractical to speak face-to-face.⁶⁹ The author's request for information was still satisfied using these methods.

⁶⁹ See selected jurisdictions pp. 149-150.

The site visits and internship allowed for close observation of practices in organisations dealing with data protection and were the most worthwhile and successful means of data gathering in the investigation of the topic. The author saw first-hand how organisations and staff interpret and respond to the provisions for data protection. It also enabled the formulation of ideas and concepts for how to deal with data protection from a records management perspective within an organisational context.

From a researcher's perspective, the best methodology for a thorough investigation of this topic would have been to conduct site visits, brief internships and face-to-face interviews within each jurisdiction. This would have uncovered any facts and realities left obscure in the written sources. However, the varied sources and methods used to gather information provided the author with a sound basis to draw conclusions and make recommendations for the region of the West Indies.

Background to Study

Privacy protection was first articulated in the legal profession as the 'right to be left alone' by American lawyers Samuel D. Warren and Louis D. Brandeis in 1890.⁷⁰ Their concerns for privacy were raised with the invention of cheap handheld cameras and the proliferation of the penny press.⁷¹ These technologies enabled the capture and dissemination of images or information about individuals. Consequently, a link was made between the use of emerging technologies and the rights of individuals to protect their privacy. This study, however, begins seventy years after the period of the 1890s, in the 1960s and covers major developments on the topic of data protection up until the year 2013. Additionally, it makes

⁷⁰ Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

⁷¹ Behrnd-Klodt, p. 7.

projections for anticipated trends in data protection and records management beyond 2014.

By the 1960s, the fear of unwarranted disclosure of personal information arose in what was considered the birth of the 'information society' or 'the computer age'.⁷² In this period, there was the introduction of information or data processing technologies on a large scale in both public and private agencies resulting in exponential growth in records creation and distribution as a means to regulate society. Computerised records were used by governments in the provision of a variety of services including the criminal justice system, healthcare, education and financial services.⁷³ This thesis explores the theory that computerised systems became the most significant tools used to control societies.

It is for this reason that the study begins in the 1960s. This period is considered a 'watershed' period in the history of information and communication technologies (ICTs) as revolutionary innovations took shape. Technology is the underlying factor driving the concerns for privacy dealt with in this thesis and therefore is the common thread or the dominant feature throughout the study. The thesis investigates how the invention of micro-processing technology in the early 1960s transformed the social, political and economic landscapes of the industrialised world and the impact technology on regulating privacy. The transformation of these societies is evidenced by the fact that five of the largest manufacturers of information-processing technologies, namely, IBM, Digital Equipment, Burroughs, Control Data and NCR total world-wide revenues exceeded \$130 billion in that period.⁷⁴

⁷² James Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* 2nd ed. (Boston, 1986) p. 7.

⁷³ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), p. 12.

⁷⁴ James Beniger, p.424.

The study considers the views of sociologists, who by the 1970s, began to take note of these technological developments and their impact on society, more specifically, on human and institutional behaviours. Sociologists Alain Touraine and Daniel Bell referred to this phenomenon as the 'post-industrial society' speaking of a shift in emphasis from manufacturing goods with the use of machine technology to theoretical knowledge based on new technological economic growth.⁷⁵ The 'post-industrial' society is said to counterpose the 'industrial' society because of its focus on *processing* in which telecommunications and computer technology are strategic for the exchange of information and knowledge.⁷⁶

It is further suggested by sociologists of the 1970s that *information* became the most valuable commodity to governments and organisations. Information is defined in sociology texts as, 'a) *records* including payrolls, government benefits, credit clearances and the like b) *scheduling* including airline reservations, inventories, product-mix information and so forth and c) *demographic and library* including census data, opinion surveys and election data...'⁷⁷

The nature of records and information and how they are defined in records management to determine what are 'personal' records and information is therefore examined in the study.

Sociologists further argue that while the infrastructure of the industrial society was based on transportation, that is, railways, roads, highways, ports and airports, the infrastructure of the post-industrial society is based on the communication of information using cables, broadband, digital TV, optical fibre networks, fax, email and integrated system digital network, combining data, text, voice, sound and images through a single channel.⁷⁸ Thus,

⁷⁵ Daniel Bell, *The Coming of Post-Industrial Society* (New York, 1973), p.112.

⁷⁶ Bell., Foreword 1976, p. xc.

⁷⁷ Bell.,p. xci.

⁷⁸ Bell., *Foreword 1999*, p. xvii.

the character of modern organisations and societies became marked by instantaneous access to vast quantities of information from remote and multiple locations.

The thesis examines whether it is the connectivity of communications systems and the seamless movement of personal data across platforms in today's technologically advanced world that further heightens the need for data protection. When discussing the 'information society', Paul Sieghart states in his seminal 1976 work *Privacy and Computers* that 'more transactions will tend to be recorded; the records will tend to be kept longer; information will tend to be given to more people...fewer people will know what is happening to the data...and data can be manipulated, combined, correlated associated and analysed to yield more information which could not be obtained without the use of computers.'⁷⁹ Hence, this study investigates whether technology in the post-1960s period is the primary factor determining the manner in which information, including recorded information, is managed. It interrogates the analysis of Colin Bennett who suggests that the technological changes of the 'information society' and the resulting growth in recordkeeping provide the context for the perceived need for data protection but it does not provide the cause. The study explores the idea that changes in human and institutional behaviours through the use technology to share and manipulate data in unprecedented ways are key factors that led to the need for data protection.

Recordkeeping is as old as civilisation itself and historical data traces a system of the creation, maintenance and distribution of personal records as far back as ancient civilizations such as the Sumerians, the Chinese, the Egyptians, the Greeks and the Romans.⁸⁰ However, the thesis investigates the idea that it was not until the twentieth

⁷⁹ Paul Sieghart, *Privacy and Computers* (London, 1976), pp. 75-76.

⁸⁰ Bradsher, *Managing Archives and Archival Institutions* (Chicago, 1988), p.19.

century with the development of complex, centralised administrations armed with powerful word-processing technology that the relationship between the citizen and the state began to take on a different character.⁸¹ From as early as the 1930s, new forms of technology such as the analog computer, hand-recorders and tele-communication enabled the collection of personal data en masse and it was the capacity to collect, share and manipulate that information by governmental agencies that heightened feelings of mistrust and suspicion of individuals with regard to invasion of their privacy.⁸² This was particularly reinforced by the occurrences which took place in World War II and subsequent events where personal data, as found in governmental records, was used as a 'tool of tyranny' by those whose desire was to eradicate and/or demean persons based on their nationality, religion, class and creed more so than at any other point in mankind's history.⁸³

Professor of Archivistis, Eric Ketelaar speaks of oppression through records in World War II Germany when the German Census of 1939 supplied data for the 'the Registry of National Character'. This data was then used to capture Jews and others considered not to belong to German *Volk* by the German Reich.⁸⁴ Similarly, notable archivist Verne Harris when speaking of archives and apartheid in South Africa states that the bureaucracy of apartheid reached into every aspect of citizen's lives. This involved the creation of records on race classification, employment, movement, recreation, culture and even sports by thousands of governmental agencies.⁸⁵

⁸¹ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), p. 13 .

⁸² James Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Boston, 1986), p. 276

⁸³ Beniger., p. 29.

⁸⁴ Eric Ketelaar, *Archival Temples, Archival Prisons: Modes of Power and Protection*, *Archival Science* 2: 221–238, (Netherlands, 2002), p. 225.

⁸⁵ Verne Harris, *The Archival Sliver: Power, Memory, and Archives in South Africa*, *Archival Science* 2: 63–86, (Netherlands, 2002), p. 66.

Consequently, the focus of this thesis is primarily the interaction between governmental and private entities with citizens. Technology is considered the main tool used in this interaction, particularly from the period of the 1960s. The study will also consider underlying issues such as power, surveillance, security, collective memory, capitalism, systems of domination, race and the treatment of human rights by the state and private organisations. It does not explore interpersonal relationships between individuals as it relates their use or abuse of personal data. Additionally, it does not fully explore the reactions and expectations of citizens with regard to the handling of their personal data in records by the state or organisations but proposes that this aspect of research be undertaken in future. The emphasis is on institutions and the actions/behaviours of staff working within institutions because this study is principally concerned with the manner in which data protection policies and legislation are upheld by state agencies and organisations and how they meet their obligation to protect the personal information of their citizens/clients/customers.

Outline of Thesis

The thesis is composed of eight chapters with images, tables and diagrams; a bibliography and appendices. The eight chapters are divided into three major sections: 1) historical context and background 2) main findings and 3) conclusions and recommendations. The following section provides a description of each chapter.

Chapter 1

In Chapter 1, the study surveys the existing literature and considers the context for the emergence of data protection as a policy to determine whether the *control* of personal data particularly that contained within governmental records was at the crux of the perceived need to protect personal data. 'The right to control information about oneself', 'the right to

minimise intrusiveness' and 'the right to enjoy anonymity' are three of the thirteen rights of an individual listed by Flaherty in his work *Protecting Privacy in Surveillance Societies*.⁸⁶

There is evidence of the fear of over powerful government as seen in the *Six-Nation Survey on Orwell* in 1984 in which in response to the statement, 'there is no real privacy because the government can learn anything it wants about you', 47 percent of Americans, 68 percent of Canadians and 59 percent of Britons responded that this condition is already happening.⁸⁷

From the onset, the thesis investigates the impact of new technologies on recordkeeping in the 'post-industrial' period (post-1960) within select jurisdictions and examines how the widespread introduction of micro-processing technologies ultimately led to fear that personal data held by governments and private organisations was susceptible to unwarranted disclosure and use. Potential dangers to be discussed are 1) the collection and storage of vast amounts of personal data 2) the possibility of unauthorised access to personal data and 3) the misuse of that data.⁸⁸

Chapter 1 explores the principles behind 'data protection' as a part of the concept of 'privacy'. These principles are said to be very humanistic in scope because they seek to protect the rights and privileges of individuals.⁸⁹ According to the literature reviewed in this chapter, data protection requires that an individual's personal information will not be revealed to others and that the individual's right to make personal decisions and choices about his or her information is preserved. In other words, it relates to 'the right of the

⁸⁶ Flaherty, *Protecting Privacy in Surveillance Societies: The Republic of Germany, Sweden, France, Canada and the United States* (North Carolina, 1992), p.8.

⁸⁷ Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), p. 16.

⁸⁸ Great Britain, *White Paper: Computers and Privacy* Cmnd 6353 HMSO (London, 1975) p. 3.

⁸⁹ Ricks, Swafford & Gow, *Information and Image Management: A Records Systems Approach* (Ohio, 1992), p. 478.

individual to have a basic decision over the rendition and use of his personal data'.⁹⁰ The right to privacy was enshrined in Article 12 of the Universal Declaration of Human Rights of 1948.⁹¹ The European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 reinforced this right in Article 8.⁹² However, as is discussed in the chapter, the right to privacy is not an absolute right in the sense that it does not transcend all other rights and interests. It is limited and there are important interfaces with other rights that should be examined. Balance therefore is needed between protecting the privacy of individuals vis-à-vis the interests of public authorities in the interest of public safety, national security and the economic wellbeing of a country, the prevention of disorder or crime, the protection of health and morals and the protection of the rights and freedom of others.⁹³

Privacy is, therefore, a complex concept to define and is divided into related concepts such as *bodily privacy* and *territorial privacy*. Privacy as it relates to data protection is referred to in some jurisdictions as *informational privacy*. Chapter 1 looks at the various terms used to describe the establishment of rules governing the collection and handling of personal data including credit information, medical and government records.⁹⁴ It explores the writings of Colin Bennett who argues that the use of the term 'data protection' in the European nomenclature, tries to distinguish the policy problem that arose in the 1960s from the broader value of privacy.⁹⁵ Thus, the 'policy problem' is clearly distinguishable in the

⁹⁰ András Jóri, *Data Protection in Europe* at www.dataprotection.eu. Accessed on 17 February 2009.

⁹¹ *Universal Declaration of Human Rights of 1948* at <http://www.un.org/Overview/rights.html>. Accessed on 28 January 2009.

⁹² *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 at www.echr.coe.int/Documents/Convention_ENG.pdf Accessed on 28 January 2009.

⁹³ Stewart Room, *Data Protection & Compliance in Context* (Swindon, 2007), p.7.

⁹⁴ *Privacy and Human Rights 2003: Overview* found at www.privacyinternational.org/survey/phr2003/overview.htm. Accessed on 9 February 2009.

⁹⁵ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992) p. 14.

European context and so the study examines the divergences that took place when looking at other data protection regimes.

Chapter 2

Chapter 2 addresses the historical background to the region referred to as the West Indies. It provides a contextual background by giving a brief history of the West Indies from emancipation to the post-independence period. Using existing literature and interviews, the Chapter provides details on the legal traditions among West Indian territories. It examines the recordkeeping tradition that emerged in the region as a result of the colonial system. It provides evidence as to the current status data protection legislation and archives legislation in the region. Ultimately, the Chapter 'sets the scene' for why the implementation of data protection may be challenging for the region from a records management perspective.

Chapter 3

A review of the literature reveals that the response to informational privacy or data protection has been wide and varied. The development of policies and later legislation to address these issues since the 1960s has been highly dependent on the social, historical and economic realities of the particular country or region. Chapter 3 of the study considers international perspectives on data protection/privacy by examining a cross-section of models or approaches developed for the management and control of personal information in select jurisdictions. This chapter is therefore a pivotal one in the thesis. Selected jurisdictions to be examined are the United States, Canada, New Zealand, Australia, as well as Germany and the United Kingdom as Member States of the European Union. Although historically related, these territories have taken different paths in developing their data

protection/privacy policies and legislation. Some of the key factors that contributed to the development of these varying models for data protection/privacy are probed.

The study discusses one of the main catalysts that led to the move towards region-wide implementation of privacy/data protection legislation by countries, particularly European countries. It is called *the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* formulated by the Council of Europe in 1981. One of the stated objectives of the Council of Europe is 'to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms.' It also sought 'to safeguard everyone's rights with respect to privacy, taking into account increasing flow across frontiers of personal data undergoing automatic processing.' The purpose of the Convention of 1981 was said 'to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, in particular his right to privacy, with regard to automatic processing of personal data to him'.⁹⁶ The study consider this moment as the time when the term 'data protection' in relation to personal information protection began to be used on a European-wide scale.

Thereafter, the Commission of European Communities formally proposed the introduction of a Data Protection Directive (95/46/EC) a high point in its leadership in European Data Protection, influencing regions outside of European borders.⁹⁷ This Directive would prove to be a very important harmonisation measure introduced under the Internal Market

⁹⁶ Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* at convention.coe.int/Treaty/EN/Treaties. Accessed on 18 December 2008.

⁹⁷ European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* found at ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. Accessed on 18 December 2008.

provisions of the Treaty of Rome.⁹⁸ The Treaty of Rome sets out the legal powers of the European Commission regarding the free movement of goods, persons, services and capital between Member States of the European Union. Hence, the European Commission decided that it was time to harmonise and remove any obstacles to the flow of personal data from within its borders. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on free movement of such data of the European Parliament and of the Council* was adopted as a legislative provision on 24 October 1995. The Directive sets out the rules to ensure a high standard of protection of personal data throughout the European Union through harmonisation. The study considers how this Directive has influenced privacy/data protection legislation around the globe and what lessons could be learnt by the West Indies from the European response to data protection.

Chapter 3 of the study also analyses the influence of the expectation and requirements of the Council of Europe's Convention and the European Union's Directive for non-European territories. Ultimately, it was the term 'an adequate level of protection' that put growing pressure on countries outside Europe for the passage of strong or stronger data protection laws.⁹⁹ The European Commission became very active in determining the 'adequacy' of 'third countries' systems for protecting privacy. For example, Switzerland and Hungary were given a passing grade on 26 July 2000 and that meant that all transfers of personal data to these countries could continue. The Commission also recognised Canadian privacy legislation as adequate in January 2002.¹⁰⁰ It is therefore important to investigate whether other selected jurisdictions met this level of adequacy. This would have implications for the implementation of data protection in the West Indies as it relates to adequacy in its dealings with Europe.

⁹⁸ Stewart Room, *Data Protection & Compliance in Context* (Swindon, 2007), p.13.

⁹⁹ See explanation of 'adequate level of protection' in Literature Review on p. 69.

¹⁰⁰ Privacy and Human Rights 2003: Overview at www.privacyinternational.org. Accessed on 9 February 2009.

The United States' (US) approach to privacy/data protection has proven the most challenging to conform to the European Union's concept of adequacy. At the heart of the issue is what has been described as the 'incomplete patchwork of federal and state provisions' which make up the US privacy/data protection regime.¹⁰¹ It took very lengthy debates and negotiations between the European Commission and representatives of the United States to reach an agreement about the US level of adequacy.¹⁰² This study examines the agreement referred to as the 'Safe Harbor' Agreement which came into being in 2000 after a programme was launched with the assistance of the US Department of Trade in which American businesses agreed to comply with the requirements of the EU Directive.¹⁰³ It explores whether there are any challenges for US companies to conform to the Agreement since its inception and how secure is this agreement today.

The study considers the main issues between the European Commission and the United States. It scrutinises some of the developments that took place in the post 9/11 era when the US Government appeared to decrease the level of privacy in its 'war against terrorism' evidenced by its insistence on introducing biometric identifiers in passports and an obligatory visa system on countries that did not want to issue these type of documents.¹⁰⁴

Chapter 3 reviews the debate on the adequacy of the US privacy regime based on 'self-regulation' which has been described as 'lagging far behind' by some critiques.¹⁰⁵

Additionally, this thesis considers the main socio-cultural factors and major historical events that have led to the approach taken to privacy by the US in the latter half of the twentieth century to the beginning of the twenty-first century. This would include a look at the impact

¹⁰¹ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York: 1992), p. 12-13.

¹⁰² András Joris, *Data Protection in Europe* at www.dataprotection.eu. Accessed on 17 February 2009, p. 5.

¹⁰³ Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, *Houston Law Review*, p. 717.

¹⁰⁴ Reidenberg, p. 717.

¹⁰⁵ Joel Reidenberg, E-commerce and Trans-Atlantic Privacy, *Houston Law Review* Volume 38, p. 719.

of the September 11, 2001 attacks on the World Trade Center and the Pentagon. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the PATRIOT Act, was enacted in the wake of the 9/11 attacks. This omnibus law contains separate titles to enhance domestic security against terrorism.¹⁰⁶ It has impacted on the movement of people and the sharing of information worldwide. This study explores its implications for privacy/data protection, not only in the US but across the globe.

Chapter 3 of the study then canvasses the Canadian federal privacy landscape. The need for privacy protection in Canada arose in the late 1960s and early 1970s when computer technologies emerged as important tools for government and 'big business'.¹⁰⁷ The Canadian government established a task force in 1972 under the auspices of the Department of Communications and the Department of Justice. The task force produced a report entitled, *Privacy and Computers: A Report of the Task Force* and this resulted in the enactment of the first federal public sector privacy protection in Part IV of the Canadian Human Rights Act of 1977. This would subsequently result in the establishment of the Office of the Privacy Commissioner with the mandate to receive complaints from the general public, conduct investigations and make recommendations to Parliament.¹⁰⁸ The study discusses the development of the Canadian model and its effectiveness.

This thesis investigates the provision for privacy in Australia, which has been described as similar to those of Canada. Both of these countries face the challenge of creating national policy within federal systems with shared constitutional responsibility for private sector

¹⁰⁶ International Association of Privacy Professionals, *The PATRIOT Act of 2001* at <http://www.iapp.org> . Accessed on 2 February 2009.

¹⁰⁷ Nancy Holmes, *Canada's Federal Privacy Laws Parliamentary Information and Research Service* found at <http://www.parl.gc.ca>. Accessed on 28 November 2008, p. 1.

¹⁰⁸ Holmes, p. 2.

regulation. Therefore, the issue of whether an integrated approach works could be examined in these jurisdictions. As a result of its federal structure, Australia has multiple privacy regimes and its approach is referred to a 'co-regulatory' model. This type of model as well as the other three types identified is examined in Chapter 2. Privacy law in Australia involves the national (Commonwealth) government, the state governments and the major territory governments. The Australian regime principally encompasses eleven Information Privacy Principles (IPPs) in the Commonwealth Privacy Amendments Act and ten National Privacy Principles (NPPs) in the Commonwealth Private Amendment (Private Sector) Act 2000.¹⁰⁹ However, the study investigates whether there are any weaknesses in this highly complex privacy regime that could provide lessons to regions like the West Indies.

Finally, Chapter 3 of the study assesses the New Zealand privacy regime. New Zealand has developed a unique model for the protection of personal information which it said to be the most comprehensive outside of Europe. New Zealand initially passed an Official Information Act in 1982. This Act declared that all government information is open unless it should be protected. New Zealand's unique response to the management of personal information will therefore be reviewed. The merits of the New Zealand privacy/FoI regime have been a source of debate in government and academic circles.¹¹⁰ This regime differs in fundamental ways from that of the European Union model although it generally conforms to European standards and it has been recognised by the EU as adequate. The study explores the suitability of the New Zealand approach in relation to the other three models.

¹⁰⁹ Bennett, Colin, *An International Standard for Privacy Protection: Objections to the Objections* (British Columbia, 1996) at www.cous.uvic.ca/poli/bennett. Accessed on 12 February 2009.

¹¹⁰ New Zealand Privacy Commissioner, *The Official Information Act and Privacy: New Zealand's Story*, Speech at the FOI Live 2005 Conference London, 2005.

By the end of Chapter 2, the core elements of data protection principles, processes and practices in these selected jurisdictions will be distilled to assess whether there are any model requirements suitable for emulation by the West Indies.

Chapter 4

In Chapter 4 of the study, the relationship between data protection and records management is fully explored in the context of the examined data protection models. As a first step, the thesis defines what a 'record' is in order to understand where personal information in records could be found as well as who creates and uses it. Records in general are essentially 'recorded information, regardless of medium or characteristics, created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.'¹¹¹ Records are created, distributed and maintained by both public and private entities in the course of their business. They are also 'naturally accumulated'¹¹² by individuals during the course of their lifetime reflecting their activities as well as their interactions/relationships with other individuals or entities. The content of records encompasses a wide range of information that may be legal, administrative, historical, cultural, statistical or medical in nature. Businesses and organisations, dependent on their core function, collect vast amounts of personal information in staff records and records of their clients. The extent to which business records contain personal information is explored as the first step in establishing the relationship between privacy/data protection and records management.

Personal information, as protected by privacy and data protection legislation, takes many forms and is collected, stored and accessed in many ways within organisations. Personal

¹¹¹ International Standards Organisation, ISO 15489-1: 2001 *Records Management Standard* at www.iso.org.

¹¹² Term coined by Sir Hilary Jenkinson, an early modern archives theorist.

information is expansive by nature, colonising all types of record forms.¹¹³ It is at times difficult to determine which information may be considered as personal. The study investigates which forms of records are subject to privacy/data protection and explores methods to help with determining what is personal. The study also investigates the challenges with protecting individuals' personal data by examining how to manage information environments in which personal data thrives.¹¹⁴

Records management as a discipline has always been concerned with the control of recorded information. The study argues that responsibility for managing privacy has been integral to records management because of the effort made in controlling access, maintenance and disposition of records. Privacy protection is inherent in records management systems in the dispersal of records (paper-based) into physical repositories where measures are established to physically protect and secure records.¹¹⁵ The need for security of data still exists when dealing with electronic records in an automated environment. The thesis investigates whether records managers have been using records management methodology to assure protection of records and privacy simultaneously and if so, whether this is intentionally or is a by-product of the records management function. The thesis will examine the synergies that exist and how a relationship between the two pursuits could be mutually beneficial.

The study further considers the main objectives of records management and highlights where data protection and security of records could fall within the ambit of the records manager. Another aim of the thesis is to provide guidance to records and information management practitioners on dealing with the challenge of balancing privacy/data

¹¹³ Menzi Behrnd-Klodt et al, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005), p. 78.

¹¹⁴ Behrnd-Klodt, p. 78.

¹¹⁵ Charles Booz, Electronic Records and the Right to Privacy, *Information Management Journal*, July 2001.

protection within records management, which has as one of its principal objectives to provide the right information to the right user at the right time. This study represents the first real attempt at setting out in detail the relevant data and guidance to empower records and information management professionals with the knowledge to grapple with the increasingly complex topic of data protection.

Further to this, Chapter 4 of the study investigates the areas where records management principles, processes, practices and policies interface with privacy/data protection administration. It explores how records management programmes can identify and map the flow of personally identifiable information in compliance with data protection and privacy laws. The study goes further by not only examining the manner in which data protection is currently managed in records management programmes but by identifying new and direct ways in which data protection can be administered throughout the 'life' of a record. This thesis dissects existing records management theories and introduces data protection management strategies throughout the processes involved with managing records and information.

It examines whether there are codes of practice designed for records managers and archivists on data protection and privacy within the selected jurisdictions. One code of practice which is easily accessible is that of the UK. This Code was originally drafted by a joint working party composed of representatives from the Society of Archivists, the Records Management Society and the Public Records Office (later The National Archives). The study will review sections of the Code dealing with responsibilities of records managers and archivists as it relates to managing personal data held by them.

Chapter 4 proposes methodologies for data protection management to be further incorporated into records management and ensure compliance with data protection legislation. It examines the main policies in which data protection measures could be addressed such as an organisation's records management policy, electronic records policy and/or e-mail policy, retention and disposition policy, access and reproduction policy, records security policy, acquisition policy, preservation policy and disaster prevention and recovery policy. Additionally, the study discusses relevant mechanisms that could be utilised by organisations in dealing with data protection management within records and archives management.

Chapter 5

Chapter 5 of the thesis summarises the changes and challenges for records managers in implementing data protection and privacy legislation in a digital world. It assesses how modern information and communication technologies including hardware such as digital cameras, smart-phones, tablets and hand-held scanners and new modes of communicating including, web-publishing, instant messaging, social networking on the Internet, blogs and wikis, are changing the ways in which personal data is created, stored and distributed within organisations. The advent of 'cloud computing' also has serious implications for managing privacy/data protection and these will be explored and discussed. It examines whether new skills are required by records managers and archivists in adapting to the changing privacy landscape.

Chapter 6

Chapter 6 of the study identifies the obstacles hindering the move towards data protection implementation. It considers the main drivers for the region to implement and makes recommendations to the West Indies on how to create a framework for data protection

regulation and management based on the comparative study of the selected jurisdictions from a records management perspective. Most importantly, the chapter sets out the lessons learnt from other jurisdictions and examines the merits and demerits of taking an integrated approach to implementing information management related legislation like data protection and freedom of information. It investigates any areas of strength or weakness in the West Indian context in preparation for full implementation of data protection legislation with a special focus on its systems of recordkeeping.

Further to this, the chapter explores how the recordkeeping style developed in the West Indies could impact on the full scale implementation of data protection and whether any adjustments and standardisation are required to prepare for successful implementation of data protection. When examining the key driving forces for the region to prepare for data protection implementation it reviews whether changes are required in its administrative structures, legislation and legal systems to ensure compliance with regulations for 'adequacy' set out by European Union and other international entities. It also investigates whether there are any expectations of the international community for the region to conform to accepted international standards for the management of the personal information of its citizens and of others in the global community.

Chapter 7

Chapter 7 states the overarching conclusions of the study, reflects on whether the objective of the research have been met and considers future prospects and developments in informational privacy and data protection. It summarises the main arguments of the thesis and states its contribution to existing knowledge.

Chapter 8

Chapter 8 projects future trends and potential mechanisms that may be useful in the increasingly challenging effort to protect personal data found in recordkeeping systems on a global scale. It offers suggestions for overarching guidance when dealing with data protection within the field of records management and offers possible topics for future research in these areas.



Image 1 *Data Protection in Action*

aujasus.wordpress.com/category/data-leak-prevention¹¹⁶

¹¹⁶ Image taken from AUJAS Company website. AUJAS is a company that provides information risk management consultancy services.

SECTION ONE

HISTORICAL CONTEXT AND BACKGROUND

1. CHAPTER 1

LITERATURE REVIEW AND BACKGROUND

This chapter surveys the literature and explores three main themes of the research, 1) the development and meaning of the term 'data protection' 2) the relationship between data protection and records management and 3) a historical background to the West Indies to provide the context for the implementation of data protection. It should be noted that new and dynamic historical, political, social and economic developments have been taking place within the timeframe of the study and these emerging trends continue to shape the legislative framework and practice within the various jurisdictions. Therefore, not all the recent developments are captured within the study but the main issues arising within the period of the study (1960 – 2013) are examined.

1.1 Data Protection: Context, Origin and Development (1960s – 1980s)

Data Protection in the 'Post-Industrial' Era

The period of the early development of the data protection policy spans approximately from the 1960s to the 1980s. This period has been considered by some scholars, whose writings are examined later in this chapter, as a 'watershed' period in the history of global society and has consequently been labelled in a number of ways such as the 'Information Age', the 'Information Society', 'Knowledge Society' and the 'Information Revolution' as a result of concepts arising from the advent of rapid technological developments. One concept that is of interest to this study is the correlation between the emergence of data protection as a policy and the sociological concept referred to as 'post-industrialism' or the 'post-industrial society'.

The concept of a 'post-industrial society' was comprehensively defined by sociologist Daniel Bell in his seminal work *The Coming of the Post-Industrial Society: A Venture in Social Forecasting* first published in 1973. Bell rejected the labelling of the emergent trends in societies as the 'information society' or 'knowledge society' stating that these terms do not comprehensively describe the dynamic changes taking place in post-1960s society. In describing the dramatic changes of this period, he advanced the theory that there was a shift from an 'industrial society' to a 'post-industrial society'. This study acknowledges Bell's theory that the changes in society were profound and the new developments in the superstructure of society were as a result of the changing shape of economies that moved from being goods oriented to being services oriented. The study also agrees that societal problems would arise as a result of these changes. The problem under examination is the perceived loss of privacy.

In placing this problem in context, a deeper look at changes that took place in society in the 1960s is necessary. The concept of 'post-industrial' is used to describe the events that took place in this era. Bell argues that 'post-industrial' period is counterposed to the former 'pre-industrial' and 'industrial' age. The 'pre-industrial' period was primarily *extractive* in nature. The 'pre-industrial' period was based on agriculture, fishing, mining, timber or other natural resources where society directly interfaced with its natural resources. The 'industrial' sector was primarily *fabricating* meaning that there was shift in focus to energy and machine technology to manufacture goods. However, Bell suggests that there was the emergence of a 'post-industrial' society which was primarily focused on *processing* where telecommunications and information technology is strategic for the exchange of information and knowledge. Therefore, post-industrial society is based on an *intellectual technology* rather than on *machine technology*.

Bell explains that if capital and labour were the major structural features of industrial society, in the post-industrial society, *information* and *knowledge* are the main features. By information, Bell meant the storing, retrieval and processing of data as the basis of all economic and social exchanges including,

- ‘a) Records: payrolls, government benefits e.g. social security, bank clearances, credit card clearances and the like
- b) Scheduling: airline reservations, production scheduling, inventory analysis, product-mix information, and so forth.
- c) Demographic and library: census data, opinion surveys, market research, knowledge storage, election data, and so forth.’¹¹⁷

By *knowledge*, Bell meant ‘an organised set of statements, of facts or ideas, presenting a judgments or an experimental result that is transmitted to others through communication media in some systematic form.’¹¹⁸

The study also considered what Bell lays out as the five dimensions or components of a ‘post-industrial’ society. They are:

- ‘1. *Economic Sector*: The change from a goods-producing to a service economy;
- 2. *Occupational Distribution*: The pre-eminence of the professional and technical class;
- 3. *Axial Principle*: The centrality of theoretical knowledge as the source of innovation and of policy formulation for the society;
- 4. *Future Orientation*: The centrality of theoretical knowledge as the source of innovation and of policy formulation for the society;
- 5. *Decision-making*: The creation of a new ‘intellectual technology.’¹¹⁹

This thesis agrees that the mark of the second half of the twentieth century is the management of ‘organised complexity’, that is the complexity of large organisations and systems. In dealing with ‘organised complexity’, ‘problem-solving’ automation is employed

¹¹⁷ Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (New York, 1973) p. XIII.

¹¹⁸ Bell, p. XIII.

¹¹⁹ Bell, p. 14.

hence *intellectual technology* such as an automatic machine and computer software. The post-industrial society is based on the provision of services, a game between persons. What is now important is not 'raw muscle power or energy, but *information*.'¹²⁰ Information becomes the new 'engine' driving information-based societies and to possess information places an individual or an organisation in a position of power. Although historically information has always been a means of power, the 'information revolution' that emerged in the 1960s due to advances in technology resulted in vast amounts of readily available information.

Boris Frankel in his study *The Post-Industrial Utopians* critically analyses the hypotheses of the main 'post-industrial' theorists of the 1960s and 1970s including Daniel Bell. He refers to Bell as a right-wing or non-Left, post-industrial theorist. Alain Touraine's text, *Defining Technological Literacy* and Alvin Toffler's text, *Creating a New Civilization: The Politics of the Third Wave* both present another interpretation on *post-industrialism* highlighting different aspects. However, there is a common thread throughout all the existing post-industrial theories, that is, *technology* in the period of the 1960s became the new mode of economic advancement.

Frankel states,

'with videotex, teletex, networks, micro-electronic processors, and the current development of voice-sensitive computers, it is not only telecommunications that have undergone a technical revolution. Newspaper articles and television programmes constantly inform us of innovations in the banking, health, social services, education, entertainment, retailing and other industries.'¹²¹

Further to this, he contends that by the mid-1980s,

¹²⁰ Bell, p. 127.

¹²¹ Boris Frankel, *The Post-Industrial Utopians* (Oxford, 1987), p. 149.

‘The race is well under way to implement fibre-optical technology, to multiply cable networks, to extend and refine existing communication with satellite networks and elaborate private and public databases.’¹²²

The theories arising out of the rapid developments in the 1960s are critical to understanding the background in which data protection concerns arose. When examining international perspectives on data protection, they provide the context that explains the need for data protection within the re-engineered, highly automated societies of the 1960s and beyond. The emergence of knowledge-based economies meant that information captured in organisational records becomes pivotal to the growth of economies and the control of societies.¹²³

Consequently, the establishment of data protection legislation in Europe and privacy legislation in other jurisdictions was driven by the fundamental changes taking place within these societies with regard to the utilization of new information and communications technologies (ICTs) in all aspects of human existence. Information and communication technologies became central to the public and private sector as well as within the homes of citizens. This facilitated the widespread distribution of information, including personal data, which could be more easily stored, manipulated and exchanged in a way that was not before possible.

Instant access to information from remote locations and the ability to manipulate that information held serious implications for the relationship between the individual citizen and the holder of personal data. Organisations collect and store vast amounts of information on people. Undoubtedly, the collection of personal data is important to the functioning of any society. Information was always collected by organisations. However, until ICTs, the ability

¹²² Frankel, p. 149.

¹²³ See Appendix 1.

to gather, record and store increased to previously unattainable levels. The capacity of ICTs to create, share and store information is also tied to the growing need for records management which seeks to regain control of recorded information created, received, distributed and maintained by organisations. Records and information are critical to the governance and development of any society. Societies are made up of group of people that need to be regulated. Hence records and information are used for a number of reasons including to uphold the rights of citizens, for commercial purposes and entertainment purposes. Although the collection of personal data is as old as recordkeeping itself, the expansion of the powers of the state and institutionalisation of information over the last century along with the use of more complex record-keeping systems based on technology augmented the need for control of personal data.

The Information Society

The study also explores the work of James W. Cortada, *Making of the Information Society: Experience, Consequences and Possibilities* which gives a comprehensive and practical background of the birth and evolution of the 'Information Age' in America. He discusses the move from the use of paper and print culture to the emergence of the computer and all its related technologies. Cortada considers the typewriter to be the precursor to the first commercially available computer likening its popularity with Americans at the turn of the 20th century up to the mid-1960s, with their 'present enthusiasm' for personal computers (PCs).¹²⁴ The typewriter prepared the way for the computer because it produced information in a useful format that made it possible to produce multiple copies simultaneously. By the 1970s, manufacturers of typewriters such as Honeywell even found

¹²⁴ James W. Cortada, *Making of the Information Society Experience, Consequences and Possibilities* (New Jersey, 2002) p. 5.

a way for typewriters to 'store' data. This capacity to duplicate and share information was a mere taste of what was to come.

Cortada's discussion on America's emerging 'love affair' with technology is useful because it puts into context what led to the emergence of today's digital world where every business, every household and every individual, in one way or another interfaces with some form of technology. Technology affects the lives of people in countless ways and has been interwoven into 'the rhythm of people's daily lives and work activities.'¹²⁵ All forms of information tools inclusive of telephones, newspapers, books, television, adding machines, typewriters and radios are now part of the continuum in the development, exploitation and co-existence of information within human society. Hence, there is the emergence of an 'information society'. Cortada further contends that as society becomes familiar with technology, society figures out new and better ways to work with it. Implicit in this argument is that societies become more comfortable with the technology and new ways of using it which may be for good purposes or ill intent. New ways of manipulating data are being discovered on a daily basis. This in itself has implications for the protection of all types of data as the capacity to retrieve and re-use information stored electronically, including personal information led to the emergence of new types of crime referred to today as 'cyber-crime'.

Additionally, in the twentieth century, the relationship between the citizen and the state became more formalised, routine and impersonal. Colin Bennett in his work, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, states that the 'information society' provides the context for data privacy/data protection but it does not

¹²⁵ James W. Cortada, p. 56.

provide the cause.¹²⁶ This is a fair statement because citizens did not appear to fear the technology itself, which is evidenced by the exponential growth in the sale of digital devices. However, the principal fear of citizens within countries arose from the changing relationship between the citizen and government. The fear augmented that powerful agencies, both public and private, would seek to control their lives with the technology. The study asserts that from the latter half of the twentieth century until the present, there is a growing tension between personal privacy rights and the informational needs of administrators and policy makers as a result of the expansion and institutionalization of state power.¹²⁷ These are all characteristics associated with bureaucracy and organisational cultures which are changing to match the growing capabilities of the technology.

In modern societies, most citizens expect the provision of a variety of social services including healthcare, a properly functioning criminal justice system and a well-funded educational system.¹²⁸ The functioning of hospitals, schools, courts and other public and private institutions requires the collection of vast amounts of personal data. The use of information and communication technologies (ICTs) has enabled these agencies to identify, target and, in some cases, manipulate data.¹²⁹ Bennett states that three types of data can be identified. *Administrative* records generated when a transaction with an agency occurs. This type of data is created when a citizen applies for a licence or gets married. *Intelligence* records are created by collecting data from a source other than the individual to whom the record pertains, for example, a police criminal file or consumer credit reports. *Statistical* records are generated through information gathering techniques such as conducting a

¹²⁶ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), p.18.

¹²⁷ Bennett, (New York, 1992), p. 18.

¹²⁸ Bennett, (New York, 1992), p. 17.

¹²⁹ Bennett, (New York, 1992), p. 19.

census or a survey. This aggregate information does not necessarily reveal the identity of the record subject.

In discussing public attitudes towards privacy, Bennett relates the results of cross-national polling in a *Six-Nation Survey on Orwell* in 1984 to compare the responses of different populations. In response to the statement, 'there is no real privacy because the government can learn anything it wants about you', 47 percent of Americans, 68 percent of Canadians and 59 percent of Britons responded that such a condition is 'already happening'.¹³⁰ Only 18 percent of Germans agreed with the statement. These results revealed that North Americans and Britons were concerned with political intrusiveness. Bennett concludes that most citizens seem to have a keen awareness of privacy as a key ingredient of human dignity and have reservations about the political implications of the disclosure of personal data held in computers.

In establishing the context that led to the perceived need for data protection, it is useful to further examine the question of data processing and bureaucracy. James Beniger argues the theory of 'the Control Revolution' which he believes is inextricably linked to the birth of the Information Society. The Control Revolution represents a restoration of and increased centralisation of economic and political control which Beniger believes was lost during the Industrial Revolution.¹³¹ Beniger contends that with rapid changes in mass media, telecommunications and technology, new infrastructures emerged that led to the re-establishment of bureaucratic organisation. He thinks of computers as the most notable

¹³⁰ Bennett (New York, 1992), p. 42.

¹³¹ James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* 2nd ed. (Boston, 1986), pg. 7

vehicle among which he refers to as 'control technologies' that drive the bureaucratic process.¹³²

Bureaucracy is at the heart of the control revolution. However, by the latter half of the twentieth century, information-processing systems dramatically transformed public and private bureaucracy. In a 1976 report, the National Commission of Federal Paper Work reported, 'Federal agencies are today churning out forms, reports, and assorted paper work at the rate of over 10 billion sheets per year. That's 4.5 million cubic feet of paper.' Ironically, technology facilitated the exponential growth of paper. The report further stated that the U.S. Department of Agriculture alone had to increase its paper store by 64,000 cubic feet – forty four-drawer cabinets per working day. All this paper was costing the U.S. Government \$40 billion annually.¹³³

When discussing the political dimension of the issue of privacy, this study considers the view of Bennett who surmises that with information technology enhancing the ability of government to collect and manipulate vast amounts of personal data on individual citizens, distrust of the power and control of the state vis-à-vis its citizenry emerges. Britons Michael Stone and Malcolm Warner warned in their 1969 article *Politics, Privacy and Computer* that, 'The computer has given bureaucracy the gift of omniscience, if not omnipotence, by putting into its hands the power to know. No fact [is left] unrecorded, nothing forgotten nor lost, nothing forgiven.'¹³⁴ Hence, an argument can be made that the fear of over powerful government armed with too much information-handling capability was deeply ingrained in American and other information driven societies.

¹³² Beniger, (Boston, 1986), p. 7.

¹³³ Beniger, (Boston, 1986), p. 414.

¹³⁴ M.G. Stone and Malcolm Warner, 'Politics, Privacy and Computers,' *The Political Quarterly* 40 (1969), p. 260.

Data protection was thus placed on the political agendas of developed nations from as early as the 1960s evidenced by newspaper articles of the period across selected jurisdictions. However, the success of data protection as a policy depended heavily on the effectiveness of its implementation in the various jurisdictions. It also would become increasingly important for international regimes to promote harmonisation in the administering of data protection throughout the public and private sector. The following section will outline the rise and development of data protection/privacy legislation using existing literature on the jurisdictions selected for closer examination and discussion in Chapter 3.

What is Privacy and Data Protection?

The terms 'privacy' and 'data protection' are often used interchangeably but a close examination of their origins reveals that 'privacy' is broader and wider ranging in its scope than 'data protection'.¹³⁵ Privacy has no definite boundaries and can have different meanings to different individuals or groups of people. It is also fluid and can change over time dependent on the social, economic and political environment. When reviewing definitions of 'privacy' in the literature, it becomes clear that 'privacy' is a complicated concept that is challenging to define theoretically. There is no universal consensus on its meaning but it is usually linked to notions of the boundary that should exist between organisations, both public and private, and individual citizens.

The term 'data protection', however, is considered by some to be more technical and specific. It was translated from the German term *Datenschutz* to mean specifically the group of policies designed to regulate the collection, storage, use and transmittal of personal information.¹³⁶ Bennett contends that the term 'data protection' has very little meaning or

¹³⁵ Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992), p.13.

¹³⁶ Bennett, (New York, 1992), p. 13.

appeal to the average citizen. Therefore, it has been suggested that it is for this reason that many English-speaking territories such as Canada and Australia have retained the term 'privacy' when naming legislation that incorporate the same functions as European-based data protection laws. However, there continues to be debate as to whether either of these terms adequately describe the main principles and practices involved in regulating personal data.

Other terms used globally include, 'information privacy', 'data privacy', 'personal data protection', 'privacy protection' and 'personal information protection'. Arguably, any of these terms could be used to convey the concept in a way that may be more meaningful for citizens or laymen to understand than data protection. The term 'privacy' alone encompasses more than one idea while 'data protection' may be easily confused with the use of the same term in the discipline of Information Technology where it is used to mean the measures utilised to back-up electronic data and ensure that data is recoverable.¹³⁷ Jurisdictions would benefit from the addition of the word 'personal' preceding 'data protection' or 'privacy' which would resonate with citizens as they would understand that these types of policies and legislation relate to them individually and directly.

In looking at the terminology, Colin Bennett in his study describes the use of the term 'privacy' as 'notoriously vague, ambiguous, and controversial.'¹³⁸ He argues that privacy encompasses diverse concerns including the right to be free from intrusive police searches, from wiretapping, from persistent journalists and to make private decisions in relation to your family. It also means the right to have some control over the collection, storage and disclosure of personal information held by governmental agencies, financial institutions,

¹³⁷ SearchDataBackup, *Data Protection Management* at searchdatabackup.techtarget.com/definition/data-protection-management-DPM. Accessed on 21 January 2014.

¹³⁸ Bennett, (New York, 1992) p. 13.

medical facilities, educational establishments and other entities. He further asserts that privacy is very subjective notion that changes over time and space and has different meanings to different groups of individuals within a society.

Privacy does not have definite boundaries but generally relates to the ability of an individual or a group of individuals to guard their personal affairs from public view. It also relates to the ability of an individual to control the flow of their personal information. Notions of security and anonymity are often associated with privacy. However, privacy in any form is not an absolute right. Privacy may be sacrificed for a greater purpose. For example, it is within the interest of citizens for the government to collect information on one's earnings and income for the collection of taxes. That same information, disclosed to the wrong person or entity may be used to violate the rights of individuals. Another area where personal privacy is sacrificed is with the collection of census data by governments. This information is useful for strategic planning for future services.¹³⁹

The term 'data privacy' is used to refer specifically to the relationship between technology and the security of personal data. Rapid technological advancements have resulted in the improper and uncontrolled disclosure of personal data, particularly sensitive information such as health, criminal, financial, genetic and location. Data privacy has been the most challenging area in privacy. It is difficult to enforce and police. Additionally, data privacy issues are dealt with differently across various jurisdictions around the world as a result of the historical, cultural and political experiences of these countries. This reality has led to disparities in the framework for legislation.

In a report produced by the Committee on Privacy in the Information Age of the Computer Science and Telecommunications Board in the U.S. Division on Engineering and Physical

¹³⁹ Privicilla.org at www.privacilla.org/index.html. Accessed on 17 February 2009.

Sciences entitled, *Engaging Privacy and Information Technology in the Digital Age*, James Waldo suggests that privacy has been a central concept from the latter 19th century when there was the emergence of large bureaucratic organisations in industrial, urban society. He states that as society moved from the agricultural to the industrial to the information age, societal and technological changes will continue to pose dynamic challenges to many aspects of modern society including the security of personal data.¹⁴⁰

Waldo discusses the definitions of the term 'privacy' and its various connotations. He suggests that privacy could refer to the physical privacy of an individual's home or office, freedom from interference from government into an individual's personal choices as well as freedom from surveillance and the ability to keep personal information including electronic communication confidential.¹⁴¹ Waldo found that privacy was 'ill-defined'. He states that the concept is well understood by people in general. He believes privacy is multi-dimensional in nature and is dependent on a given situation where it may be in tension with other values or desires of the individual, subgroups, and society at large. The Committee, however, agreed that the everyday usage of the word 'privacy' generally includes reference to the types of information available on an individual that may be behavioural, financial, medical, biometric, consumer and biographical in nature.

The report outlines what the Committee considers to be the main drivers of change to the notion of privacy. These drivers are technological change, societal shifts and discontinuities in circumstances. On the matter of today's advances in technology, the report states that the technological changes refer to major differences in today's technological environments from what existed decades ago. The hardware used today is more powerful and has a far

¹⁴⁰ James Waldo, *Engaging Privacy and Information Technology in a Digital Age* (Washington, 2007), pg.22.

¹⁴¹ Waldo, (Washington, 2007), pg. 22.

greater capacity allowing for more data to be collected, stored and analysed in ways that it could not in the past. Networking means that data is becoming increasingly available on-line and new algorithms that allow extraction of information from vast amounts of data. This essentially makes it more difficult to protect data. As information technologies become cheaper and cheaper to produce, they become more readily available to individuals, corporations and government.¹⁴²

In the report, the *societal shifts* refer to evolutionary changes that are taking place in the institutions within society that are making use of the aforementioned technological systems. These systems are incorporated at the very core of business and are used to generate and make available personal information on an unprecedented scale. This thesis supports the view that the expectations and demands of the clients/users across all sectors have equally increased among all classes of people including old age pensioners, the unemployed and homeowners. Finally, the term 'discontinuity in circumstance' used in the report refers to the emergent concerns and transformation in the US national debate on privacy as a result of sudden and unexpected occurrences such as the events of September 11, 2001. The entire nation was catapulted into counterterrorism, national security and border defence. These issues moved higher on the public agenda than at any other period in US history.

This study explores the US position on privacy in Chapter 2 with a view to understanding how their approach to the public issue has been informed by their cultural, political and social circumstances.

¹⁴² Waldo, (Washington, 2007), pg. 2.

Privacy as a Human Right

The 'right to privacy' was first outlined in Article 12 of the *Universal Declaration of Human Rights* of 1948. Article 12 states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation...¹⁴³

The *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 further reinforced this right in Article 8 which states,

Everyone has the right to respect for his private and family life, his home and his correspondence...¹⁴⁴

The Organisation for Economic Co-operation and Development (OECD) affirms that "privacy is a fundamental social right that concerns one and all".¹⁴⁵

In 1981, the Council of Europe reaffirmed its position on privacy and freedom of information by adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* in response to 'the increasing flow of across frontiers of personal data undergoing automatic processing.' The Council felt that it was necessary to reconcile the fundamental freedoms as well as human rights with respect to privacy and the free flow of information between people.¹⁴⁶ In this convention, the Council set out basic principles for data protection in an automated environment.

¹⁴³ United Nations, *Universal Declaration of Human Rights of 1948* at <http://www.un.org/Overview/rights.html>. Accessed on 28 January 2009.

¹⁴⁴ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 at human-rights-convention.org. Accessed on 28 January 2009.

¹⁴⁵ Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (Paris, 1981) at www.oecd.org. Accessed on 28 January 2009.

¹⁴⁶ Council of Europe, ETS no. 108 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* at conventions.coe.int. Accessed on 28 January 2009.

Samuel D. Warren and Louis D. Brandeis first articulated 'the right to privacy' or 'the right to be left alone' to the American legal profession in 1890.¹⁴⁷ However, it was not until the late 1960s and early 1970s that the Federal Government of the United States of America gave serious consideration to privacy matters. As with other societies, it was not until technology began to advance and there was the proliferation of databanks along with the accumulation of vast amount of personal data held by public and private institutions that the possibility of linking and manipulating information through sophisticated computer programmes increased the concerns with privacy.¹⁴⁸

When Warren and Brandeis examined 'The Right to Privacy' as articulated in the U.S. Constitution, they asserted that the right to privacy is considered a purely individual right of living individuals. They too agreed that the right to privacy relates to the customs of specific times and places and is not absolute. Warren and Brandeis defined the legal right to privacy for the first time based on precedents from legislation on copyright, defamation and disclosures of intimate or offensive private information. Their articulation of 'the right to privacy' was extremely influential in Supreme Court decisions as well as other jurisdictions in the twentieth century.

Seventy years after the Warren-Brandeis article, noted tort scholar William L. Prosser's analysis influenced the shaping of American privacy law and beyond. The tort right of privacy is distinct from the constitutional right to privacy, which is based on the U.S Bill of Rights. Prosser outlines four aspects of the tort of privacy that were subsequently enacted into law in whole or in part by state legislatures. These aspects are:-

- Intrusion on the plaintiff's seclusion or solitude, or into his private affairs

¹⁴⁷ Samuel Warren and Louis Brandeis, 'The Right to Privacy', *Harvard Law Review* Vol. IV, Massachusetts, 1890-1891.

¹⁴⁸ Menzi L. Behrnd-Klodt et al, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago: 2005), pg. 3.

- Public disclosure of embarrassing private facts about the plaintiff
- Publicity that places the plaintiff in a false light in the public eye
- Appropriation, for the defendant's advantage of the plaintiff's name or likeness¹⁴⁹

The Role of International/Trans-national Organisations in the Protection of Personal Data

The Organisation for Economic Co-operation and Development (OECD)

The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* was the first attempt at providing general guidelines on the handling of personal information in public and private sectors internationally. Approximately half of OECD member countries adopted some form of privacy legislation to prevent what was considered violations to fundamental human rights, namely the unlawful storage of personal data and the abuse of or unauthorised disclosure of such data.¹⁵⁰ Disparities in the various pieces of national legislation caused concerns that the free flow of data across borders could be hampered. Consequently, guidelines were developed to assist with harmonising national privacy legislation.

The OECD guidelines address data quality, specification of the purpose and limitations on collecting personal data, required security safeguards, openness, individual participation and accountability in the form of seven principles. The principles embodied in the Guidelines were that personal information must be:-

- collected fairly and lawfully
- used only for the purpose specified during collection
- adequate, relevant and not excessive to that purpose

¹⁴⁹ Prosser, William, *Handbook of the Law of Torts 4th ed.* (Minnesota, 1971).

¹⁵⁰ Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (Paris: 1981) at www.oecd.org . Accessed on 28 January 2009.

- accurate and up-to-date
- accessible
- kept secure
- subject to disposal after the purpose is completed¹⁵¹

The OECD principles, however, are nonbinding, and privacy laws vary widely across the globe. In some cases, like the U.S, the OECD recommendations are endorsed but not implemented in law. All seven principles were incorporated into the EU Data Protection Directive.

The EU Data Protection Directive 95/46/EC

The European Union Directive entitled *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, referred to in this study as the EU Data Protection Directive was adopted as a legislative provision in October 1995. This Directive required implementation of national data protection legislation by all EU Members States by 24 October 1998. The EU Data Protection Directive can be seen as a general framework legislative provision, which has as its objectives:

- a) The protection of an individual's privacy in relation to the processing of personal data; and
- b) The harmonisation of data protection laws in Member States.¹⁵²

In essence, the EU Data Protection Directive sets out to establish an equivalent level of protection for personal information across all Member States in order to facilitate the cross border transfer of that information within the European Union. It provides the conditions

¹⁵¹ Organisation for Economic Cooperation and Development (OECD), *Guidelines*. Accessed on 28 January 2009.

¹⁵² European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* found at ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. Accessed on 28 January 2009.

under which the processing of personal data is lawful, the rights of data subjects and the standard of data quality.

The EU Data Protection Directive applies to personal data processed in whole or in part by automatic means, as well as manual data held in filing systems that are structured by reference to individuals. It excludes areas not covered by EU law such as public safety, defence, State security and activities of the State in areas of criminal law. It also specifically excludes domestic and household activities.

In Article 6 of the Directive, fundamental principles are set out that have to be respected when processing personal data. Article 7 sets out a number of conditions that must be satisfied before data can be processed. This processing must take place only with the data subject's consent except when processing is necessary:

- a) for the performance of a contract to which the data subject is a party;
- b) for compliance with a legal obligation;
- c) to protect the vital interests of the data subject;
- d) to perform a task carried out in the public interest or in exercise of official authority;
or
- e) to meet the legitimate interests of the data controller, unless those interests are overridden by interests or fundamental rights and freedoms of the data subject.¹⁵³

There are special categories of data that may be processed under certain strict conditions. Data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, offences and criminal convictions can only be processed with explicit consent of the data subject except where a Member State's law provide that the prohibition of sensitive processing cannot be waived by the data subject.

¹⁵³ European Commission, *Directive 95/46/EC*. Accessed on 28 January 2009.

The Rights of 'Data Subjects' under the EU Data Protection Directive

The concept of the 'data subject' is well defined in the EU Data Protection Directive. It states clearly that the data subject has the right to be informed of where data is being collected either from the data subject or from a third party, the identity of the data controller, the purposes for which the data is being used and any further information necessary to ensure fair processing. Other rights of data subjects under the EU Data Protection Directive (95/46/EC) are:

- The right of access to personal data without constraint, at reasonable intervals and without excessive delays or expense;
- The right to object to processing of personal data, and where there is a justified objection, to have the processing stopped;
- The right object to personal data being used for purposes of direct marketing; and
- The right not to be subject to a decision that has legal effects on which is based on solely automated processing of data (unless the data subject's interests are safeguarded).¹⁵⁴

Conditions for the Cross-Border Exchange of Personal Data

The EU Data Protection Directive sets out conditions under which personal data that are processed or which are intended for processing may be exchanged or transferred to non-Member States. The countries are referred to as *third countries*.¹⁵⁵ These types of exchanges are facilitated through what are referred to as standard contractual clauses which specify the conditions under which personal data may be transferred.¹⁵⁶ In general, a transfer can take place if the third country can ensure 'an adequate level of protection' for the rights and freedoms of data subjects. There are exemptions in cases where the data subject gives

¹⁵⁴ European Commission, *Directive 95/46/EC*. Accessed on 28 January 2009

¹⁵⁵ Centre for Democracy and Technology at www.cdt.org/privacy/eudirective/EU_Directive_.html. Accessed on 17 February 2009.

¹⁵⁶ European Commission, *Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors of third countries under Directive 95/46/EC* at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF. Accessed 13 January 2014.

consent or if the transfer is necessary for contractual or legal requirements on public interest grounds.

The EU Data Protection Directive has been criticised for not adequately explaining the meaning of 'an adequate level of protection'. Yet, the Directive has effectively influenced third nations to re-visit and improve their existing privacy legislation in order to bring them in line with EU standards. In determining adequacy, the EU applies five criteria:-

- 1) The lawfulness of processing of personal data.
- 2) The special protection of sensitive data.
- 3) The rights of the data subjects.
- 4) The security of the actual processing of information.
- 5) The existence of control and enforcement measures.

The Directive could be viewed as the first real step towards unifying disparate international privacy regimes.¹⁵⁷ The lack of harmonisation will be discussed in the following section.

The International Organisation for Standardisation (ISO)

One challenge that is evident in the discourse on data protection and privacy is the lack of harmonisation on this subject in countries around the globe. In September 1996, the International Organisation for Standardisation (ISO), an umbrella body for national standards agencies, explored the feasibility of an ISO standard that would reflect the EU Data Protection Directive.¹⁵⁸ It was felt that such a standard would be welcomed by governments, businesses and organisations around the world. It was envisaged that this standard would provide a mechanism that would complement rather than replace

¹⁵⁷ European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* found at ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. Accessed on 28 January 2009.

¹⁵⁸ International Standards Organisation at <http://www.iso.org>. Accessed on 17 February 2009.

legislation; encourage best practice through a certification scheme and assist with accountability by facilitating independent audits.¹⁵⁹

However, the reality of the global privacy landscape does not appear to lend itself to the formulation of an overarching standard. There is very little consensus among nations about the specific features of such a standard. It was felt by those who participated in the negotiation of the privacy standard that it would be difficult to bridge the vastly different approaches to regulating data privacy.

Colin Bennett in his study *International Standard for Privacy Protection: Objections to the Objections* provided logical reasons why the standardisation of privacy protection is critical in the globalised economy. Among these reasons he states,

There is a manifest need for the negotiation of an international, technology-neutral, certifiable, management standard for the implementation of the information privacy principles that may be implemented by any public or private organisation that collects, uses, processes and discloses personal information via the Internet, or through any other public or private network.¹⁶⁰

At least seven objections were raised against the establishment of such a standard. It was useful for this study to review Bennett's objections on why a standard was not a viable option. These objections provide insight into the apparent lack of motivation for global harmonisation of privacy/data protection laws by some critiques and would help to inform the recommendations for the West Indian region. They are as follows:

Objection 1: Privacy is not a fundamental human right and has no place within the standards arena.

¹⁵⁹ Colin Bennett, *An International Standard for Privacy Protection: Objections to the Objections* (British Columbia: 1996) at www.cous.uvic.ca/poli/bennett. Accessed on 12 February 2009.

¹⁶⁰ Colin Bennett, *An International Standard...* Accessed on 12 February 2009.

Bennett's Rebuttal: There is already a common international consensus on what it means to treat personal information in a privacy-friendly manner. A privacy standard could operate as a management standard, rather than a technical standard, which could measure for consumers, clients, competitors and regulators the extent to which organisations do indeed treat the personal information under their control in appropriate ways.

Author's Viewpoint: The idea of incorporating baseline guidance for organisations in the form of a management standard is feasible. At a fundamental level, the principles for privacy/data protection are similar across the globe and so there is some basis for an international approach.

Objection 2: An international privacy standard would be difficult to negotiate among widely different cultures.

Bennett's Rebuttal: The historical and cultural sources of privacy concerns may differ in interesting and dynamic ways, but the definition of what it means to be 'responsible' has increasingly converged. A basic and common understanding [exists] of how the responsible organisation should treat the personal data that it collects, stores and processes, regardless of technology.

Author's Viewpoint: If a global standard is developed, it would need to be reasonable and practicable, not overly prescriptive so as to be adaptable within any environment.

Objection 3: We already have three sets of Guidelines from OECD (on privacy, security and cryptography), why another instrument?

Bennett's Rebuttal: The OECD Guidelines are indeed still in force. They have been a useful template for eliciting commitment from four major companies in the U.S and Canada to adhere to privacy principles. However, the OECD guidelines have been surpassed by the EU

Data Protection Directive which in four little words have [ensured] that organisations outside of Europe will have to take their commitment to privacy seriously, *adequate level of protection*. Personal data should not be transferred outside European Member States unless the receiving jurisdiction [meets this requirement.] Businesses that transfer personal data about European clients, consumers and competitors will have to assure European authorities that their industry and professional codes are complied with. A statement of good intentions will not suffice. An international standard could simplify the process of determining adequacy within a highly complex and networked data processing environment.

Author's Viewpoint: An international standard will apply regardless of jurisdiction and would foster harmonisation required for global e-business to be conducted without complications.

Objection 4: No organisation would adopt an international privacy standard.

Bennett's Rebuttal: A privacy standard is the most efficient way to allay consumer fears regarding privacy protection. It allows advocates to measure business standards according to a common yardstick and gives companies that want to develop a privacy policy, a template. A standard (unlike a code of practice) can be referenced in a contract. European data protection agencies might enforce Article 25 of the EU Data Protection Directive by requiring any recipient of European data to be registered to the international standard. The standard may serve to harmonise the existing, and highly variable, "privacy seals" for websites. If privacy is good business, then the market should be forcing continual improvement in the presentation and quality of these different self-regulatory mechanisms. [This can be made possible] through a conformity assessment regime like an ISO standard.

Author's Viewpoint: As has been the case with other global standards, a global standard for privacy will be respected and as long as it is reasonable and attainable, countries will seek to raise their profile by adopting the standard.

Objection 5: An international privacy standard would be too costly.

Bennett's Rebuttal: First, the loss of one's reputation as a responsible corporate citizen because of privacy scandal can be very costly. Adoption of a privacy scandal can save time and energy otherwise spent on a contentious process of claims and counterclaims. Second, implementing privacy protection policy is not generally a complicated process. It would certainly be more straightforward than those within the ISO 9000 series of management standards. Privacy protection could be a component of 'total quality management' and indeed there are some interesting parallels between the fair information principles and the requirements of quality assurance. Third, many organisations are probably already conforming to a good number of the privacy principles without even knowing it. The introduction of a credible international standard within the marketplace would provide a far more effective measurement tool.

Author's Viewpoint: Jurisdictions recognise that they must comply with international expectations for privacy in order to remain competitive and to be respected. This study suggests that these jurisdictions will seek to do what is necessary not to lose any favour with their more developed counterparts and potential benefactors.

Objection 6: One standard cannot 'fit all'

Bennett's Rebuttal: This is true but it is hardly an obstacle. Any set of data protection rules will need to be adapted to the specified circumstances of different sectors. Many legislative schemes enable the negotiation of codes of practice in order to translate the language of

the law into practical advice for banks, direct marketers, health-care providers, telecommunications companies and so on. The privacy principles are sacrosanct, but tailoring them to their needs and problems, different organisations might develop codes of practice that explain how the principles will be implemented.

Author's Viewpoint: There has already been success with other global legal initiatives such as dealing with intellectual property and copyright. At a local level, it is sensible to use other legal instruments in the form of regulations and codes to implement the global standard for adaptability to meet national expectations and requirements. The standard should be implemented in way that does not contradict existing national legislation.

Objection 7: It would never work in the United States

Bennett's Rebuttal: It is disappointing but not surprising that the initial American reaction to this initiative should have been so negative. The US is "different". But should it not be allowed to be different? Whatever the cultural, constitutional and institutional differences, the reality remains that American multi-nationals in every sector, and many manufacturing sectors, will need to convince European authorities that when they process personal data on European citizens that they comply with fair information practices. Furthermore, the current 'Safe Harbor' negotiations (1996) between the EU and US Department of Commerce indicate that one principle of European concern is that many American companies might hide a number of privacy invasive practices being the 'Safe Harbor' label. The adherence to Safe Harbour principles by organisations will hopefully entail a commitment to implement those principles.

Author's Viewpoint: It is true that the US is allowed to be different but the need for harmonisation should override America's cultural, political and other differences. In

conducting cross-border business, the US would need to conform to the global standard like other jurisdictions to prevent restrictions and complications with exchange of information. The Safe Harbour agreement could be seen as the first step towards conforming to a global standard.

Bennett further concludes that a separate international privacy standard is in the interest of all nations and stakeholders. He contends that the internationalisation of personal data communications within the global information infrastructure will require a concomitant internationalisation of privacy standards. He adds that in reality only a minority of countries will be motivated to conform to the EU model of a general data protection law overseen by an independent supervisory authority. Therefore, a comprehensive ISO standard is a crucial instrument for data protection within the 21st century fluid, networked and computerised environment.¹⁶¹

This thesis contends that it is challenging to garner consensus towards the establishment of a comprehensive international standard for data protection. It appears difficult to achieve accord even on the nomenclature and the definition of the term. The cultural and other factors that influence how privacy is perceived from country to country vary to a degree that would inhibit full harmonisation. However, it is possible to have a basis or framework to assist countries with operating in a homogeneous environment. In 2011, the ISO International Electrotechnical Commission (IEC), managed to formulate an international standard entitled the *Information Technology – Security Techniques – Privacy Framework* ISO/IEC 29100: 2011. This standard, which was born out of long debate and arduous work according to its authors¹⁶², seeks to provide a privacy framework that specifies a common

¹⁶¹ Colin Bennett, *An International Standard for Privacy Protection: Objections to the Objections* (British Columbia, 1996) at www.cous.uvic.ca/poli/bennett. Accessed on 12 February 2009.

¹⁶² Presentation at the IAPP Europe Data Protection Intensive 2013 held in London 23-25 April 2013.

privacy terminology; define the key actors and their roles in processing personal identifiable information (PII); describe privacy safeguarding considerations and provides references to privacy principles for IT.¹⁶³ This framework is the first real step towards fostering a homogenous environment across privacy regimes. Yet, full harmonisation remains unattainable.

The US privacy regime, as will be seen in the following chapter, appears to be a 'polar opposite' of the European approach. The US paradigm is not partial to a centralised, omnibus piece of data protection legislation or regulation of privacy in the public and private sector. The challenge with harmonisation across these two regimes is evidenced by the re-emergence of debate and discussion on the 'Safe Harbor' agreement first establishment in 2000.¹⁶⁴ Recent developments with anti-terrorist measures taken by the US Government including the activities of the National Security Agency (NSA) and the Central Intelligence Agency (CIA) have given rise to renewed fears and/or concerns about the use of personal data, not only of US citizens but of travellers worldwide. It is alleged that these agencies continue to monitor private telephone exchanges as well as private Internet activity globally. Hence, the need for privacy in today's environment is a global reality because of the highly networked Information and Communication Technologies (ICTs). Added to these occurrences is the 2010 'WikiLeaks' scandal where key secret military documents and diplomatic reports were released for public viewing by an on-line journalist organisation.¹⁶⁵ News also broke about a former contractor for the CIA, Edward Snowden, who in 2013, leaked details about the extensive Internet and telephone surveillance

¹⁶³ International Standards Organisation, ISO/IEC 29100: 2011 *Information Technology – Security Techniques – Privacy Framework* at www.iso.org.

¹⁶⁴ PistolStar Authentication Blog, *Problems in the "Safe" Harbor* at blog.pistolstar.us/blog/problems-in-the-safe-harbor. Accessed on 25 January 2014.

¹⁶⁵ The Most Important News, *WikiLeaks Scandal Explodes* at themostimportantnews.com/archives/the-wikileaks-scandal-explodes. Accessed on 25 January 2014.

undertaken by American intelligence services.¹⁶⁶ Consequently, the rise of privacy advocates and groups as well as the emergence of a cadre of privacy professionals in today's interconnected societies can be viewed as a 21st century response to the growing need for privacy and should lead to more fervent efforts at harmonisation in the not too distant future.

Common Ground in International Legislation on Privacy

In 2003, the study entitled, *Data Protection Laws around the World* stated that forty countries were then engaged in enacting some form of privacy legislation.¹⁶⁷ In 2014, the number is approaching sixty countries.¹⁶⁸ In spite of the variances in the international legislation dealing privacy/data protection, there exists some common ground as it relates to the principles that underpin the legislation. The doctrine of 'fair information principles' (FIPs) initially developed in the U.S, appears explicitly or implicitly in all national privacy/data protection laws including those of Australia, New Zealand and Canada.¹⁶⁹ They also form the basis of international agreements. Although the principles may vary over time and space, a study by David Basinar on data protection laws around the world identify the following common tenets:

An organisation (public or private):-

- 'must be *accountable* for all personal information in its possession
- should *identify the purposes* for which the information is being processed at or before the time collection
- should only collect personal information with the *knowledge and consent* of individuals (except under specified circumstances)

¹⁶⁶ BBC News, *Edward Snowden: Leaks that exposed US spy programme* at www.bbc.co.uk/news/world-us-canada-23123964. Accessed on 25 January 2014.

¹⁶⁷ David Basinar, *Data Protection Laws around the World* (April 2003) at www.privacy.org/survet/dpmap.jpg Accessed on 7 February 2009.

¹⁶⁸ Information Shield, *International Privacy Law* at www.informationshield.com/intprivacylaws.html. Accessed on 25 January 2014.

¹⁶⁹ David Basinar, *Data Protection Laws around the World* (April 2003) www.privacy.org/survet/dpmap.jpg Accessed on 7 February 2009.

- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes
- should *not use or disclose* personal information for purposes other than those identified, except with the consent of the individual (the finality principle)
- should retain information only *as long as necessary*
- should ensure that personal information is kept *accurate, complete and up-to-date*
- should protect personal information with *appropriate security safeguards*
- should be *open* about its policies and practices and maintain no secret information system
- should allow the data subject *access* to their personal information with an ability to amend it if it is inaccurate, incomplete or obsolete¹⁷⁰

Principles which underpin the establishment of legislation are critical when seeking to implement data protection. Article 6 of the EU Data Protection Directive speaks to five principles that are among the above stated principles of the OECD.¹⁷¹ These ideas are also represented in the Information Privacy Principles of the Australian Privacy Act. The main notion of these principles is that personal information should be processed fairly and lawfully and held securely.

Unlike legislation, principles will not change over time based on case law and other societal factors. Therefore, when considering the main elements required for the establishment of a successful data protection regime, the formulation of main principles should be taken into account.

Understanding European Data Protection

In examining the development of data protection in the European context, the study considers the writings of András Jóri, Hungarian Data Protection Ombudsman in his 2006 study *Data Protection in Europe* where he provides insight into the use of the term 'data

¹⁷⁰ David Basinar, *Data Protection Laws around the World*.

¹⁷¹ European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* found at ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

protection'. He surmises that data protection (derived from German term '*Datenschutz*') is seen as a part of privacy protection. His work supports the idea that data protection as a concept became wider spread in the 1970s hence signifying a new type of protection compared to earlier notions of privacy protection. Data protection, Jóri argues is far wider than just being a European legal solution to a problem. Yet, the term 'data protection' is only understood in the framework of privacy protection as a legal tool of privacy protection arising within a given social and technical context.¹⁷²

Jóri contends that this type of privacy protection existed long before data protection. Data protection as a specific legal tool appeared as a result of the weakening or disappearance of some natural boundaries that earlier ensured protection of privacy. Data protection, thus, may be interpreted as part of privacy protection. He further states,

Data protection in all cases means the legal protection of an individual's privacy which appeared in Europe as an answer to the dangers of electronic data processing which were becoming widespread via electronic revolution, beginning with the 1970s, and the content of the legal protection provided by it has changed significantly since its appearance several times, and is still changing presently.¹⁷³

Jóri argues that data protection cannot be identified with the right of 'informational self-determination' as has been argued by some scholars because data protection laws did not guarantee an individual control over his personal data. According to his argument, data protection includes all regulations that, via the regulation of the treatment of an individual's personal data, aim at the protection of these data, irrespectively of whether this regulation ensures the right of informational self-determination of an individual or not. Interestingly, this German concept reflects a different meaning from 'the right to privacy' in the US context. The US 'right to privacy' is based on concept of the right of the individual to be left alone whereas the concept of informational self-determination is concerned with the right

¹⁷² András Jóri, *Data Protection in Europe* (2006-2007) at www.dataprotection.eu. Accessed on 17 February 2009.

¹⁷³ András Jóri, *Data Protection in Europe*...Accessed on 17 February 2009.

of the individual to choose what information he or she wants shared and under what conditions. It is much narrower in focus when compared with privacy in the US context. Data Protection evolved from this concept of informational self-determination and in a similar way deals more specifically with the use and/or abuse of personal data.

Jóri outlines three stages in the development of data protection theory. He refers to these stages as 1) the first generation data protection norms 2) the second generation data protection norms and 3) globalisation.

The first generation acts were born in the second half of the 1960s when organisations owning large amounts of records, both in the public and private sector, started to use computers.¹⁷⁴ This led to the emergence of databases and ‘integrated data management’. These developments led to the so-called data protection debates (*Datenschutzdiskussion*) in Germany and later the data protection act.¹⁷⁵ In this period, computers were owned by few, and data-controllers were primarily state-run. There was a perceived threat that the state would gain informational superpower by connecting various registries. Hence, the first data protection laws took special consideration of the challenges in dealing with new technology.¹⁷⁶

The second generation data protection norms were triggered by the 1983 German Federal Constitutional Court declaration that some of the provisions of the act concerning the census of 1983 were unconstitutional. He argues that this was a catalyst for change in the data protection policies and laws around the globe. In the famous census decision (*Volkszählungsurteil*), the court ruled that the ‘basic right warrants [...] the capacity of the

¹⁷⁴ András Jóri, *Data Protection in Europe...*

¹⁷⁵ *Federal Data Protection Act 1994 (Germany - Bundesdatenschutzgesetz BDSG)* at www.iuscomp.org/gla/statutes/BDSG.htm.

¹⁷⁶ *Privacy in Research, Ethics and Law* at www.privireal.org. Accessed on 17 February 2009.

individual to determine in principle the disclosure and use of his/her personal data.¹⁷⁷ Consequently, it was the German Federal Constitutional Court that first rendered the term 'informational self-determination' based on this principle.

The third stage of development relates to the need for harmonisation in national legislations to facilitate the transborder flow of personal data. The first development in the globalisation of data protection occurred when the Organisation for Economic Co-operation and Development (OECD) formulated its data protection guidelines in 1980. The OECD guidelines might be understood to be the first common denominator between Europe and the United States. The Council of Europe's adoption of the 1981 Convention for Data Protection was another step towards the process of unifying the data protection regime. Ultimately, the *EU Data Protection Directive* of 1995 (95/46/EC) has had the most significant international impact as a result of the need for 'adequacy' by non-EU countries to meet EU standards. It has influenced change in privacy/data protection legislation including that of Canada, Australia and Argentina.¹⁷⁸ This examination of the stages of data protection provided significant insight into the mindset of European leadership as it relates to informational privacy.

Conclusion

The literature on the origins and development of privacy as a concept and data protection as a response to a public issue has revealed two significant conclusions. Firstly, that advances in technology are the principal factor in enabling organisations to create, manipulate, use and retain vast amounts of records and information containing personal information. Secondly, there is a direct and tangible link between the fear of citizens of the

¹⁷⁷ Federal Government of Germany, *The Census Act of 1983* found at www.servat.unibe.ch/dfr/bv065001.html.

¹⁷⁸ Privacy in Research, *Ethics and Law* at <http://www.privereal.org>. Accessed on 17 February 2009.

exponential increase in the capacity of organisations to manipulate information using powerful technology and the development of data protection as a public policy. It can be argued that there is significant difference between the period under examination in this study (1960 – 2014) and any other period in human history.

Today, personal information can lead to the incarceration of individuals in the ‘post 9/11’ world where US agencies like the National Security Agency (NSA) have used the terrorist attacks in New York in September 2011 to justify spying or what it refers to as ‘intelligence gathering’ on American and global citizens.¹⁷⁹ In recent times, the American Civil Liberties Union has accused the NSA along with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) of spying on Americans illegally since the Bush administration and are acting in breach of the US Constitution. This practice, referred to as ‘government eavesdropping’, has heightened the tension between the need for protection of the nation by agencies and the danger of those agencies becoming domestic spying agencies.¹⁸⁰ At the crux of this tension is the development of increasingly intrusive technologies used to collect personal data.

This thesis builds upon the factors identified in the literature but does so from a perspective not yet explored in any international discourse on privacy and data protection. It is the first study that engages explicitly with the relationship between data protection and the management of records and information of citizens. It asserts that there is an irrefutable relationship between data protection and records and information management. As will be seen in the chapters to follow, the processes for the successful management and necessary protection of personal information and the theories underpinning records and

¹⁷⁹ The Guardian, *The NSA Files* at www.theguardian.com/world/the-nsa-files. Accessed on 21 January 2014.

¹⁸⁰ American Civil Liberties Union, *NSA Spying on Americans is Illegal* at www.aclu.org/technology-and-liberty/nsa-spying-americans-illegal. Accessed on 20 April 2014.

information management are complementary. The thesis further recognises that the relationship between data protection and records management is influenced by underlying issues relating to power, control and domination as it relates to how records and information containing personal data are used in modern societies. This relationship will ultimately be considered in the context of the unique and unexplored context of the West Indies.



Image 2 Origin of the term 'data protection' - German

www.dreamstime.com/stock-images-data-protection-image19541884¹⁸¹

¹⁸¹ Stock Image from stock image and video website *Dreamstime* focusing on data privacy.

1.2 Data Protection: Relationship to Records Management

What are Records?

Records management literature provides a number of definitions of a 'record' which at the core are similar in meaning. The International Standards Organisation defines a record as, 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business' (ISO 15489.2 *Records Management Standard*). Elizabeth Shepherd and Geoffrey Yeo in their text, *Managing Records: A Handbook of Principles and Practice*, simply define a record as 'any recorded evidence of an activity'.¹⁸² Yeo, however, would later expand on the philosophy behind the definition of a record as 'a persistent representation' of an activity.¹⁸³ This theory has significant bearing on the discussion of the changing nature of records in the digital world and how that relates to data protection and will be further explored in the Chapter 3.

The definition of a record in a recent text by Laura Miller, *Archives: Principles and Practices* where she defines a record as, 'a piece of information that has been captured on some fixed medium...and that has been created and used to remember events or information or to provide accountability for decisions or actions', is also relevant because it speaks to the role of a record as it relates to ensuring accountability in actions are preserved.¹⁸⁴ This idea is pertinent to the discussion on records and privacy when examining the issues of personal data retention and erasure. These issues have become topics for debate and discussion under the proposed changes to the European data protection regime and will be examined more closely in Chapter 4.

¹⁸² Elizabeth Shepherd and Geoffrey Yeo, *Managing Records: A Handbook of Principles and Practice* (London, 2003), p. 2.

¹⁸³ Geoffrey Yeo, *Records and Representations*, Paper presented at the Conference on the Philosophy of Archive, Edinburgh, Scotland, 10 April 2008.

¹⁸⁴ Laura Miller, *Archives Principles and Practices* (London, 2010), p. 3.

Further to this, Miller explores the evidential quality of records stating that records are supposed to convey evidence in part because they are created in order to remember something – a piece of information, a decision, an opinion – at a particular moment in time.¹⁸⁵ She describes the characteristics of records stating that a record should not sit alone as an isolated item but its meaning is derived from a combination of its content, context and structure. *Content* is the text, images, sounds, or other information that makes up the substance of the records; *Context* is the functional, organisational and personal circumstances surrounding the creation of the record and *Structure* relates to the physical and intellectual characteristics that define how a document is created and maintained. Other values attributed to records are that they must be static, unique and authentic. The study considers in Chapter 3 how all of these characteristics and values are employed when seeking to be compliant with data protection in a recordkeeping environment.

The word ‘record’ is also defined by ARMA International as ‘recorded information, regardless of medium and characteristics’.¹⁸⁶ Traditionally, records were created in paper-based formats, taking the form of correspondence, reports and forms. However, as a result of technological advancements, records began to be created and used in a range of formats including microfilm, punch cards, magnetic tapes, disk, map, photographs and computer print-outs.¹⁸⁷ The study examines and discusses the types of records involved in the regulating of privacy/data protection within public and private organisations. Understanding what is a record, what type of record contains personal information and how that record should be treated will be considered. Most importantly, defining what elements of a record make it truly personal is a critical aspect of the study of data protection and its relationship to records management.

¹⁸⁵ Miller, (London, 2010), p. 5 - 9.

¹⁸⁶ ARMA International at www.arma.org. Accessed on 26 February 2009.

¹⁸⁷ Mary F. Robek et al, *Information and Records Management* 4th ed. (California, 2000), p. 4.

The thesis considers the writings of Luciana Duranti who argues that there are new uses for the old science of diplomatics which looks at the origin and historical development of documents to assess their authenticity and originality. Diplomatics is principally concerned with archival documents.¹⁸⁸ Duranti discusses the concept of originality where an original document is distinguished from a copy or draft by determining 'the degree of authority' of the document under examination. One of the key criteria according to the science of diplomatics is that a record is a 'written document'. This idea traditionally used to determine the originality and authenticity is challenged in today's digital world because of new technological trends such as instant messaging, social media and 'cloud-computing'. 'Documents' in electronic formats are being created in one form and transmitted in another format. 'Documents' are also being moved across platforms and stored remotely by their creators. In this environment, 'documents' are fluid. Documents are no longer just found within the control of archives and/or public and private organisations but may be found on the Internet, made available intentionally or unintentionally by their creators. This study discusses the changing meaning of the term 'document' as well as the changing nature of records to assess the implications for managing privacy.

David Bearman also examines the new role for diplomatics when dealing with electronic records management. He compares and contrasts the European and American archival traditions as it relates to their response in dealing with electronic records management. Bearman contends that the European archival tradition is more strongly governed by bureaucratic authority and there is a reliance on staff compliance with policies and procedures to control recordkeeping in automated environments. The American tradition relies more heavily on the technology itself, using metadata to track actual transactions

¹⁸⁸ Luciana Duranti, *Diplomatics: New Uses for an Old Science* Achiviara 28 at journals.sfu.ca/archivar. Accessed on 30 January 2014.

within systems rather than relying on staff to ensure that policies and procedures are upheld. He surmises that the Canadian approach represents a 'middle ground' between the European and American response to electronic records management.

The elements of Bearman's discourse that are most useful to this study are his views on what he considers the fundamental problem when dealing with electronic records held with automated systems, that is, determining the authenticity of electronic records. He speaks to the need to identify functional provenance of electronic records to establish 'evidential historicity'. The user must be able to ascertain the contextual background of the electronic record. He further argues that European 'diplomats-like principles' are needed to identify functional provenance of electronic records.¹⁸⁹ In the digital world, automated environments make it more challenging to determine which records are true records because of the fluid nature of electronic environment. Additionally, organisational records created in electronic environments are less formal than in the paper world of the past. Staff of organisations are mixing business information with personal information especially when using electronic mail communications. This phenomenon has implications for data protection because it is difficult to identify which data or records are private or business-related in nature in order to ensure data protection compliance. These issues are fully explored in Chapter 4.

What is Records Management?

From the time humankind began to utilise forms of technology to produce information, there has been the need to manage and control information. Chosky in her study,

¹⁸⁹ David Bearman, *Diplomatics, Weberian Bureaucracy and the Management of Electronic Records in Europe and America* Archives & Social Studies: A Journal of Interdisciplinary Research at archivo.cartagena.es/publicas/catalogos/social_studies/_vYni1KYCfL-ZPeZr1dQhYw. Accessed on 30 January 2014.

Domesticating Information: Managing Documents inside the Organisation, discusses the history of 'records management'; a term first coined in the U.S, and tracks the development in the use of the term from the late nineteenth century to recent times. Records management was traditionally practised to some degree as part of archival administration in the European and British traditions. A leading American archival theorist, Theodore R. Schellenberg, propagated a major reason for archival interest in records management thereby setting apart records management as a separate but related discipline to archival studies.¹⁹⁰

In 1941, the National Archives of the U.S established a records administration programme. Chosky asserts that the practice of records management remained fairly stable until the early 1960s. It was at this time that the U.S Federal government increased its use of computer technology in record creation and this led to the preservation of records in databases or back-up tapes. There was, however, a definite loss of control over records evidenced by the fact that an entire 1960 set of census data was lost.¹⁹¹ Hence, there was the perceived need to control and manage records from this period and beyond. For this study, this is the beginning of the relationship between data protection and records management. Both pursuits arose as a result of similar circumstances, that is, the need to control information due to rapid advances in technology.

Recordkeeping systems evolved over the passage of time moving from manual, paper-based systems to highly networked, automated systems. By the 1970s, there was the proliferation of mini-computers and the computerisation of organisations. Additionally, there was the emergence of two types of machines, 'data processing' and 'word processing' machines.

¹⁹⁰ James Bradsher, *Managing Archives and Archival Institutions* (Chicago, 1989), p.34.

¹⁹¹ Coral Chosky, *Domesticating Information: Managing Documents inside the Organisation* (Maryland, 2006), p. 29.

Ironically, in spite of the use of automation, the widespread use of carbon paper and the photocopier resulted in exponential growth in the creation and distribution of paper records. By the late 1980s, an explosion in the creation of electronic records also added a new dimension to the need for control recordkeeping. The most significant development in recordkeeping was yet to come. It took place in the 1990s with the invention of the World Wide Web and the Internet which resulted in a paradigm shift in computing with agencies, both public and private, participating in e-commerce and e-government.¹⁹² Records and information were created, received, distributed and stored in highly networked environments which increased the risks of duplication, unauthorised disclosure and questionable security in recordkeeping.

By the 1960s, the advent of the use of revolutionary technologies in the business process would raise questions about the *integrity* and *authenticity* of records created and used within automated systems. There is also the need to ensure the *security* of organisational records and information which is a key concern in data protection. The definition provided by Robek et al which describe 'records management' as, 'the application of systematic and scientific controls to recorded information required in the operation of an organisation's business' is very useful.¹⁹³ The use of the words 'systematic and scientific' suggests that the practice should be carried out in manner which is consistent from the beginning to the end of the process and always has the same results. A records management programme, therefore, ensures that organisational information is timely, accessible, accurate, authentic, usable and complete.

¹⁹² Chosky, p.31.

¹⁹³ Mary F. Robek et al, *Information and Records Management* 4th ed. (California, 2000), p. 24.

Mary Robek highlights one of the core concepts of records management as a discipline, the 'life-cycle' concept. This concept highlights the stages where records management controls are applied to business records. The five major stages are 1) *creation* stage, 2) the *distribution and use* stage, 3) the *storage and maintenance* stage, 4) the *retention and disposition* stage and 5) the *archival preservation* stage.¹⁹⁴ Frank Upward of Australia would later introduce a new concept to the discipline called 'the Records Continuum' or 'post-custodial' concept. The Records Continuum concept seeks to represent the nature of records through space and time highlighting both social and organisational relationships. The concept principally takes into account the changes brought about in recordkeeping by new technologies. It is a departure from the traditional custodial approach taken by archivists.¹⁹⁵ This concept which speaks of four dimensions of recordkeeping activity as well as four vectors demonstrating the characteristics of records and emphasizing both their organisation efficiency and cultural meaning. This concept is pertinent to the study because it is best suited to deal with how records should be managed in the digital world.

The lifecycle concept has been criticised for its shortcomings for electronic records management. Although it remains useful in establishing a sense of order in physical records management, the artificial separation of roles and functions between the records manager and the archivist is inadequate when dealing with managing electronic records in automated systems. A symbiotic relationship between the records manager and archivist is promoted in the continuum concept.¹⁹⁶ In the digital world, records must be managed from the outset and they are pluralised in meaning and value from their creation. Alan Bell, in his

¹⁹⁴ Robek, (California, 2000), p. 24.

¹⁹⁵ Frank Upward, *Structuring the Records Continuum – Part 1 Postcustodial Principles and Properties* found at www.infotech.monash.edu.au/research/groups/rcrg/publications/recordscontinuum-fupp1.html. Accessed on 17 October 2012.

¹⁹⁶ Jay Atherton, *From Life Cycle to Continuum: Some Thought on Records Management – Archives Relationship* Achivaria 21at journals.sfu.ca/archivar. Accessed on 30 January 2014.

article entitled, *Participation vs. principle: Does technological change marginalize recordkeeping theory?*, in his discourse about the continuum explains that in the continuum, records exist in multiple contexts and encompass multiple value propositions concurrently.¹⁹⁷ It is therefore important to examine how to deal with privacy in the multi-dimensional records continuum where multiple values are competing and therefore have to be reconciled in order to strike a balance between protecting individual privacy and preserving societal meaning. This idea will be further discussed in Chapter 3.

Exploring the Relationship between Data Protection and Records Management

Key principles in the regulation and management of privacy/data protection and related information rights legislation such as Freedom of Information (FoI) are integral to records management. A core purpose of data protection principles and legislation is to ensure the security and integrity of personal information. Records management ensures the security and integrity of all forms of records information as well as safeguarding accountability and promoting transparency. Data protection has as its main objective to protect individuals from harm, inconvenience, embarrassment, and/or unfairness by safeguarding the confidentiality and integrity of personal data contained within records.¹⁹⁸ Whilst records management closely examines business processes within an organisation to ensure that standards for recordkeeping are maintained from the creation of records to their final disposition. The two pursuits both achieve the same end and could be considered 'two sides of the same coin'. This is even evident in the use of the terminology as will be discussed in the following section.

¹⁹⁷ Alan Bell, 'Participation vs. principle: does technological change marginalize recordkeeping theory?' *In Archives and Recordkeeping: Theory into Practice* ed. Caroline Brown (London, 2014), p. 242.

¹⁹⁸ Ricks, Swafford & Gow, *Information and Image Management: A Records Systems Approach* (Ohio: 1992), p. 478.

RM and Related Terminology Using the UK Data Protection Act (DPA) 1998

The term 'data' is defined in the UK Data Protection Act (DPA) of 1998 as information which is:

- a) being processed by means of equipment operating automatically in response to instructions given for that purpose;
- b) recorded with the intention that it should be processed by means of such equipment;
- c) recorded as part of *a relevant filing system* or with the intention that it should form part of a relevant filing system;
- d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record, or
- e) *recorded information* held by a public authority and does not fall within any of paragraphs (a) and (d).¹⁹⁹

Two terms used in this definition directly relate to the records management function. These terms are 'recorded information' and 'a relevant filing system'. Records management as a professional discipline is primarily concerned with the management of document-based information systems but it also deals with the management of database information systems in which information is stored electronically.²⁰⁰ Records containing 'personal data' form a significant part of any organisation's informational assets. These records are usually found within the manual and automated systems which are usually managed by archivists/records managers, directly or indirectly. In highly centralised systems, archivists/records managers develop classification schemes to arrange records/information into categories that facilitate quick retrieval and comprehensive control of the data within.²⁰¹

The EU Data Protection Directive defines the term 'personal data' as 'any information relating to an identified or identifiable natural person...specific to his physical, physiological,

¹⁹⁹ *Data Protection Act 1998* (UK) Section 2 at www.legislation.gov.uk/ukpga/1998/29/contents.

²⁰⁰ Ricks, Swafford & Gow, (Ohio: 1992), p. 24.

²⁰¹ Mary F. Robek et al, *Information and Records Management* 4th ed. (California, 2000), p. 4.

mental, economic, cultural or social identity'.²⁰² The UK DP Act defines 'sensitive personal data' as personal data consisting of information about the racial or ethnic origin of the data subject, their political opinion, their religious beliefs or beliefs of a similar nature, whether he/she is a member of a trade union, his/her physical or mental health or condition, his/her sexual health and the commission or alleged commission of criminal offences. Other jurisdictions have used similar definitions based on that found in the EU Directive and will be scrutinised further in the study. Recorded personal information is predominately found in records in the human resources, finance and administration sections of any given organisation. Some organisations would have a higher concentration of records containing personal data because of the nature of their business such as educational, medical or judicial institutions. The study will examine how records management programmes in these institutions would need to put additional measures in place to ensure the security of highly sensitive data.

Another term shared by data protection and records management is that of 'processing' data. The UK DP Act defines 'processing' as, 'obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- a) organisation, adaptation or alteration of the information or data;
- b) retrieval, consultation or use if the information or data;
- c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- d) alignment, combination, blocking, erasure or destruction of the information or data.'²⁰³

²⁰² European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* found at ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. Accessed on 11 May 2014.

²⁰³ *Data Protection Act 1998* (UK) Section 1 at www.legislation.gov.uk/ukpga/1998/29/contents. Accessed on 21 April 2014.

Many of these actions are carried out as part of records management programmes where documents and records, including, those containing personal information, are created or received, classified, arranged, distributed, consulted, updated, maintained, appraised, destroyed when no longer needed, reviewed or archived, are part and parcel of processing that data. The paper will examine how these terms really impact on the relationship between data protection and records management.

Data Protection Code of Practice for Archivists and Records Managers UK

The United Kingdom is the only jurisdiction to date to have developed a Code of Practice for Archivists and Records Managers under the DPA 1998. It is a useful document which will need to be considered in the study. The Code was originally drafted by a joint working party composed of representatives of the Society of Archivists, the Records Management Society and the Public Records Office (later The National Archives). This Code falls under Section 51 (4) of the Data Protection Act. The Code states in its introduction that,

Records managers are clearly most immediately concerned [with the Data Protection Act] but archivist may well have records passed to them which contain information about who are still alive and may themselves create relevant databases, electronic documents or paper files of personal information that are subject to the Act.²⁰⁴

As a result, the Code is intended:

- 'To explain how data protection must be integrated into corporate information and security policies
- To provide guidance for the processes that records manager carry out in the order in which they need to be addressed from the point of view of records managers
- To provide similar guidance to archivists, where this different from the guidance applicable to records managers
- To explain terms used in the Act and this Code

²⁰⁴ The National Archives (UK), Society of Archivists, Records Management Society and National Association of Information Managers, *Code of Practice for Archivists and Records Managers Under Section 51(6) of the Data Protection Act 1998* at www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf. Accessed on 28 January 2009, p. 3-4.

- To draw attention to the main provisions of the Act insofar as they affect records managers and archivists
- To provide specimen forms and forms of word'

The Code comprehensively states the responsibilities of records manager and archivists when dealing with records containing personal data from acquisition to retention to the provision access. The Code covers the entire records lifecycle and addresses records in all formats. It does not seek to cover unlikely issues that affect records managers and archivists. The Introduction to the Code points out that those working in a specialist repository will probably need to seek additional advice. Nonetheless, the document in its entirety is evidence of the connectivity between records and archives management and data protection regulation. The study will examine whether this type of Code is relevant and adequately assists records managers and archivists to efficiently carry out the functions required to regulate data protection within their organisations.

CONCLUSION

This thesis asserts that data protection cannot be successfully implemented if the records management environment in which a public or private entity operates is not sound. There is a mutualistic relationship between the two pursuits. Data protection cannot be successful if records and information are managed in an ad hoc manner. Control of records and information in a systematic way is critical to data protection. Records management principles and processes are essential to firstly identifying which records and information contain personal data, secondly to providing adequate security of those records and information regardless of format, thirdly controlling access to those records and information internally and externally and fourthly, appropriately handling the final disposition of those records and information.

All key aspects of records management in principle and practice and its relationship to data protection are explored in Chapter 3 of the study. Incorporation of data protection principles in accepted records management concepts such as the 'lifecycle' concept and the 'records continuum' concept are undertaken. Ultimately, the study develops a new concept that would assist archivists and records management in understanding which records are truly personal and subject to data protection.

Literature on Privacy and Data Protection

There is a substantial amount of literature on privacy and data protection available in the form of books, magazine articles, case law, newspaper articles, journal articles, pamphlets, information brochures and web-pages. As the concerns for privacy intensify, conference papers are being written for annual conferences on privacy and data protection such as the Conference and Data Protection Intensives of the International Association for Privacy Professionals, the Computer Privacy and Data Protection Conference, the Privacy Law Conference, the International Conference of Data Protection & Privacy, the Data Protection & Privacy Commissioner's Conference and more.

This trend is expected to steadily increase as the use of technology to create, manipulate and store records and information in all aspects of human activity rises. Professionals across sectors are concerned with the threat posed to privacy by the globalised, automated environment and are embarking on research to assess how this would impact on their various professions. The globalisation of businesses and organisation in the 21st century has augmented issues of 'adequacy' and standardisation in the regulation of privacy and generates much debate as to creating 'a level playing field' for all across jurisdictions.

The papers produced as a result of the Sedona Conference International Programme provide insight into recent developments and trends in global law including data privacy. The Sedona Conference was established to allow leading jurists, lawyers, experts and academics to meet and form 'mini-think tanks in the form of working groups to engage in dialogue in order to advance law and legal thinking. The Conference investigates and assesses key issues in law and how they are being dealt with in various jurisdictions. Reports and other publications are produced at the end of each conference. There is also the conferences, seminars and Data Protection 'Intensives' held by the International Association of Privacy Professionals along with its 'daily dashboards' that provide much information on developments in privacy/data protection on a global scale.

Nonetheless, literature on data protection in particular tends to be more descriptive than highly analytical. It has proven to be easier to find information on the various data protection principles, provisions in the Acts, definitions of terms and case law than on finding hypotheses for why data protection models have developed the way they have across jurisdictions. The study hopes to unearth some of main factors that have lead to the unequal development of data protection provisions in select regimes from a records management perspective.

Literature on Records Management and Data Protection

Existing literature on records management as a discipline and data protection as a legal provision has not explicitly or irrefutably made the link between the two pursuits. Small pockets of research have been undertaken but predominately by individuals outside of the records management profession. Some effort has been made by members of ARMA International, a body for records management professionals in North America, to initiate meaningful research and debate in the subject area in recent times. The University of

Dundee's Centre for Archive and Information Studies, as a tertiary level institution offering an MSc Records Management and Information Rights since 2006, has led the way for academic research that will lead to much needed results.

2. CHAPTER 2

BACKGROUND TO THE WEST INDIES

The region of the West Indies, which is the main concern of this study, presents some challenges for the researcher particularly as it relates to the subject under review. In examining the historical, administrative and legal background of the region, it was discovered that it would be difficult to distil the relevant facts from the existing literature. For the purpose of this study, it is critical that some background is provided on the history and development of the region itself. This would help to provide some insight into the political, economic and social context of the region and would assist in understanding the main reasons why implementation of data protection will be challenging for West Indian administrations. The key elements for consideration have never before been brought together into one overarching study. This literature review and other research undertaken as a part of this study provides the basis for developing the right framework for the region as it relates to the successful implementation of data protection and other information management related legislation.

The region referred to as the West Indies is one of the most historically rich, politically complex and socially cosmopolitan regions of the world. The specific area under review in this study is the portion of the West Indies formerly known as the British West Indies or English-speaking Caribbean which is principally identified today as the Caribbean Community (CARICOM).²⁰⁵ The islands of the British West Indies are geographically separated by the Caribbean Sea but historically shared a bilateral bond with Britain. This historical reality has had a lasting impact on all aspects of development of the region. The historiography of the region speaks to its eventful past and therefore provides the

²⁰⁵ See Appendix 5, *List of British West Indies territories vs. CARICOM Territories*, p. 405.

background for understanding the political, social and economic environment in which the implementation of the policy referred to as data protection would need to take place.²⁰⁶

The ultimate goal of this study is to provide recommendations to the West Indies on the implementation and operation of data protection as a public policy from a records and archives management perspective. In this study, it is pertinent to review and understand West Indian law, legal systems and its recordkeeping traditions. The literature would reveal that the area of the West Indies under review was greatly influenced by three main historical events. The first key occurrence was the establishment of the plantation economy and the colonial system; the second was the emancipation of slavery and the rise of the working class and the third was the post-independence period. However, the period that will be the focal point of the study is the post-independence period from the 1960s.

2.1 West Indies History - Early Period (17th – 19th Century)

The Colonial System in Brief

The text *A Short History of the West Indies* by Parry et al provides an overview of the history of the colonial system based on a plantation economy in the islands of the West Indies. Parry et al state that the Dutch started a sugar revolution without even realising it.²⁰⁷ They contend that the plantation economy of the West Indies was a powerful engine of economic and social change. Initially, crops of indigo, tobacco and cotton were the mainstay but it was the sugar cane and the 'insatiable demand' for sugar in Europe that revolutionised the political, social and economic development of the West Indies, and led to a firmly entrenched colonial system.²⁰⁸

²⁰⁶ See Appendix 6, *Timeline of British West Indies History (Post-Emancipation to Post-Independence)*, p. 406.

²⁰⁷ J.H. Parry et al, *A Short History of the West Indies* 4th ed. (Oxford, 1987), p. 60 - 67.

²⁰⁸ Parry et al, (Oxford, 1987), p. 61.

The sugar revolution then spread to other British colonies in the New World including the Carolinas, Virginia and Maryland. This type of plantation system required a large labour force greater than what was required with indigo, tobacco and cotton. Indentured labour mainly from Ireland and Scotland had been the chief source of labour on these plantations in the 1640s. However, with the introduction of the sugar plantation, the Dutch began a steady trade of slaves from West Africa, first with the Portuguese of Brazil and then extending that trade into the West Indies. Consequently, the number of African slaves brought to the West Indies grew exponentially by the early 1700s. Thus, the region of the West Indies stands today as a 'melting pot' of cultures, practices, beliefs and traditions.

By the latter half of the eighteenth century, Parry et al state that 'a triangular trade' had developed between the Gold Coast of Africa, the West Indies and England/Europe. This imperialist, political and trading system resulted in separateness and insularity among the islands and islanders, as each island had a greater connection to their colonial power than to each other. Parry et al argue that the British government introduced a direct Crown colony system in its colonies which was retained for a century without the introduction of any degree of elected representation.²⁰⁹ In the older British West Indian colonies, a representative system of government with elected Houses of Assemblies and elected local governments had been established. In the field of local government, a parochial structure emerged in these colonies. The 'trustees' were referred to as freeholders who were elected for twelve months and had 'power to levy rates for the poor, for the support of the clergy and for the upkeep of roads.'²¹⁰ Hence, the power to make decisions was concentrated in the hands of a few landed and predominately white people throughout this period.

²⁰⁹ Parry et al, (Oxford, 1987), p. 179 - 183.

²¹⁰ Parry et al, (Oxford, 1987), p. 180.

A pattern of government developed in these territories was very much like that of England in miniature. However, Parry argues that the West Indian system remained fixed and rigid. In the West Indies, only a small section of society was free and sought to maintain the status quo in order to maintain a rigid social and economic structure. This rigidly resonated well beyond the period of colonialism and arguably resulted in the slow pace of modernisation of the region.

Interestingly, at this point in history, there was no professional civil service in the West Indies and absenteeism was a main characteristic of government. Parry et al further describes in sufficient detail the variations and patterns of colonial government that evolved throughout the islands of the British West Indies with Barbados being the only island to retain the old representative system, rejecting the idea of a confederation with Windward Islands in 1876. Trinidad and St. Lucia were said to be complete models of Crown colony government along with the island of Jamaica up to 1885. British Guiana maintained elements of an oligarchy based on limited franchise up to 1891. It was thus after the First World War that a local nationalism in the West Indies took root, changing the political landscape towards a establishment of a representative government. This localised nationalism has been seen as one of the main reasons for the failed attempts of the region to unite up until the present. The resultant insularity and inability to unite would have a lasting effect on the region that will be highlighted and discussed in Chapter 5.

The Abolition of Slavery in Brief

In order to understand the second phase of West Indian development, this thesis considers the work of Eric Williams. In his seminal work *Capitalism and Slavery*, Williams agrees with Parry et al with regard to the settlement and development of the British West Indies. However, Williams pays a great deal of attention to the economic benefits derived from

slavery for Britain. The West Indian planter became a familiar figure in British society by the eighteenth century, very rich and absentee. Once they made their fortune in 'the Indies', they returned to a lavish life in Britain.²¹¹ This situation may explain the 'vacuum' that existed in the governance of the islands that has hindered the advancement of the region in line with the developed world.

Williams' most significant contribution to the historiography of the West Indies is his discourse on the reasons behind the abolition of the slave trade and subsequently slavery. Whereas other West Indian historians such as William A. Green acknowledge and highlight the work of the humanitarians and abolitionists of the period, Williams argues that the importance of humanitarians was 'seriously misunderstood and grossly exaggerated' in the destruction of the slave system.' Williams contends that the abolition of the slave trade and later the emancipation of slaves was not driven by 'justice and humanity' but was 'dictated by selfish motive[s].' He states emphatically that the commercial capitalism of the eighteenth century developed the wealth of Europe by means of slavery and monopoly but it was economic changes and 'the rise and development of new interests that [led to] the necessity of the destruction of the old.' Williams further contends that once the West Indies was no longer the hub for economic activity, attention turned away from the region and it was left to rise or fall on its own.²¹² Human rights such as privacy would not have featured strongly in a West Indian society built on slavery.

The planters rebelled against the changes and their arrogant behaviour and language inflamed the minds of the already restless slaves. When the slave trade was abolished in 1807, the slaves misconstrued this to mean that the British Parliament desired their general

²¹¹ Williams, *Capitalism and Slavery*, (Cambridge, 2004), p. 85.

²¹² Williams, (Cambridge, 2004), p. 85.

emancipation and so the slaves all over the West Indies began to rebel and show their displeasure for what was perceived as the planters' disregard for their freedom. Consequently, a number of slave revolts took place across the region in the period of the 1820s. According to Williams, by 1833 the alternatives were clear. 'Emancipation from below or emancipation from above. But EMANCIPATION.'²¹³ But would emancipation bring about any real changes?

Emancipation and the Birth of the Working Class

In examination the third phase of West Indian development, the study considers the theory of O. Nigel Bolland in his study on *Systems of Domination After Slavery: The Control of Land and Labour in the British West Indies After 1838*, discusses the working and living conditions of the ex-slaves in the post-emancipation period. He states that the change in legal status of the slaves did not abolish their struggle.²¹⁴ Bolland contends that the former slaves were no longer defined as 'forced labour' but were still seen as the 'labour force' and the shift from slave labour to wage labour was simply a transition from one system of labour control to another.²¹⁵ The ex-slaves were in no position to acquire the education and skills needed to advance society and were still very much the underclass. Their rights as individuals and citizens were not elucidated or promoted.

Bolland therefore deduces that that full emancipation was not attained in the post-1838 period. He contends that there were 'persistent power structures' which sought to maintain the status quo and so freedom was merely an illusion.²¹⁶ The general situation that prevailed was a submissive labour force, disciplined through law enforcement by police,

²¹³ Williams, (Cambridge, 2004), pp. 178 - 208.

²¹⁴ O. Nigel Bolland, 'Systems of Domination after Slavery: The Control of Land and Labour in the British Caribbean', edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996), p. 108.

²¹⁵ Bolland, (Princeton, 1996) p. 108 - 111.

²¹⁶ Bolland, (Princeton, 1996) p. 118.

magistrates and prisons. Despite being freed, as seen in the Belizean context, the free labourer was 'completely at the mercy of his employer' who remained in a position of dominance in every aspect of society.²¹⁷

The use of personal data by governments and private organisations is a main point of examination in this thesis. Issues of power and domination are therefore examined. As this thesis seeks to analyse the power structures in the region and the relationship between citizen and state, it is also important to understand the reasons for the retarded development of governmental authorities. Roy Augier in his work on post-1838 conditions in the British West Indies, *Before and After 1865*, closely examines the political conditions that arose after emancipation. He states that under crown colony system, the British Government used the political authority it was given, claiming that its presence within society was justified.²¹⁸ In speaking on Jamaica, he contends that they [British] felt only they could 1) tidy up the public service and administration, making them more efficient 2) provide impartial government between conflicting classes and 3) look after the interests of blacks, protecting them from whites and from themselves.²¹⁹

Augier contends that the merits of the British system were that it established a modern state; old departments were made more efficient and new ones were created; rational procedures for the administration of the country's finances were introduced. However, efficiency was attained by concentrating all decision-making power in the hands of the Colonial Secretary. Undoubtedly, a dependency on the British Government arose and was evident as the local Assemblies blamed emancipation and free trade for ruining the economy and did not adequately support the administrative systems after the British

²¹⁷ Bolland, (Princeton, 1996), p. 117.

²¹⁸ Roy Augier, "Before and After 1865" edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996), p. 177.

²¹⁹ Roy Augier, (Princeton, 1996), p. 177 - 179.

Government relinquished control to them. This situation meant that there was little or no accountability in governance. The local people had little say in how their territories were being administered and expectation for protection of their human rights was very low. This factor must be acknowledged when examining the expectations of West Indian citizenry as it relates to their rights even up to the present.

Augier criticises this political arrangement for damaging the society by appointing foreigners as heads of departments long after there had been time to train locals for these posts. The argument that natives were not desirable for the interest of justice was proffered. Hence, paternalism and the elevation of the white skin as the necessary quality for jobs at the top level prevailed as a main characteristic of West Indian society.²²⁰ Augier, speaking in relation to the Jamaican context, claims that the British failed in large measure to be impartial administrators, to protect the interest of the poor and to teach society responsible politics. Frustration over this unequal system and the dominance of the wealthy would manifest itself in the form of riots throughout the region in the 1930s.²²¹ It was also in this period that educated, black West Indians began to agitate for change and sought to rise to positions of leadership to become more involved in steering the direction of the region. However, as will be seen, the more things changed, the more they remained the same.

2.2 The Move towards Independence in the West Indies (1930s – 1960s)

The appeal for independence was gaining momentum by the 1930s and according to Barrow-Giles, it was felt by both the British Government and the West Indian political leaders, that independence was best achieved through a federation.²²² The realisation of

²²⁰ Roy Augier, (Princeton, 1996), p. 179.

²²¹ Roy Augier, (Princeton, 1996), p. 180.

²²² Cynthia Barrow-Giles, *Introduction to Caribbean Politics* (Kingston, 2002), p. 254.

that type of association, however, depended on several variables.²²³ By the late 1940s, it was hoped that the establishment of the Federal Government would bring together all the constituent parts needed to form a viable West Indian Nation.²²⁴

The concept of a federation must be understood in the context of this study where it seeks to understand the best approach to take when developing 'model' requirements for data protection. Barrow-Giles states that a federation is one of three forms of political integration.²²⁵ Federation is a form of political association in which two or more states establishes a common government but each member state retains some measure of domestic autonomy. The main distinguishing mark of a federation is that participating constituent units are not in any way insubordinate to each other and there is a division of power between the central and national governments. In order for these commitments to be respected, they must be fixed in a written constitution, which serves to protect the national governments ensuring that their autonomy is upheld. It is further argued that for a federation to be successful there must be a strong desire for political independence by the society and its political leaders. The support of the political leaders is a crucial factor in fostering a favourable climate in which the federation can be successfully achieved.

G.K. Lewis in his work *The Growth of the Modern West Indies* surmises that, 'West Indian politicians are representative men who reflect, and who must reflect if they wish to survive...'²²⁶ This view is in harmony with the K.C. Wheare's opinion on the factors favourable for the success of a Federation. Wheare states that these factors include:

1. The political will and desire for both civil society and political leadership
2. A desire to be united under a single government for certain purposes

²²³ Barrow-Giles, (Kingston, 2002), p. 254.

²²⁴ Barrow-Giles, (Kingston, 2002), p. 253.

²²⁵ Barrow-Giles, (Kingston, 2002), pp. 224-226.

²²⁶ G.K. Lewis, *The Growth of the Modern West Indies* (Kingston, 2004), p. 392.

3. A desire for political independence
4. A desire and scope for economic gains
5. The need for administrative efficiency, especially where critical mass is in short supply
6. A commonality of political and cultural institutions
7. Geographical proximity and geographical neighbourhood.
8. A sense of military insecurity²²⁷

These objectives are all desirable for regional development and would be facilitated greatly by increased harmonisation and standardisation in all systems of governance. In the initial stages, these desires were there. Sir Shridath Ramphal, a West Indian Federalist and notable international statesman, when speaking of the compulsions of regional engagement in the West Indies, argues that the decade of the 1930s was the final and decisive phase for the federal movement by West Indian leaders.²²⁸ T.A. Marryshow of Grenada and A. Cipriani of Trinidad played leading roles in the push for West Indies Federation. In this period, a host of riots and disturbances took place throughout the region.²²⁹ The case for closer association became stronger and a clamant demand for representative self-government arose. By the end of the 1930s, the call for constitutional changes and political reform grew louder and more insistent in the West Indian territories. Federation, by the 1940s, possessed an appeal as 'a possible alternative to improbable local self-government'.²³⁰ In 1947, a Montego Bay Conference, which was really a meeting of key West Indian politicians, was where the ideas of federation, nationhood and self-government came together.

²²⁷ Kenneth Clinton Wheare, *Federal Government*, 4th ed. (New York, 1964), p. 80.

²²⁸ David Dabydeen and John Gilmore, *No Island is an Island: Selected Speeches of Sir Shridath Ramphal* (London, 2000), pp. 27-38.

²²⁹ David Dabydeen and John Gilmore, pp. 27-38.

²³⁰ Shridath Ramphal, 'Rough Handling Federation' *When '10' May Have Been An Odd Number: Some Perspectives on the West Indies*, Lecture commemorating the 50th Anniversary of The West Indies Federation (2008).

In the post-World War II period in the West Indies, an impressive cadre of 'homegrown' dynamic men and women were rising to the top levels of West Indian politics.²³¹ Some of these individuals were graduates of the 1948 University College of the West Indies (UCWI), a college of the University of London that later became a full-fledged university in its own right in 1962. Many of them had pursued graduate studies at some of the best universities and colleges in the world. They had returned to the West Indies with strength, confidence and determination to take the region into a new era of political, economic, social and cultural advancement. It is with this drive and energy that this cadre appeared at first to embrace the idea of political independence and did what was necessary for the region to begin its journey towards this end.²³²

²³¹ Interview of Sir Shridath Ramphal conducted part of an Oral History Project of the West Indies Federal Archives Centre entitled "Remembering the West Indies Federation" in (Bridgetown, 2006).

²³² Interview with Sir Shridath Ramphal, 2006.

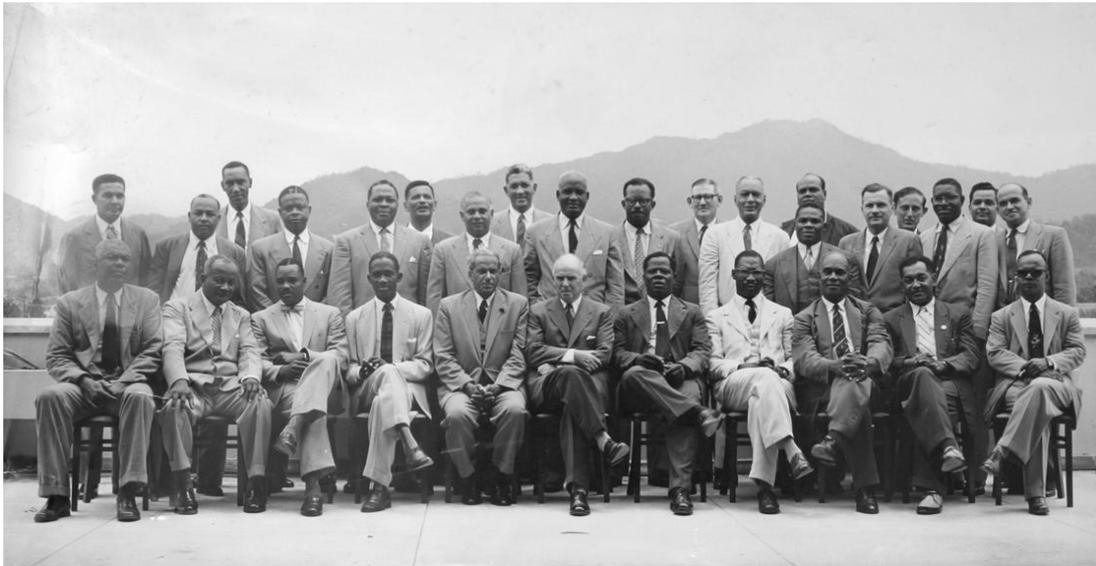
The Lancaster House Agreements: The London Delegations

Image 3 Photograph of London Delegation in 1953 compliments W.I. Federal Archives Centre

The delegations to London in the 1950s included stalwart West Indian politicians such as Sir Grantley Adams (Barbados), Mr. Norman Manley (Jamaica), Dr. Eric Williams (Trinidad & Tobago), Mr. V.C. Bird (Antigua), Mr. Robert Bradshaw (St. Kitts), Mr. T. Albert Marryshow (Grenada), Mr. William Bramble (Montserrat), Mr. Carl LaCorbiniere (St. Lucia), Mr. Franklyn Baron (Dominica), Mr. E.T. Joshua (St. Vincent) and Sir Shridath Ramphal (Observer - British Guiana) among others.²³³ These men acted as chief negotiators on behalf of the West Indian region in the federal negotiations with the Colonial Office. Two decisive conferences took place at Lancaster House in London, in 1953 and 1956 respectively, which were intended to settle all outstanding federal issues. It was at the 1956 conference that some measure of finality was brought to the federal negotiations. On 23 February 1956, representatives of ten territories (along with observers from British Guiana and British Honduras) met at Lancaster House to sign an agreement to form a federation of ten British West Indian territories namely, Jamaica, Antigua, Barbados, Trinidad and Tobago, Grenada, Montserrat,

²³³ Photograph digitised from the Federal Information Service Photographic Collection at W.I. Federal Archives Centre, The University of the West Indies, Cave Hill Campus, Barbados.

St. Christopher/Nevis/Anguilla, Dominica, St. Lucia and St. Vincent. Further to this, the British Caribbean Federation Act of 1956 provided for the establishment of a West Indies Federation.²³⁴

However, the experiment of federation in the West Indies would be challenged on a number of levels. Elizabeth Wallace and other notable historians in their 'post-mortem' studies on the failure of the Federation suggest that one of the main reasons for the rapid decline of the West Indies Federation was politics. West Indians politicians of that period were described in the literature as men of 'unquestionable ability' but were accused of having possessed 'political ambitions still rooted in insularity'.²³⁵ In June to September 1961, Sir Alexander Bustamante began a referendum campaign that drove anti-federal sentiments across the island of Jamaica.²³⁶ As a result, Jamaicans began to develop intense nationalistic feelings and their own concept of nationhood. Mr. Norman Manley, Premier of Jamaica and major supporter of the Federation sought to counter these sentiments arguing that a vote against federation would be 'a breach of faith deserving worldwide contempt'. Yet, in the end, the vote was 54.1% against The West Indies Federation and 45.9% in favour. The passing of the Jamaica referendum was thus the first step towards the end of the first federal experiment.²³⁷ Unfortunately, other attempts at regionalism since this period have been weak and the region continues to grapple with issue such as under-development and disparity in many areas. How this legacy impacts on the region's competitiveness today and what influence would this have on the successful implementation of data protection will be a topic of discussion in Chapter 5.

²³⁴ File **FWI-FS-IS-7&8**, *Federal Information Service Press Releases* (1957).

²³⁵ Elizabeth Wallace, 'The Break-up of the West Indies Federation' in *Caribbean Freedom: Economy and Society from Emancipation* ed. to the Present (London, 1993), p. 470.

²³⁶ Wallace, (London, 1993), p. 455.

²³⁷ Wallace, (London, 1993), p. 457.

2.3 Post-Federal Attempts at Regional Integration

A subsequent attempt was made to form a smaller federation of islands at a conference held in Barbados in March 1962.²³⁸ This conference was attended by representatives from Antigua, Barbados, Dominica, Grenada, Montserrat, St. Kitts-Nevis-Anguilla, St. Lucia and St. Vincent. The principal aim of the conference was to discuss the possibility of the closer association of these territories into federation that would be referred to as 'Little Eight'. Evidence was provided at the conference to convince the British Government that this federation would be viable and another conference was held in London in May to further discuss the details. A Regional Council of Ministers was subsequently established and a call for further research into the financial matters of the islands was made. However, there was reluctance by the British Government to support this federation's proposed independence and after more meetings in 1963 and 1964; there was a breakdown in talks. By 1965, this proposed federation ended before it really began.

The West Indian Federation and the attempts at a 'Little Eight' federation, although deemed failures, did leave a legacy of regional co-operation that would serve the region well in the years to come.²³⁹ In December 1965, a preliminary agreement for a Caribbean Free Trade Association was signed and a final agreement reached in May 1968 by a Treaty of Antigua.²⁴⁰ The early signatories to this agreement were Antigua, Barbados, Guyana and Trinidad. In the three months that followed, they were joined by St. Vincent, St. Lucia, Dominica, Grenada, St. Kitts-Nevis-Anguilla and finally Jamaica and Montserrat. British Honduras joined in 1971 to make twelve members in what would be called the Caribbean Free Trade Association (CARIFTA).²⁴¹

²³⁸ Anthony Payne, *The Political History of CARICOM* (Jamaica, 2008), pp. 67-87.

²³⁹ Interview with Sir Shridath Ramphal, 2006.

²⁴⁰ Payne, (Jamaica, 2008), pp. 67-87.

²⁴¹ Payne, (Jamaica, 2008), pp. 67-87.

The aim of this association, very similar to that of the current European Union, was to foster the economic development of its individual members, by increasing trade and encouraging the diversification of products. It was intended that all custom duties would be removed between the member countries in a hope to stimulate the movement of goods. The ultimate goal was to create a common market that would, for all intents and purposes, bring full employment and improve the standard of living throughout the region. Hence, just as with the European Union, harmonisation of the region's structure, laws and practices would be desirable.

CARIFTA was organised into:

- a) a Heads of Government Conference to outline general policy;
- b) a Council of Ministers which would translate the general policy into specified schemes when the need arose;
- c) A Commonwealth Regional Secretariat which would be a permanent body based in Georgetown, Guyana. The aim of this Secretariat was to keep the association together and organise the trade and development schemes that the Ministers decided upon.²⁴²

A constitution was written that allowed new members to join by applying to the Council of Ministers.²⁴³ The role of CARICOM in implementing data protection on a regional basis will need to be examined and discussed as a part of this study.

CARIFTA faced some challenges at first with the removal of the customs duties. A period of adjustment had to be given for territories. In 1968, less than ten percent of the members were trading with each other. After five years, however, the flow of goods between members began to increase and by 1974, the members were ready and anxious to take a bolder step.

²⁴² Payne, (Jamaica, 2008), pp.67-87.

²⁴³ Payne, (Jamaica, 2008), pp. 67-87.

W. Andrew Axline in his study, *From CARIFTA to CARICOM: Deepening Caribbean Integration* states the CARIFTA Heads of Government realised that they were at a crucial stage in the development of Caribbean integration. A compromise was reached to establish the Caribbean Common Market and Community. This was embodied in the Georgetown Accord signed on 12 April 1973. Ten of the twelve CARIFTA members signed the Georgetown Accord, with Montserrat and Antigua not joining because they were not convinced that it would be beneficial to them.²⁴⁴ Axline states that after several concessions Antigua and Montserrat joined CARICOM and signed the Treaty of Chaguaramas in 1974. Axline contends that the countries of the Commonwealth Caribbean succeeded in advancing the integration process with the goal of the economic development of the region.

There have been attempts to unite the region to create a political association similar to that of the European Union, the United States of America, Canada and Australia.²⁴⁵ Although there is common ground in the history, culture and language of the territories, a peculiar localised development has developed in each individual territory caused by imbalances in the economic, political and social conditions that would impact on their constitutional, legal and administrative landscapes.²⁴⁶ Some West Indians hold firm to the view that integration is a means of rising above the main challenges that face the region including geographic separation, parochialism and insularity, disparities in size, resources and economies and poor communication.²⁴⁷ Thus, in the post-1930s period, Federation was seen, for all intents and purposes, as the path or road to political independence. It was the British Government

²⁴⁴ Andrew Axline, 'CARIFTA to CARICOM: Deepening Caribbean Integration', edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996), p. 483.

²⁴⁵ Barrow-Giles, (Kingston, 2002), p. 265.

²⁴⁶ Based on interview conducted in March 2010 with Jamaican-born legal scholar at The University of the West Indies.

²⁴⁷ Based on oral history interview on The West Indies Federation with Sir Fred Phillips in 2009.

that first advocated the federating of the West Indies as ‘the shortest path to independence’.²⁴⁸

However, CARICOM was the first formation of its kind in the region because it did not focus on political and administrative integration as with previous attempts but rather sought to provide a regional approach towards dealing with the problems of economic stabilisation and development. There was a need for closer collaboration, economic integration and foreign and external trade policy coordination and so the Georgetown Accord signed on 12th April 1973, provided for the signing of the Treaty of Chaguaramas signed on 4th July 1973 that established CARICOM.²⁴⁹

However, the intent to harmonise key regional activities is relevant to this paper on the implementation of data protection. This is the key basis for the argument of taking an integrated approach to data protection regulation. In Article 4 of the *Treaty of Chaguaramas*, the objectives of the Caribbean Community are clearly set out. It states,

‘The Community shall have as its objectives:-

The economic integration of the Member States by the establishment of a common market regime (hereinafter referred to as “the Common Market”) in accordance with the provisions of the Annex to this Treaty with the following aims:-

- i. the strengthening, coordination and regulation of the economic and trade relations among Member States in order to promote their accelerated harmonious and balanced development;
- ii. the sustained expansion and continuing integration of economic activities, the benefits of which shall be equitably shared taking into account the need to provide special opportunities of the Less Developed Countries [LDCs];

²⁴⁸ Based on oral history interview on The West Indies Federation with Sir Shridath Ramphal in 2009.

²⁴⁹ Barrow-Giles, p. 227.

- iii. the achievement of a greater measure of economic independence and effectiveness of its Member States in dealing with States; groups of states and entities of whatever description;
 - a) the coordination of the foreign policies of Member States; and
 - b) functional cooperation, including—
 - the efficient operation of certain common services and activities for the benefit of its peoples;
 - the promotion of greater understanding among its peoples and the advancement of their social, cultural and technological development; and
 - activities in the fields specified in the Schedule and referred to in Article 18 of this Treaty.²⁵⁰

It is clear from the stated objectives that information would need to be shared between the territories. This would include the sharing of personal information of the citizens of the region to operate common services and activities, promote greater understanding among the people and regulate trade.

The CARICOM Single Market & Economy (CSME) of 2001 is the most recent initiative that is intended to be a forerunner for political integration. The main objectives of the CSME are full use of labour (full employment) and full exploitation of the other factors of production (natural resources and capital); competitive production leading to greater variety and quantity of products and services to trade with other countries. It is expected that these objectives will in turn provide improved standards of living and work and sustained economic development. Key elements of the Single Market and Economy include:

- *“Free movement of goods and services* - through measures such as eliminating all barriers to intra-regional movement and harmonising standards to ensure acceptability of goods and services traded;
- *Right of Establishment* - to permit the establishment of CARICOM owned businesses in any Member State without restrictions;

²⁵⁰ CARICOM, *Treaty Establishing the Caribbean Community* found at www.caricom.org. Accessed on 14 January 2011.

- *A Common External Tariff* - a rate of duty applied by all Members of the Market to a product imported from a country which is not a member of the market;
- *Free circulation* - free movement of goods imported from extra regional sources which would require collection of taxes at first point of entry into the Region and the provision for sharing of collected customs revenue;
- *Free movement of Capital* - through measures such as eliminating foreign exchange controls, convertibility of currencies (or a common currency) and integrated capital market, such as a regional stock exchange;
- *A Common trade policy* - agreement among the members on matters related to internal and international trade and a coordinated external trade policy negotiated on a joint basis;
- *Free movement of labour* - through measures such as removing all obstacles to intra-regional movement of skills, labour and travel, harmonising social services (education, health, etc.), providing for the transfer of social security benefits and establishing common standards and measures for accreditation and equivalency.

Other measures:

- *Harmonisation of Laws* - such as the harmonisation of company, intellectual property and other laws.²⁵¹

There are three objectives here that are very relevant to supporting a regional approach to data protection: 1) the 'movement of goods and services' 2) 'freedom of labour' and 3) 'harmonisation of laws' measure provides sound justification for a regional approach to data protection because in the first phase of its implementation, the free movement of skilled people is being addressed.

The movement of goods and services would involve the exchange of personal information across borders within the single economic space. It would also have implications for electronic commerce done via the Internet using personal data related to credit card purchases. Undoubtedly, harmonisation throughout the CSME space of data protection legislation would augur well for trade and the exchange of tangible and intangible services.

²⁵¹ CARICOM Community Secretariat, *Caribbean Single Market and Economy* found at www.caricom.org/jsp/single_market/single_market_index.jsp?menu=csme. Accessed on 14 January 2011.

The movement of persons from nation to nation would involve the exchange of personal information including travel documents, relevant academic qualifications and job experience as well as any criminal/police records on that individual. Technology would be tremendously useful in this regard. A proper, well-functioning and secure database would be required to collect and store the vast amounts of personal data that is involved.

2.4 West Indian Recordkeeping in Brief

The challenges experienced in the region with integration are directly a result of its colonial past with the term 'insularity' and 'dependency' being used repeatedly throughout the literature. This would also be reflected in another key aspect of administration at all levels in West Indian society. The situation with the region's recordkeeping has to be considered in this study in context of its historical development. However, there is not much documented on the recordkeeping systems that were established for the 'management' of records and information in the region. There was only one major Archives Conference in 1965 which was driven by Caribbean historians under the auspices of the History Department of The University of the West Indies to discuss the dire situation with recordkeeping and the provisions for archives.²⁵² This is the only existing document to date that outlines the main challenges and although now dated, many of the challenges presented in the papers of that Conference still exist today.

The tradition that has developed in the West Indian as it relates to the recordkeeping is derived mainly from the British recordkeeping tradition. This resulted from the very strong ties that developed with Britain in the colonial period evidenced in the previous section. Jeannette Bastian best describes the recordkeeping situation in the West Indian region in

²⁵² The University of the West Indies, *Report of the Caribbean Archives Conference held at The University of the West Indies, Mona, Jamaica September 20-27, 1965.*

her work, *Reading Colonial Records through Archival Lens: The Provenance of Space, Place and Creation*. She discusses the records themselves and contends that they reflect the exploits and conquest of the coloniser and a second class status adheres to the history of the colonised. She argues that the voices, that is, views, opinions and experiences of the colonised are not reflected in the records. This essentially can be interpreted to mean that the records are not a complete representation of what occurred. She further states that there are many weaknesses in post-colonial recordkeeping systems. The weaknesses will be more closely examined in Chapter 6.

There are issues with the custody of records in the colonial period that may have led to a further weakening of the West Indian recordkeeping system. The *provenance*²⁵³ of the records would have been that of the coloniser and upon leaving at independence many records did not remain in the physical custody of the newly independent territories and even today can be found in repositories across Britain. In addition, the British imposed the 'Grigg system' on the colonial records which meant that some records that would have been the key evidence of activities in the territories were 'weeded out' or purged by them before the close of the colonial system. Hence, in some cases, major gaps were created within the recordkeeping system.²⁵⁴

Another area of weakness that would impact on the implementation of data protection as it relates to records management is the lack of skilled personnel to manage records in the region up to the present. This is in agreement with Augier's assessment that when the foreign interests 'pulled out' of the region those who designed and implemented the

²⁵³ The term 'provenance' used in archival studies refers to the acknowledgement of the true creator/owner of the records. This would have implications for how the records are arranged, maintained, appraised and interpreted.

²⁵⁴ The National Archives (TNA), *Appraisal Policy – Background Paper: 'The Grigg System' and Beyond* found at www.nationalarchives.gov.uk/documents/information-management/background_appraisal.pdf. Accessed on 23 January 2013.

administrative systems that were in place took the skills and knowledge needed to continue the operation of these systems in an efficient and effective way. To date, there still remains a dearth of trained archivists and records managers in the region. Postgraduate studies are required for those working with records and information to properly manage records and information throughout their lifecycle. Currently that training has to be obtained overseas as there are not any postgraduate programmes available at regional tertiary institutions. An unpublished study by the Caribbean Branch of the International Council on Archives (CARBICA) undertaken in the 1990s revealed that this was also coupled with the lack of strong archival legislation throughout a large percentage of the territories. The implications of this will be discussed when looking at recommendations for the West Indies going forward.

2.5 The West Indies: Law and Legal Systems

Albert Fiadjoe in his work, *Commonwealth Caribbean Public Law*, presents a comprehensive overview of public law in the English-speaking Commonwealth Caribbean. He defines public law broadly as,

All law dealing with relations between an individual and the state or between states and the organisation of government, i.e. criminal, administrative, constitutional and international law.²⁵⁵

This branch of law is particularly relevant to the study of data protection and its relationship to records management because of the focus between the relations between an individual citizen and organisations including governments. Fiadjoe provides the context in which public law in the region developed.

²⁵⁵ Albert Fiadjoe, Commonwealth Caribbean Law Series, *Commonwealth Caribbean: Public Law* 3rd ed. (New York, 2008), p. 3.

Fiadjoe contends that certain historical factors greatly influenced how public law developed.²⁵⁶ He argues the Caribbean, just like England, was principally motivated by intense social legislation after the two World Wars. He argues that it was the period after World War II when ideas about human rights, democracy and freedom became prevalent. He also states that there was the growth of a welfare-based society in the Caribbean which led to a great increase in the exercise of administrative powers by the state. Fiadjoe also posits that the development of public law was inextricably linked with the general colonial law and UK law was applied throughout the English-speaking region. However, there is evidence that a peculiar, localised development of law has taken place throughout the territories. Fiadjoe identified three stages of development in law in the region. The first stage was as a result of the *Moyne Commission Report*. The Moyne Commission was established under the chairmanship of Baron Moyne and its stated objective was 'to investigate social and economic conditions in Barbados, British Guiana, British Honduras, Jamaica, the Leeward Islands, Trinidad and Tobago and the Windward Islands'. The report totalling 483 pages sets out wide-ranging recommendations touching on several matters of public concern including social and political advancement. Fiadjoe identifies the second phase as the 1950s period fight for political independence from Britain. He states that this period saw the establishment of various administrative bodies dealing with matters such as agriculture, industries, tourism and housing. The third phase identified by Fiadjoe was the period of the 1960s when the territories gained independence. New challenges would arise for the region as a result of independence.

Independence came with new constitutions which guaranteed fundamental human rights and provided a secure foundation for establishing Caribbean public law. Fiadjoe states that

²⁵⁶ Fiadjoe, (New York, 2008), p. 4 - 5.

public law in the Caribbean is raising a number of fundamental issues about the role and effectiveness of law as a tool of public administration and the basic commitment of government to the rule of law.²⁵⁷ One of the most acute challenges as identified by Fiadjoe is the need for means to control the rational exercise of discretion and also to provide an efficient scheme of legal remedies to rein in the abuse of power by public bodies and officials. Fiadjoe contends that the principles of natural justice are embedded in Caribbean constitutions and the way has been paved for the constitutional protection of the citizenry against state power.

In briefly examining West Indian law and legal systems, it is useful to consider the writings of Rose-Marie Belle Antoine in her study of Law and Legal Systems in the Commonwealth Caribbean. She is in agreement with Fiadjoe that the Caribbean territories 'borrowed heavily from international human rights instruments when drafting their Constitutions.'²⁵⁸ She contends that the region's law and legal systems are still striving to be West Indian and speaks of the dominance of English common law.²⁵⁹ Antoine states that most of the countries in the Commonwealth Caribbean have, in the main, retained the ideals of the English common law tradition. However, the region has to a limited extent, deviated from some of the fundamental principles through its embrace of written Constitutions and its favour of constitutional supremacy.²⁶⁰

In examining the sources of law in the Commonwealth Caribbean, Antoine states that the law is derived from a) the Constitution b) legislation c) the common law and judicial precedent d) custom e) international law including the law of regional treaties and f)

²⁵⁷ Fiadjoe, (New York, 2008), p. 5.

²⁵⁸ Rose-Marie Bell Antoine, *Commonwealth Caribbean: Law and Legal Systems* 2nd ed. (New York, 2008), p. 5.

²⁵⁹ Antoine, (New York, 2008), p. 5.

²⁶⁰ Antoine, (New York, 2008), p. 55.

equity.²⁶¹ She contends that of the six, international law is not a traditional source but it has increasingly become important as a means of affording the region validity and authority in particular in relation to labour law and the law of human rights. She states that the two most important human rights bodies impacting on the region are the European Court of Human Rights (European Court) and the United Nations Human Rights Committee (UNHRC). The Commonwealth Caribbean has been influenced by this jurisprudence and has allowed it to filter through to its law.²⁶² Antoine also discusses the legal obligations and influences that arise from regional treaties and agreements; the two most significant treaties being the CARICOM Treaty and the Inter-American Convention on Human Rights. There are also the treaties of the Organisation of Eastern Caribbean States (OECS) sub-regional grouping, performing a similar function as the CARICOM for the Eastern Caribbean territories.²⁶³ These arguments are important to consider in understanding the changing global context in which the region is influenced by where there are new expectations regarding the legal parameters in which a civil society should operate in light of human rights.

To fully understand the region's legal traditions, this study considered the work of Sir Fred Phillips on *Commonwealth Caribbean Constitutional Law*, where he examines the sources of Caribbean Constitutional Law and the nine key fundamental rights and freedoms addressed by Constitutions in the region. These rights are:

- A. freedom of association
- B. equality before the law
- C. the right to personal liberty
- D. the right to life
- E. the right to protection from deprivation of property

²⁶¹ Antoine, (New York, 2008), p. 96.

²⁶² Antoine, (New York, 2008), p. 207.

²⁶³ Antoine, (New York, 2008), p. 214.

- F. the right to retain and instruct a legal adviser
- G. protection from inhuman and degrading punishment
- H. the right to freedom of movement
- I. the right to freedom of expression²⁶⁴

According to Sir Fred Phillips, these fundamental rights and freedoms have formed an integral part of the independence constitutions of the former British colonies in the region.²⁶⁵

In view of this legal background, it appears that data protection as a public policy could naturally fit into the ethos of modern Caribbean law as a human right. The constitutional climate for this legal provision now exists. However, other societal variables resulting from the region's historical, political and social development as former colonies and the resultant dependency on the colonial system as well as its persistent failures in integrationist and collaborative initiatives would need to be seriously addressed when offering 'model' requirements or a framework for the implementation of data protection and will be fully explored in Chapter 5.

2.6 Current Status of Data Protection Legislation vis-à-vis Records Management in the West Indies

The section explores that current status of data protection/privacy legislation in the West Indies and how it relates to the provisions for records management which is usually dealt with as part of Archives legislation.

²⁶⁴ Fred Phillips, *Commonwealth Caribbean Constitutional Law* (London, 2002), p. 38.

²⁶⁵ Phillips, (London, 2002), p. 37.

In assessing the current status of Personal Data Protection (PDP) in CARIFORUM States,²⁶⁶ important evidence was gathered in preliminary research done in 2010 as part of the CARIFORUM-EU Economic Partnership Agreement (EPA)²⁶⁷ which revealed that:

- i. Trinidad and Tobago has foreshadowed Personal Data Protection in its national policy dated December 2005 to establish a comprehensive Data Protection regime based on the European Model.
- ii. Barbados has provided a mechanism in its Electronic Transactions Act (2001) for businesses to voluntarily self-certify, through a registration process.²⁶⁸
- iii. Guyana has proposed to permit its Minister to make regulations dealing with Personal Data Protection in its draft E-Commerce Bill.
- iv. St. Kitts and Nevis are making preparations to develop Data Protection legislation.²⁶⁹

Preliminary research also revealed that the CARIFORUM presently has a ‘relatively nascent’ PDP regime or none at all.²⁷⁰ As suppliers of services and goods worldwide, information on people would need to be gathered, stored and processed in the global marketplace. In this competitive arena, abuses of personal data can take place particularly with the engagement of technologies. As it stands, CARIFORUM States are not able to take full advantage of opportunities for diversification into the information-based industries and services that collect, process and/or transfer personal data and this has hindered economic development.²⁷¹ This assessment is supported by the following table produced by the author, which provides evidence of the current status of data protection legislation and archival legislation in the region. Some early conclusions are reached and discussed in relation to this study.

²⁶⁶ CARIFORUM has approximately forty Member States in Africa, Caribbean and the Pacific region.

²⁶⁷ See CARIFORUM-EU, Economic Partnership Agreement, Chapter 6, Title II, Protection of Personal Data, p. 409.

²⁶⁸ Barbados has provided for the Minister with responsibility for International Business to make regulations prescribing for standards for the processing of personal data whether or not it originates in Barbados at www.pwcglobal.com/br/eng/ins-sol/articles/e-commerce1.html.

²⁶⁹ CARIFORUM, *Project Proposal* to assist CARIFORUM with meeting its obligations under the Personal Data Protection chapter of the EPA (April, 2010). The link to this document is no longer accessible.

²⁷⁰ No further research results have been revealed or information given as to how this data was used.

²⁷¹ CARIFORUM, *Project Proposal* to assist CARIFORUM with meeting its obligations under the Personal Data Protection chapter of the EPA (April, 2010). The link to this document is no longer accessible.

Table 1 Current Status of Archives Legislation vs. Data Protection/Privacy Legislation in British West Indian Territories

W.I. Territories	Archives Legislation	Data Protection/ Privacy Legislation
1. Antigua and Barbuda	Yes (1983)	Bill (2013)
2. Barbados	Yes (2001)	Bill (2005)
3. Belize	Yes (2000)	No
4. Dominica	No	Bill (2007)
5. Grenada	No	Bill (2012)
6. Guyana	Yes (1982)	No
7. Jamaica	Yes (1983)	Bill (2012)
8. Montserrat (British Overseas Territory)	No	No
9. St. Kitts & Nevis	Yes (2002)	Bill (2012)
10. St. Lucia	No	Bill (2011)
11. St. Vincent and the Grenadines	No	No
12. Trinidad and Tobago	No	Yes (2011)

The table shows that data protection started emerging in the West Indian territories under review from 2005 and the first Data Protection Act was enacted in 2011. The data suggests that the West Indies region is still in the embryonic stages as it relates to establishing a data protection regime. This study explores the main obstacles that result in the slow enactment of data protection legislation in the region. However, what is evident in this table is that only half of the territories under review have enacted Archives Acts to properly address the management of public records and information. Additionally, Trinidad and Tobago, the sole territory with a Data Protection Act, does not have Archives legislation and the enforcement of the legislation in this territory has been sluggish. The Government Archivist of Trinidad and Tobago, Ms. Avril Belfon states, 'to my knowledge, this piece of legislation [data protection] has so far had little effect on the activities of the National Archives and record

keeping across the Public Service'. She has expressed her concern for the absence of Archives legislation in the face of Data Protection legislation. Ms. Belfon's comments submitted to the Trinidad and Tobago Government are very clear and reflect her disappointment with the manner in which the role of the National Archives is undermined.²⁷² The reasons for this reality are explored in Chapter 6.²⁷³

This position support a key argument being developed in this study that data protection cannot work effectively if the records management environment is not sound. Another point to note in the table is that the existing Archives Acts are indeed out-dated and therefore cannot adequately address issues in the current digital environment. The most current Archives legislation is that of St. Kitts and Nevis' Archives Act of 2002. This is however more than ten years old and many devices, trends and changes to data collection, distribution and storage have taken place since that time. At this point, the territories would require an overhaul of their Archives legislation which includes provisions for records management before any attempt could be made to successfully implement data protection in a stable environment. This discussion is further developed in the recommendations to the West Indies at the end of this study.

Another important piece of evidence about the status of data protection in the West Indies is that some of the Bills, for example one in 2005 and one in 2007, have not progressed to full enactment even though a long period of time has passed. This suggests that there are some factors in these societies that are retarding progression. This study examines the main obstacles to the implementation of data protection in Chapter 6.

²⁷² See Appendix 3 for comments from the Government Archivist of Trinidad and Tobago, p.412.

²⁷³ See Chapter 6, p. 312.

2.7 The International Cricket Council (ICC) World Cup of 2007: A Regional Effort at Effective Personal Data Management

The possibility for regional cooperation does exist as it relates to personal data management. In 2007, the ICC World Cup which was the most significant cricket tournament to be held in the region to date took place between the months of March to April. In preparation for this tournament, a number of critical issues concerning the free movement of people as well as security had to be addressed. A coordinated approach was taken for the first time across the region since the demise of the West Indies Federation (1958-1962) to deal with these matters. The tournament was scheduled to take place in the islands of Antigua and Barbuda, Barbados, Grenada, Guyana, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines and Trinidad and Tobago. The Heads of Government of CARICOM were charged with coordinating the logistical aspects of the tournament in keeping with standards of the International Cricket Council.²⁷⁴ Towards this end, there was the establishment of a 'Single Domestic Space' that was implemented to ensure that all the security mechanisms needed were in place for the movement of persons from within the region as well as the thousands of visitors to the region.²⁷⁵

The provisions made under this arrangement are very relevant to the study of the data protection because of the vast amounts of personal data which had to be processed within this Single Domestic Space. The passports of all travellers to the Caribbean for the World Cup had to be checked against an international database to ensure that they were not fraudulent or stolen documents. The region was the first place in the world to put this system into operation. INTERPOL reported that among the ten territories involved in the

²⁷⁴ Cricket World Cup 2007, *Cricket World Cup Schedule* found at www.travour.com/icc-cricket-world-cup-2007-west-indies/schedule-for-cricket-world-cup.html.

²⁷⁵ CARICOM Community Secretariat, *Statement by H.E. Edwin Carrington on the Occasion of the Inauguration of the CARICOM Single Domestic Space* (1 February 2007), found at www.caricom.org/jsp/pressreleases/pres26_07.jsp.

World Cup one hundred and twenty-nine thousand passport checks were run between January and the first half of February and a total of forty-one passports were stolen or lost passports.²⁷⁶

Immigration officials from the territories were deployed to their countries respective High Commissions or Embassies to issue CARICOM Special Visas²⁷⁷ to persons intended to visit the islands where matches were played in an attempt to collect personal data for the international database administered by INTERPOL.²⁷⁸ The tournament took place incident-free and the major stakeholders were lauded for the high-level of security that existed. However, CARICOM Chairman and Prime Minister of St. Vincent and the Grenadines felt that the Single Domestic Space would not survive beyond the tournament and this prediction proved to be true as the region reverted to the disjointed arrangements that existed before ICC World Cup 2007.²⁷⁹

This study views this initiative as a sterling example of regional cooperation that could have been a pilot for the implementation of data protection measures. This thesis asserts that the World Cup 2007 tournament could have been the platform for the harmonisation of data protection throughout the territories. Governmental agencies could have tested and enacted data protection as it related to transport, travel and commerce in the first instance. Technology deployed through a Wide Area Network (WAN) would have facilitated the seamless transmission of relevant personal information from territory to territory. Data on West Indians would be collected, exchanged and stored in keeping with data protection principles resulting in easier and less bureaucratic entry of CARICOM citizens from island to

²⁷⁶ INTERPOL, *Caribbean officials visit INTERPOL to Plan for Cricket World Cup* found at www.interpol.int.

²⁷⁷ See Appendix 10 CARICOM Community Secretariat, CARICOM Special Visa found at www.caricom.org/jsp/pressreleases/pres26_07.jsp, p . 413.

²⁷⁸ Cricket World Cup 2007, *Cricket World Cup Schedule* found at www.travour.com/icc-cricket-world-cup-2007-west-indies/schedule-for-cricket-world-cup.html.

²⁷⁹ Starboek News (Georgetown, 2007) found at landofsixpeoples.com.

island. This too would lend itself to facilitating the free movement of people promoting regional tourism and enhanced job recruitment. The regulation of data protection taking a regional approach would have taken place in a meaningful way.



Image 4 ICC Cricket World Cup 2007 Logo²⁸⁰
www.cricketstar.net/cca/images/ICC%20quarterly_12%202005.pdf

CONCLUSION

Many of the requirements involved in regulating data protection are dependent on the existence of sound administrative systems with efficient recordkeeping and so any weaknesses in these areas would have implications for successful implementation of data protection. Hence, the fact that the region still grapples with problems in its public and private administrative structures have to be dealt with in this study.²⁸¹ The study therefore investigates whether the background of the West Indies would influence how privacy/data protection is being interpreted and enforced.

Other pertinent research questions when considering recommendations for the West Indies are: What main elements could be extrapolated from the selected data protection jurisdictions that would best suited to the West Indies?; What are the main factors that could hinder successful implementation in the West Indies? Why should the West Indies even be concerned with records management as a profession and data protection as a

²⁸⁰ Image taken from the website CricketStar which offers a statistical management system for cricket leagues.

²⁸¹ Based on experience with regional RIM consultancies and interviews.

public policy? What would be the merits of pursuing data protection regulation collectively? Would implementing data protection strengthen regional development? What future trends in data protection and the digital world should be of concern to the West Indies? The answers to these questions are explored in Chapter 5.

On the archival side, some research has been undertaken by The Society of American Archivists evidenced by presentations prepared for their annual conference and the text *Privacy & Confidential Perspectives: Archivists & Archival Records* edited by Menzi L. Behrnd-Klodt and Peter J. Wosh. In addition, papers have been presented at the most recent CITRA Conference of the International Council on Archives that highlight the nexus between archives/records management and data protection. Archivists and records managers are becoming increasingly aware of the impact of these pieces of legislation on their day-to-day practice. Still the archival literature on the subject of privacy, particularly from an international perspective is very sparse. It is therefore hoped that this study on international perspectives on data protection and its relationship to records and archives management will help to fill the void.

Literature on the West Indian Historical Background

The writings on West Indian history have predominantly focused on the settlement of the islands, plantation economy, slavery, abolition of the slave trade, emancipation and the immediate post-emancipation period. There remains much work to be done on the immediate pre-independence and post-independence periods (1960s -) which are the main concerns of this study. The absence of a comprehensive study of the contemporary history of these former British territories presents some challenges when establishing a context for implementing data protection in the region and examining its relationship to records management.

SECTION TWO
MAIN FINDINGS



The charming simplicity
of Australian privacy law

Image 5 www.sangrea.net/free-cartoons/privacy-cartoons.html



Image 6 Propaganda Poster – Big Brother (US, 1984)²⁸²
www.typophile.com/node/82726

²⁸² These images were politically motivated and were intended to make a statement about what was perceived to be the complex nature of present-day privacy regulation in Australia and the perceived threat of the loss of privacy in the US in the 1980s and beyond.

3. CHAPTER 3

INTERNATIONAL PERSPECTIVES ON DATA PROTECTION - FINDINGS

The principal concern that privacy seeks to address, regardless of geographic location, is the protection of the dignity, uniqueness and identity of people at both an individual and collective level. The value of privacy is even further amplified in liberal, democratic societies where there is an attempt to balance the state's requirements for the collection and use of personal data with the citizen's concern for unnecessary intrusion into his or her private affairs i.e. characteristics, decisions and personal information. This study examines selected jurisdictions which can be considered strong examples of 'information-based societies' that fully utilise the available technological advancements for the processing and use of information and recorded information in the form of records. The jurisdictions selected for the investigation are Australia, Canada, New Zealand, the United States of America as well as Germany and the United Kingdom as Member States of the European Union. The approaches developed to deal with privacy/data protection across these countries can provide the basis for understanding the impact of privacy/data protection on modern societies.

Although other jurisdictions could have been reviewed, these ones were selected because they clearly represented four distinct approaches to dealing with data protection/privacy. In the case of the EU, Germany and UK were chosen because the readings suggested that they were very different in their interpretation of the EU Directive even though they operate in the same data protection regime. Additionally, many of today's key advocates for privacy may be found in the selected countries and the earliest conflicts and debates at a public

level also occurred in these jurisdictions.²⁸³ Additionally, most of these countries, with the exception of the United States, have established privacy or data protection agencies with various levels of oversight and regulation of privacy. They have also introduced privacy or data protection legislation as a response to the growing use of technology in the regulation of society. Research into the emergence of data privacy as a policy in these jurisdictions has revealed that their response to the policy problem arose around the same period between the 1960s and 1980s.

Moreover, some of these countries share a similar background as it relates to the development of their recordkeeping traditions. The history and development of their recordkeeping systems are relative or even linked with some being borne out of a shared historical experience. The UK tradition for recordkeeping was spread across the Commonwealth including the region of the West Indies. This situational factor would enable a contextual comparison to be made when examining the emergence of privacy/data protection as a public policy and legislative provision while showing its relationship to records management.

Further to this, these societies have established similar programmes for their citizens which require the same kind of personal data to be collected in the form of records with a prime example being census records. The services offered, include but are not restricted to, financial services, employment services, health services and educational services. They also seek to carry out well functioning criminal justice systems for the proper regulation of society. The main types of records resulting from these services are administrative records, statistical records, criminal records, medical records and educational records. Increasingly, in these societies, technology is being utilised to facilitate every aspect of the collection,

²⁸³ Bennett, (New York, 1992), pp.5-9.

access and storage of information including personal data in an attempt to efficiently and effectively carry out the aforementioned services seamlessly.

Another significant factor for the selection of these jurisdictions relates to their system of governance. Among these six countries are four federal systems and two of them are a part of the European Union which is an economic and political partnership between twenty-eight countries.²⁸⁴ The ultimate goal of the study is to inform the region of the West Indies of the best approaches to the governance of data protection and in doing so, the merits and/or demerits of an integrated approach is investigated. By reviewing the privacy and data protection provisions, policies and practices of these selected territories, some recommendations as to the most suitable approach could be presented to the region of West Indies in dealing with this matter from a records management perspective.

3.1 Privacy/Data Protection ‘Models’

Four distinct models for data protection/privacy are identified among the selected jurisdictions. One of these models is said to be that established by the Europe Union (EU) and subsequently adopted by the United Kingdom, Germany and other EU Member States. This model is referred to as the *comprehensive* model. A variation of this model was said to have been developed in Canada and Australia and is known as the *co-regulatory* model. Other countries did not enact comprehensive legislation and have sought to deal with the issue of privacy with a cross-section of legislation. The principal example of this model can be found in the United States and is known as the *sectoral* model. The final model identified is referred to in existing literature as the *omnibus* model as seen in New Zealand which

²⁸⁴ Europa, *Basic Information* found at europa.eu. Accessed on 24 April 2014.

seeks to deal with Freedom of Information and Data Protection in a single piece of legislation.²⁸⁵

In order to conduct a comparative study of the provisions, policies and practices in managing privacy/data protection, these societies are examined using the same criteria. However, it is not feasible to try to examine every aspect of privacy/data protection in the selected countries. The detailed examination of the provisions of the various pieces of legislation and their accompanying regulations are not reviewed in this study but rather the origins, core principles and mechanisms established as a result of the legislation. The study does not rank the successes or failures of the selected jurisdictions in regulating or enforcing privacy/data protection but rather assesses the usefulness of the approaches in dealing with the main issues to develop model requirements. The study does not closely examine any sanctions for breaching the legislation to determine whether they are adequate in relation to the severity of breach. This would be difficult to judge using the same criteria as the boundaries of privacy shift frequently and its meaning changes even among the jurisdictions selected.

The chapter, however, assesses the impact of privacy/data protection using key sectors as case studies namely, the health sector, the finance sector, the higher education sector and local governmental authorities, in order to understand some of the main issues arising within each jurisdiction at a sectoral level from a records management perspective. These case studies will point to fundamental weaknesses and based on an assessment of reports from the Data Protection/Privacy Commissioners' Offices across the selected jurisdictions, an assessment of whether these cases of breaches are representative will be made.

²⁸⁵ Privacy International, *Privacy and Human Rights: An Overview* found at www.privacyinternational.org. Accessed on 9 February 2009.

The chapter then identifies who the key 'actors' are in regulating, enforcing and managing privacy/data protection. Thereafter, any societal tensions are unearthed that may have arisen among various 'actors' in the quest to implement privacy as a nationwide policy. A clear distinction is made between those sectors which fall under the remit of the public service vis-à-vis those which are dealt with by private interests. Consequently, the probe into these jurisdictions should glean which elements of the 'models' are most feasible for the West Indies and which elements may need to be revisited.

In addition, the points of convergence and divergence across the selected jurisdiction become apparent. References are made to the various infrastructures established for privacy/data protection and the impact of these on overall governance of privacy/data protection. Ultimately, the suitability of these approaches taken deal with privacy/data protection in the countries representing the four 'models' is examined and an evaluation of whether any of these approaches could qualify as model requirements for the West Indies is undertaken.

Selection of Case Studies

The case studies are useful to strengthen and understand the actual challenges that organisations face in dealing with data protection/privacy with their records and information within each jurisdiction. The ones reported in this study are some documented ones that were selected from among several recorded incidences uncovered by the research undertaken across the selected jurisdictions. They were derived from the official websites of Information Commissioners, reports from the International Association of Privacy Professionals and on-line newspapers and illustrate sectors where there are large concentrations of personal data. An examination of the type of information that data

protection legislation protects leads to the conclusion that the legislation will impact on some sectors in a more significant way than others. The sectors with heavy concentrations of personal information and used for the case studies in this Chapter are health, education, criminal justice and the financial sector. The health sector was looked as an important sector across jurisdictions as health information is classified as highly sensitive information. Therefore, the Chapter is broken down by selected jurisdiction and then cover two cases studies for each one with a special focus on the health sector. In addition, it was recognised that all the cases relate to how public and private organisations treat the records and information containing personal data of staff or their clients regardless of sector. In this sense, the choice of specific sector does not make a difference to the privacy problem manifesting itself in these societies and so the cases studies were chosen because they best illustrate the realities of how staff in organisations are coping with and reacting to data protection requirements.

3.2 Data Protection in Germany

Germany may be considered as the birthplace of the term 'data protection'. One of key catalysts for the emergence of data protection in Germany in the late 1960s was the centralisation of population data in public agencies with the accompanying plan to use personal identification numbers (PINs) for citizens. These PINs were to be used in governmental automated processing systems, both for identification and authentication of individual citizens. The systems were designed to facilitate communication, linkages with record-keeping systems towards promoting greater efficiency and accuracy. The Germany Federal Ministry of Interior wanted to introduce a 12-digit PIN for improving registration of local and foreign residents in Germany. This proposal, introduced in 1973, was called the Population Registration Bill (*Bundesmeldesgesetz*). However, because these personal

identifiers were the first of their kind to track an individual's interaction with the government from birth to death, the simultaneous introduction of a data protection bill was seen as necessary to reconcile the enactment of this comprehensive and pervasive PIN system.²⁸⁶

The 'right to privacy' was not a new concept in West Germany. Although there was no equivalent word for 'privacy', there was an area of law based on the 'rights of the personality' (*Personlichkeitsrechte*). Data protection received constitutional protection in Germany in 1983 articulated as 'a right to informational self-determination'. This meant that the individual, not the government, should control what information is kept and used on his or her self.²⁸⁷ This impact of this concept was felt in Germany and beyond. The word 'datenschutz', which literally translates to 'data protection', was coined and became part of the European nomenclature to deal with the emerging problem of protecting personal data held within automated systems by government and private organisations.²⁸⁸

The German (Federal) Data Protection Act of Germany (*Bundesdatenschutzgesetz* or 'BDSG') was passed in 1977.²⁸⁹ A 1969 resolution had demanded general regulation of data processing as soon as possible. The resolution led to in-depth deliberations by an inter-parliamentary working group which was charged with formulating a preliminary plan for the protection of privacy to guard against the misuse and abuse of automatically processed personal data. The matter of data protection in Germany was debated at length and reviewed by several committees with the central issue being that of enforcement.²⁹⁰

²⁸⁶ Bennett, Colin, *Regulating Privacy*, (New York, 1992), pp. 50-53.

²⁸⁷ Data Protection in Europe, *Second Generation* found at www.dataprotection.eu. Accessed on 11 March 2012.

²⁸⁸ Bennett, Colin *Regulating Privacy*, (New York, 1992), p. 77.

²⁸⁹ *Federal Data Protection Act 1994* (Germany - *Bundesdatenschutzgesetz* BDSG) at www.iuscomp.org/gla/statutes/BDSG.htm.

²⁹⁰ Bennett, p. 79.

The BDSG is viewed as an omnibus law that deals with data protection in both the public and the private sector to a lesser degree. There are also sector specific regulations. The BDSG contains provisions which state that personal data can only be collected on individuals if they have given prior consent. It also has provided very specific rules regarding 'sensitive personal data'. Germany refers to 'special classes of person-related data' that contains any of the following information:

'Information on:-

- Race
- Political opinion
- Religious and political affiliation
- Affiliation with a trade union
- Health data
- Sexual orientation²⁹¹

The BDSG stipulates that personal data may only be processed for the purpose for which it has been collected. This is a key principle in German data protection law. It also states that companies may not collect and store personal data arbitrarily for later use and that the individual must be told the purposes for collection. Consent must be given by the individual to use his or her information for a new purpose.²⁹²

The Federal Data Protection Commissioner was instituted as the supervisory authority under the BDSG. The key role of the Commissioner is to ensure that the Act is implemented correctly and to monitor compliance with the Act. The Act grants him or her powers to access information and inspect at any time. The Commissioner also has the right to report any breaches of the Act to higher federal authority and could be requested to give opinions

²⁹¹ *Federal Data Protection Act 1994* (Germany - *Bundesdatenschutzgesetz* BDSG) at www.iuscomp.org/gla/statutes/BDSG.htm.

²⁹² The Sedona Conference Working Group Series, *International Overview of Discovery, Data Privacy & Disclosure Requirements, Germany...* p. 101.

or make recommendations with regard to the law.²⁹³ Penalties for breach of the Act include fines and imprisonment. The Federal Data Protection Commissioner also became responsible for Freedom of Information after the revision of the Freedom of Information Act in 2006.

An office was established since 1999 for the Berlin Commissioner for Data Protection and Freedom of Information who monitors data protection compliance in the state of Berlin in both the public and private sector. Berlin has its own House of Representatives and has set up its own sub-committee to deal with 'Privacy and Freedom of Information'. The Berlin House of Representatives regularly debates the annual reports presented by the Berlin Commissioner of Data Protection and Freedom of Information.²⁹⁴

However, what has been described as the 'lynchpin' of data protection legislation in Germany for public and private entities is that they must have an in-house Data Protection Officer (DPO). The legislation stipulates that larger entities must hire a DPO if they have more than twenty employees that process personal data. The DPO is treated as an employee of the organisation that hires him or her. This individual is selected by the organisation and not imposed on them by any Data Protection Authority (DPA). The primary responsibility of the DPO is to advise the organisation on all matters related to privacy and the processing of personal data within the organisation and to act as an interface with the DPA. Larger companies have work councils that serve as representative bodies for

²⁹³ Privireal: *Data Protection – Germany* found at www.privireal.org/content/dp/germany.php. Accessed on 11 March 2012.

²⁹⁴ Berlin Commissioner for Data Protection and Freedom of Information, *Parliament* found at www.datenschutz-berlin.de/content/berlin/parlament. Accessed on 11 March 2012.

employees who must give consent to any type of work surveillance impacting on the privacy of employees.²⁹⁵

Germany, as a Member State of the European Union, is subject to the 1995 EU Directive 95/46/EC on the protection of individuals with regard to processing of personal data. This Directive was introduced to harmonise provisions for data protection across Member States.²⁹⁶ As a result of the comprehensive nature of German data protection legislation, the transition to adopt the provisions set out by the Directive did not appear as challenging as in other Member States.²⁹⁷ However, although German Federal data protection legislation is described as stringent and comprehensive, a patchwork of laws and regulations has arisen across the sixteen states of Germany.

Data protection of the private sector comes under the responsibility of the states with exception of telecommunications and postal services companies which are handled at federal level. However, there is little uniformity among the states as it relates to supervision of the private sector. In some states, the supervision is carried out by the Ministry of Home Affairs and in the other by Data Commissioners.²⁹⁸ The State Commissioners for Data Protection are responsible for supervision of state public authorities and organisations. In North Rhine-Westphalia, the supervision is the responsibility of the Commissioner of Data Protection and Freedom of Information for the region. This individual also supervises State

²⁹⁵ The Sedona Conference Working Group Series, International Overview of Discovery, Data Privacy & Disclosure Requirements, *Germany* p. 101.

²⁹⁶ European Commission *Justice* found at ec.europa.eu/justice/data-protection/index_en.htm

²⁹⁷ Privireal: *The History of Data Protection – Germany* found at www.privireal.org/content/dp/germany.php. Accessed on 11 March 2012.

²⁹⁸ LDI, *Data Protection Authorities in Germany* found at www.lidi.nrw.de/LDI_EnglishCorner/mainmenu_DataProtection/Inhalt2/authorities/authorities.php. Accessed on 12 March 2012.

Parliament, public prosecutions services and the courts as it relates to their administrative functions.²⁹⁹

Case Studies in Germany

Data Protection and Healthcare in Germany

When examining data protection at a sectoral level in Germany, some tensions among the main stakeholders become apparent. The tensions are evidenced by the discord and debate about the provisions for German healthcare. There was an IT project started in 2006 in which is intended to facilitate the establishment of a national e-health programme. The German national health IT project initially sought to connect over 2,200 hospitals, 100,000 GPs, 21,000 pharmacies and 200 public health insurance companies. A smartcard infrastructure was incorporated as a method to deal with security issues in the systems. The national electronic prescribing record was to become mandatory for all Germans and an electronic emergency dataset and a personal electronic health record was to be created for each citizen on a voluntary basis.³⁰⁰

It was initially intended that the electronic smartcard the 'gesundheitskarte' (eGK) be issued by the health insurance companies while giving doctors and pharmacists access to patient information. The medical professionals were to be issued their own smartcard which would be a separate 'health professional card' to be able to access patient data as well as electronic prescriptions.³⁰¹ However, given the intent of data protection regulation, this method of collecting, storing and disseminating what would be sensitive personal data typical of medical records would have serious implications for the security.

²⁹⁹ LDI, *Data Protection Authorities in Germany*.

³⁰⁰ E-Health Europe, *German National, E-Health Programme: Contested but Driven Forward* found at www.ehealthurope.net/Features/items. Accessed on 12 March 2012.

³⁰¹ E-Health Europe at www.ehealthurope.net/Features/items. Accessed on 12 March 2012.

Further to this, the project was two years behind its 2006 inauguration as a result of the power struggles that existed in the initial stages between the professional doctors, pharmacists and health insurance companies supported by their respective associations.³⁰²

These power struggles may be a manifestation of unresolved and unclear lines of accountability as it relates to the security of the data and each group questioning the trustworthiness of the custodianship and access to the data. These bodies have come together in the German national IT organisation 'gematik', which currently functions as governmental agency.

A nation-wide roll-out of health cards was initiated by the Federal Government around 2008. Seven pilot projects were starting with 10,000 patients each were set up in selected regions across Germany. Electronic prescriptions were established first in Eastern Saxonia. However, resistance of the doctors was said to increase as implementation got closer. German doctors voted against the electronic health card system because they feared the loss of privacy. One of the concerns mentioned was the bureaucracy attached to the use of digital signatures for electronic prescriptions. In addition, another major concern was the vast amount of money required to implement the smartcards and e-health infrastructure in general. Most of this money would be given to the public health insurance companies. Doctors had to ensure that their IT systems are upgraded which would then be reimbursed through a transaction-based scheme.³⁰³

³⁰² IHS Healthcare and Privacy Blog, *Germany's E-Health Card: Revolutionary Step or Another Doomed Initiative?* at healthcare.blogs.ihs.com/2012/11/12/germanys-e-health-card-revolutionary-step-or-another-doomed-initiative. Accessed on 24 April 2014.

³⁰³ E-Health Europe at www.ehealthurope.net/Features/items. Accessed on 12 March 2012.

A report on the system was to be undertaken in 2013 but no official report has been accessible to date.³⁰⁴ As a result of the tension arising by the national e-health project, many German hospitals, insurance companies, regional governments and private investors have chosen to carry out their own e-health projects.³⁰⁵ This situation poses new risks to the protection of the sensitive personal data that would be managed in these systems. How would compliance with data protection be guaranteed in this environment?

Interpretation of EU Data Protection and Data Retention in Germany

Another issue that raises concern for advocates of data protection in Germany has been the retention of personal data for fighting crime. The monitoring of telecommunication traffic data is seen as crucial to investigating criminal activity.³⁰⁶ This practice increased in Europe particularly after the terrorist attacks in New York, London and Madrid. It was further enforced when the European Union passed the Data Retention Directive (2006/24/EC) on 15 March 2006 to facilitate Europe-wide cooperation on criminal investigations.³⁰⁷ This Directive seeks to address 'the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.' The traffic would include information necessary to identify the originator and the recipient of emails, telephone calls (including Internet telephone calls) with information on the date, time and

³⁰⁴ IHS Healthcare and Privacy Blog, *Germany's E-Health Card: Revolutionary Step or Another Doomed Initiative?* at healthcare.blogs.ihs.com/2012/11/12/germanys-e-health-card-revolutionary-step-or-another-doomed-initiative. Accessed on 24 April 2014.

³⁰⁵ E-Health Europe at www.ehealthurope.net/Features/items. Accessed on 12 March 2012.

³⁰⁶ *Pros and Cons of Data Retention* found at www.vorratsdatenspeicherung.de/content/view/83/87/lang,en. Accessed on 11 March 2012.

³⁰⁷ European Union, *Data Retention Directive (2004/24/EC)* found at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML. Accessed on 28 August 2012.

durations of the telecommunication.³⁰⁸ As a result, debate ensued in Germany over the potential abuse of personal data being retained for the investigation of criminal offences.³⁰⁹

The legal validity of the Directive was questioned by the German Parliament as it relates to its compatibility with the EU Charter of Fundamental Human Rights.³¹⁰ A Working Group on Data Retention was formed and prepared an Opinion where they stated that 'it is clear that the success of blanket communication data retention is very limited'. This group was not convinced that retaining traffic data in order to investigate criminal activity was achieving enough success to justify the violation of the human right to economic and professional freedom and/or the protection of personal data.

This sentiment is further echoed in a German article discussing the pros and cons of data retention where the author argues that data retention leads to exhaustive recordkeeping resulting in harmful effects. It purports that in Germany there is a significant amount of abuse of telecommunications data citing examples of the Deutsche Telekom (T-Mobile) analysing hundreds of thousands of records of its directors, its employees and of journalists in order to identify a leak within the company. A legal matter arose involving a German parliamentarian and privacy advocate Malte Spitz, who in 2009 sued Telekom to gain access to six months of his detailed mobile phone records stored by the company in compliance with German law and the EU Data Retention Directive. Germany was among some European countries to overturn its own version of the law and declared the law unconstitutional in March 2010. As a result, Spitz received a massive file detailing with precision his location whenever his switched on his mobile phone for a six month period. Vodafone has also been

³⁰⁸ Francesca Bigami, 'Protecting Privacy Against the Police in the European Union: The Data Retention Directive', *Duke Law School Faculty Scholarship Series*, Paper 76 (North Carolina, 2007)

³⁰⁹ *Pros and Cons of Data Retention ...* Accessed on 11 March 2012.

³¹⁰ Statewatch News Online, *Impossible to Legality of EU Communications Data Retention Directive Says German Parliament* found at www.statewatch.org/news/2011/jun/eu-mand-ret-wp-on-dp-prel.pdf. Accessed on 28 August 2012.

named as one of the companies who have repeatedly failed to protect its communications data.³¹¹

The German Data Protection Commissioner is reported in 2009 to have found that access to data was not being logged and that more data than necessary was allowed to be retained and not deleted in time.³¹² Interestingly, even the European Data Protection Supervisor is recorded as condemning the Data Retention Directive of 2006 as not adequately meeting privacy and data protection requirements. Germany continues to debate whether it is obliged to comply with this EU Directive.³¹³ The ultimate question in this issue is, does this type of surveillance through the long-term storage of traffic data help or harm innocent people?

In spite of these issues and tensions, Germany continues to be regarded as one of the Member States that upholds the EU Directive in the manner that it was intended. It continues to make efforts to protect its citizens from the unwarranted use of their information while balancing the need to improve information sharing and provide a better service to its citizens.

³¹¹ Cyrus Farivar, *EU Data Protection Authority Condemns Data Retention Directive* published in 2011 found at www.dw.de/dw/article/0,15120172,00.html. Accessed on 29 August 2012.

³¹² *Pros and Cons of Data Retention* found at www.vorratsdatenspeicherung.de/content/view/83/87/lang,en. Accessed on 11 March 2012.

³¹³ Cyrus Farivar, *EU Data Protection Authority Condemns Data Retention Directive*.



Image 7 eH880 Secure Smart Card Terminal used in the German E-Health Programme³¹⁴

www.eh880.com/eh880.php

³¹⁴ Image from the website of the *Advanced Card System (ACS)* company to show device used to managed the smart card in the German health system.

3.3 Data Protection in the United Kingdom

Arduous discussions on data protection as a public policy started in the UK in the early 1970s. The Younger Committee on Privacy was set up to examine the threat posed to personal data by the growing use of computers to regulate society. In 1972, the Younger Committee recommended ten guiding principles for the use of computers that manipulated personal data in its 'Report of the Committee on Privacy' referred to as the 'Younger Report' after its Chair, Kenneth Younger.³¹⁵ The UK government's response to the report was to issue a White Paper which stated that 'the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems, adequately safeguard privacy'.³¹⁶ This Committee recommended ten (10) principles for the use of computers that manipulated data. The UK Government's response was to publish a White Paper. In the Paper, the threat to privacy was identified from five (5) different features of computer operations:

- 1) They facilitate the maintenance of extensive record systems and retention of data in those systems.
- 2) They can make data easily and quickly accessible from many different points.
- 3) They make it possible for data to be transferred quickly from one information system to another.
- 4) They make it possible for data to be combined in ways that might not otherwise be practicable.
- 5) The data are stored, processed, and often transmitted in a form which is not directly intelligible.³¹⁷

Although the recommendations of the Younger Committee were never enacted, the government set up the Lindop Committee to advise on the establishment and composition of a Data Protection Authority.³¹⁸

³¹⁵ Cmnd 5012, 1972.

³¹⁶ Cmnd 6353, 1975.

³¹⁷ Carey, p. 2.

³¹⁸ Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (Oxford, 2004), p. 3.

The Lindop Committee charged in its report that while the Younger Committee had to deal with the whole field of privacy [their] task had been to deal with that of 'data protection'.³¹⁹

The Lindop Report went on to make recommendations for the establishment of a Data Protection Authority and Codes of Practice for different sectors of the business community. These proposals, once again, were not acted upon by the UK government. Newspaper articles of the mid-1970s to early 1980s reveal the overwhelming disappointment of various privacy activists and working groups at the British Government's failing to act on privacy and data protection. The Lindop Committee had strongly advised that data protection be dealt with 'as a matter of urgency' and it was felt that 'security measures [should] be taken to protect the data stored against accidental or unauthorised destruction, accidental loss, unauthorised access, alteration or dissemination.'³²⁰

There were several appeals to the British Government addressed to the then Minister of Home Affairs to indicate the Government's policy on data protection. The concern expressed was 'our European friends are moving ahead of us and we shall be forced eventually into accepting legislation which is unlikely to be satisfactory for this country.'³²¹

By 1980, other western European countries had already brought in privacy and data protection laws namely, Sweden, France, West Germany, Norway, Denmark, Luxembourg and Austria.³²² In an article entitled, 'UK Lagging Behind in Data Protection', the author stated that, 'At the root of the matter are three fundamental facts 1) There is growing world dependency on stored information 2) There is public awareness of increasing vulnerability to use or misuse of personal data, the existence of which may be unknown to those

³¹⁹ Cmnd 7341, 1978.

³²⁰ Frances Gibb, 'British Dilemma over Data Privacy Convention', *The Times* October 22, 1980.

³²¹ C.P.D. Davidson, *Continuing Dangers of Uncontrolled Storage Data*, *The Times* July 17, 1980.

³²² Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (Oxford, 2004) p. 5.

concerned and 3) Great Britain is trailing behind its overseas trading partners in the matter of the introduction of data protection measures.³²³

There were two main catalysts that eventually drove the British Government, as well as other governments that had not yet enacted privacy/data protection legislation, to act. The first emerged at the beginning of the 1980s when the transborder flow of personal data became of economic and societal importance.³²⁴ It was recognised that for the global economy to survive, it was critical that information, particularly personal information, could be exchanged between countries and across continents. This would enable the vital public functions such as air travel and law enforcement, namely the detection and prevention of international crime.³²⁵

There is evidence from newspaper editorials, from the period 1975-1985, that there was some resistance by the UK government to enact these proposals and much lobbying for data protection was done after this period.³²⁶ However, in 1981 the Council of Europe's Convention provided impetus for the passage of the UK Data Protection Act with provisions that corresponded closely to the Convention.³²⁷ This is the second driver for the move to implement data protection in the UK. The UK's first Data Protection Bill was introduced in the House of Lords in December 1982 but its passage was halted. A second Bill was introduced in July 1983 and that went on to become the Data Protection Act of 1984.

The Act introduced a new data protection regime for the holding and processing of personal information. For the first time, data users (data controllers) were obliged to register with a supervisory body in the form of the Office of the Data Protection Registrar. Criminal

³²³ C.P.D. Davidson, 'UK Lagging Behind in Data Protection', *The Times* March 28, 1980.

³²⁴ Stewart Room, *Data Protection & Compliance in Context* (Swindon, 2007), p. 10.

³²⁵ Room, p. 10.

³²⁶ *The Times Newspaper* (1975-1985) in Bibliography, p. 380.

³²⁷ Carey, (Oxford, 2004), p. 2.

offences were introduced for failure to comply with its provisions. The legislation was underpinned by fundamental principles. Although the principles formed the backbone of the 1984 data protection legislation, there was no requirement to comply with their provisions. However, non-compliance could lead to the service of an enforcement notice.³²⁸

It was after the EU Data Protection Directive (95/46/EC) that the UK government, like Germany, re-visited its Act. The Directive required implementation of Member States by 24 October 1998. The UK complied with its legislative obligations by passing the Data Protection Act 1998 which came into force on 1 March 2000 and allowed organisations to achieve compliance by 24 October 2001. The new Act took data protection legislation to a higher level of complexity in the UK. Significant changes were made to the 1984 Act. A host of secondary legislation accompanied the Act. However, the principles that underpinned the Act were, for the most part, maintained. The eight principles are as follows:

‘1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

- (a) At least one of the conditions in Schedule 2 is met, and
- (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

³²⁸ Carey, *Data Protection: A Practical Guide to UK and EU Law* (Oxford, 2004), p. 261.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.³²⁹

The Information Commissioner was set up as the UK's supervisory, independent authority, responsible for promoting the following of good practice by data controllers and for compliance with the Act.³³⁰ The Information Commissioner later became responsible for upholding information rights in the public interest including regulating the Freedom of Information (Fol) Act of 2000 and secondary legislation, the Privacy and Electronic Communication Regulations and the Environmental Information Regulations. The Information Commissioner reports directly to Parliament.³³¹

Part V of the UK Data Protection Act provides methods by which the Information Commissioner can ensure that 'data controllers' comply with the provisions of the Act. The powers of the Commissioner revolve around serving notices on data controllers. It is a criminal offence to fail to respond to any of these notices. In addition to the powers of enforcement given to the Information Commissioner under the legislation, an individual who is the subject of loss or distress may bring court proceedings against the data controller for compensation. Initially, data breach notifications to the UK Information Commissioner were discretionary; however, changes at the level of EU require mandatory data breach notifications among Member States under Directive 2002/58/EC.³³² The Information Commissioner also has the power to assess whether processing of personal data is being carried out in compliance with the Act.

³²⁹ *Data Protection Act 1998* (UK) Part 1, Section 2 at www.legislation.gov.uk/ukpga/1998/29/contents.

³³⁰ Ticher, p. 8.

³³¹ Information Commissioner's Office (ICO), *Legislation* found at www.ico.gov.uk. Accessed on 7 September 2012.

³³² European Commission, *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* at euwiki.org/2002/58/EC. Accessed on 11 May 2014.

In compliance with the EU Directive, medium to large organisations in the UK have been required to hire Data Protection Officers (DPOs) to ensure compliance with the local DPA. The responsibilities of DPOs include seeking to carry out a thorough review of all personal data held by the employer and to setting up procedures and policies for governing the relationship between the employer and its employees.³³³ This post of DPO has in itself opened up debate among EU Member States, particularly Germany, which has raised many questions as to its validity and relevance.

In the UK context, Scotland, Wales and Northern Ireland are treated as satellite offices to the Information Commissioner's Office in regulating data protection. These regions are all subject to the UK Data Protection Act of 1998. However, Scotland has its own Information Commissioner who mainly deals with regulating the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulation 2004 and the INSPIRE (Scotland) Regulations 2009.³³⁴ An ICO Assistant Commissioner takes the lead on behalf of the UK-based Information Commissioner for data protection in Scotland and Northern Ireland. Similarly, there is an ICO Assistant Commissioner who takes the lead with data protection matters in Wales.³³⁵

Some variations in the Act across the data protection regime in the UK may be seen in 'exemptions' in the Act particularly in areas such education, social work as well as particular functions/posts that are permitted to have special status as it relates to data protection in order carry out work that would require use of personal data. For example, the Welsh Administration Ombudsman, the Assembly Ombudsman for Northern Ireland and the Health Service Commissioner for England and Wales, whose duties are to protect the public

³³³ Ticher, p. 215.

³³⁴ Scottish Information Commissioner, The Commissioner at www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx. Accessed on 11 May 2014.

³³⁵ Information Commissioner's Office (ICO) at www.ico.gov.uk. Accessed on 10 September 2012.

within their jurisdiction against misconduct or mismanagement from public and/or private agencies are granted special privileges under the UK Data Protection Act.

Interpretation of EU Data Protection Directive in the UK

In spite of the attempts to strengthen the UK DPA to meet the EU Directive (95/46/EC), a Country Study done in 2010 on the UK provisions entitled, 'New Challenges to Data Protection', describes the Act as 'quirky and extremely complex' and goes on to state that the Act fails to fully implement the requirements of the EU Data Protection Directive.³³⁶ The study posits that even when the concepts appears to broadly correspond to the EU Directive, the UK courts and ICO limit the concept in sometimes in a far different way than in Europe. It cites the concept of 'personal data', 'a relevant filing system' and 'personal data filing system' as examples of the UK narrow interpretation of crucial concepts.³³⁷

The Country Study generally concludes that the data protection regime in the UK remains very weak in comparison with its European counterparts. This it says is evidenced by the low compliance with the law in spite of the increased powers of the ICO. It further argues that, 'the courts are disinclined to give strong protection to personal information and privacy; many matters are regulated not through binding law but through non-binding guidance e.g. the Code for Practice for Archivists and Records Managers. It states that the ICO is quite tightly controlled by Government and does not have enough independent status as it relates to the EU Directive and the application of the law is not sufficiently transparent.'³³⁸

A PricewaterhouseCoopers (PCW) *Information Security Breaches Survey Technical Report* in April 2012 reveals that this year had historically high levels of data protection breaches in

³³⁶ Douwe Korff, European Union, Directorate-Justice, Freedom and Security, *Comparative Study on Different Approaches to New Privacy Challenges, In Particular in Light of Technological Developments, Country Studies – UK* (June 2010) at ssrn.com/abstract=1638938. Accessed on 10 September 2012.

³³⁷ Douwe Korff, *Country Study – UK* (June 2010) pp. 5-7.

³³⁸ Douwe Korff, *Country Study – UK* (June 2010) p. 73.

the UK.³³⁹ The breaches cost UK companies billions of pounds to resolve. Many of the breaches have resulted from the continued escalation of cyber-attacks. The report states that many organisations are struggling to target their security expenditure and there is evidence of complacency particularly in large organisations.

One of the main problems identified by the report is the changing environment in which most organisations, large and small, public and private are operating. It mentions remote hosting of data such as cloud computing as the latest trend with email and websites remaining the most commonly used services. Social networking also has become very important to organisations in the UK and increasingly confidential data is being stored on smart phones and tablet computers.³⁴⁰ This new highly technological recordkeeping environment is having a significant impact on the number of data protection breaches overall and is further explored in the Chapter 4.

Case Studies in the UK

Data Protection and Healthcare in the UK

On 30 April 2012, a Welsh health board became the first NHS organisation to be fined a monetary penalty for a data protection breach. Aneurin Bevan Health Board (ABHB) was issued a fine of £70,000. The Information Commissioner's Office (ICO) reported that a sensitive report containing explicit details on a patient in the system was mistakenly sent to another patient. They further discovered that the staff who made the error were not adequately trained in data protection and there were poor practices throughout the organisation as it related to safeguarding personal information.³⁴¹ The medical profession and health related institutions hold some of the most sensitive personal data within any

³³⁹ The report states that in total 447 organisations complete the survey between February and March 2012.

³⁴⁰ PricewaterhouseCoopers, *UK Information Security Breaches Survey – Technical Report* at www.pwc.co.uk. Accessed on 13 September 2012

³⁴¹ Information Commissioner's Office (ICO) found at www.ico.gov.uk. Accessed on 13 September 2012.

given society and so data protection awareness and training is critical at an organisational level.

A privacy activist group called 'Big Brother Watch' produced a report entitled, *NHS Breaches of Data Protection Law: How patient confidentiality was compromised five times every week* in October 2011. The report claims that according to a Freedom of Information request made by Big Brother Watch, between July 2008 and July 2011, no fewer than 806 incidents of breaches of data protection policies took place in 152 NHS Trusts. This makes an average of 268 incidents per year or 5 times a week. Of the 806 incidents, 23 were said to have occurred when NHS personnel posted confidential medical information on social networking sites. They argue that at least 129 of those incidents occurred when NHS employees inappropriately accessed or used private medical information of their colleagues or families. Approximately, 91 of the incidents occurred when unsecured medical information was lost, left somewhere or stolen. The group states that these breaches do not indicate the full scale of the issues of data protection breaches as they did not get responses from 74 NHS Trusts in the FoI request.³⁴² These figures on the number of breaches in the National Health Service in the UK are alarming by any standard but they are a reflection of what is taking place in other UK public bodies.

Data Protection and UK Local Authorities - Councils

In a news release dated 10 February 2012, the Information Commissioner reported that five councils breached the data protection law by failing to keep personal data secure. He cited that in July 2011, an employee of Brighton and Hove Council emailed details on the personal data of another employee to 2,821 council workers. Basingstoke and Dean Borough Council

³⁴² Big Brother Watch, *NHS Breaches of Data Protection Law: How patient confidentiality was compromised five times every week* found at www.bigbrotherwatch.org.uk/home/2011/10/nhs-data-protection.html. Accessed on 9 September 2012.

were said to breach the DPA on four separate occasions in a two month period. In September 2012, a very significant breach took place. The Scottish Borders Council was fined £250,000 when former employees' pension records were found in an overstuffed paper recycling bank at a supermarket car park. The Council had employed an outside company to digitise the records but did not ensure that the personal data in the records were kept secure. The ICO Assistant Commissioner for Scotland concluded by saying that one thing coming out of the incident is that organisations must realise the importance of properly managing third parties who process their personal data.³⁴³

In response to the number of breaches, the Information Commissioner carried out a number of audits with local authorities to assist them with identifying the weaknesses in their systems and improve the security of personal data within their care. Further to this, he has provided guidance to local authorities for them to understand and meet their data protection obligations. The Information Commissioner took a further step of writing to the local authorities to remind them of their need to comply with their obligations.³⁴⁴ How effective is the outreach of the Information Commissioner in reducing the incidence at organisational level? It may be necessary for the ICO to insist that internal audits and data protection assessment surveys occur with more frequency.

Data Protection: Germany and the UK Compared

The two Member States of the EU examined in this study, do appear to have some issues with their implementation of the Directive. On 24 July 2014, the Information Commissioner's Office (ICO) in the UK published a data breach report which provides statistics and figures showing quarterly data breaches, the types of incidents and incidents

³⁴³ Information Commissioner's Office (ICO) found at www.ico.gov.uk. Accessed on 13 September 2012.

³⁴⁴ Information Commissioner's Office (ICO) found at www.ico.gov.uk. Accessed on 13 September 2012.

by sectors.³⁴⁵ The following image is a graph from the ICO's website which clearly shows that the majority of the breaches occurring in the UK are as a result of human error followed by lost or stolen paperwork. However, the volume of the paperwork created, used and maintained by organisations is not discussed. The trends illustrated here prove that poor organisational processes and practices are impacting on data protection management in this jurisdiction. Unfortunately, similar data is not accessible for Germany where data breach reporting is still emerging.

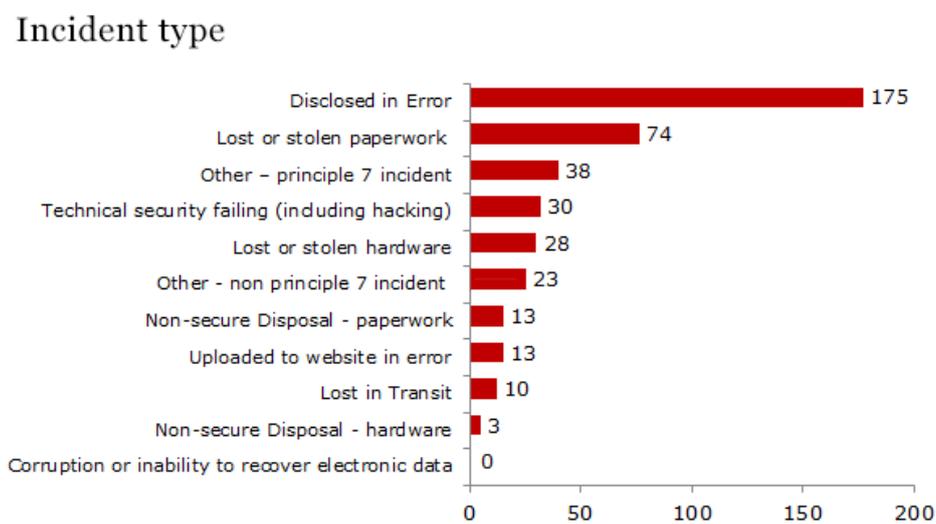


Image 8 Data Breaches - Incident Types (UK)
ico.org.uk/enforcement/trends³⁴⁶

Two global legal consultants commissioned by the European Union have sought to map the levels of data breach notifications³⁴⁷ among its Member States in the European Union for public and private stakeholders. In the mapping, Germany and the United Kingdom are among those Member States ranked as high risk according to the data breach risk index.³⁴⁸

³⁴⁵ Information Commissioner's Office (ICO) *Data Breach Enforcement Trends* at ico.org.uk/enforcement/trends. Accessed on 12 September 2014.

³⁴⁶ Image from *Data Breach Enforcement Trends* at ico.org.uk/enforcement/trends. Accessed on 12 September 2014.

³⁴⁷ Data breach notifications are when a breach of privacy/data protection legislation is reported to the Privacy or Information Commissioner. The Commissioner is therefore notified about the breach and it is recorded. This map shows the situation among EU Member States in 2012.

³⁴⁸ *Interactive Maps of Breach Notification Status* found at info@databreachmaps.com. Accessed on 13 September 2012.

This data along with the case studies and official news on breaches are considered when assessing whether these two countries under the EU Data Protection regime could be considered ‘models’ of data protection in principle and practice.

DATA BREACH MAPS

VISUALIZING DATA BREACH NOTIFICATION REQUIREMENTS AROUND THE WORLD



IMAGE 9 DATA BREACH MAPS

INFO@DATABREACHMAPS.COM

3.4 Data Protection in the United States

Privacy protection in the US has been repeatedly described in the literature as a complex patchwork of laws, regulations, administrative decisions, court orders, constitutional rights and state laws.³⁴⁹ The US approach has been one of self-regulation and what has been referred to as *sectoral* model. The US framework does not support a universal method for merging the privacy issue but rather individual laws have been developed to deal with privacy in government, credit bureaus, financial institutions and health care entities.

In the U.S a balance is sought between an individual's privacy rights and the public's right to know particularly in the case of a public figure.³⁵⁰ Although privacy rights are not explicitly mentioned in the U.S. Constitution, The Bill of Rights, which is the protector of the rights of the minority over majority rule, by limiting the government's power of interference with individual's liberty effectively affirms privacy concepts. The notion of privacy is alluded to in the Third, Fourth, Fifth and Ninth Amendments of the Constitution. In his work, *The Right to Privacy*, Brandon Garrett contends that privacy was an important concern after the American Revolution and this is evidenced by the Fourth Amendment which states,

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched or persons or things to be seized.³⁵¹

The U.S initially led the way with defining privacy. American privacy rights are implicit in the U.S Constitution which broadly affirms privacy concerns by limiting the government's power to interfere with individual liberty.³⁵²

³⁴⁹ Jody R. Westby, *International Guide on Privacy* (Chicago, 2004), p. xx.

³⁵⁰ Brandon Garrett, *The Right to Privacy* (New York, 2001), p. 13.

³⁵¹ United States Courts, *The Fourth Amendment* at www.uscourts.gov. Accessed on 21 April 2014.

³⁵² Menzi Behrnd-Klodt, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005), p. 10.

The U.S government was the first to propose Fair Information Practices (FIPs) in a 1973 report entitled, *Records, Computers and the Rights of Citizens*.³⁵³ A committee was set up under Elliot Richardson, then Secretary of the Department of Health, Education and Welfare in response to the growing use of automated data systems. The United States established by law the Privacy Protection Study Commission in 1974. The principal contribution of this Advisory Committee was to develop a code of fair information practices to safeguard personal privacy at the same time that the Younger Committee was discussing the threat the privacy posed by computerised data in Great Britain.

At least eight states guarantee personal protection in their state constitutions. However, some of the state constitutions merely reiterate the federal constitutional provisions. For example, the Hawaii and Louisiana constitutions both incorporate 'Fourth Amendment-like' provisions. The state constitutions mainly impose restrictions on state governmental activities. These are said to have very little significance and could easily be overridden by the federal law when there is conflict. Their significance is further limited by the global context in the face of cross border informational networks with multinational and national agencies.³⁵⁴

The US Federal Government passed its Privacy Act in 1974.³⁵⁵ The Act served to regulate the collection, maintenance, use and dissemination of personal information maintained by government, as well as to protect the privacy of the individual about whom information is maintained by prohibiting unauthorised disclosure of certain types of information.³⁵⁶ In the

³⁵³ Robert Gellman, *Fair Information Practices: A Basic History* at bobgellman.com/rg-docs/rg-FIPshistory.pdf. Accessed on 31 December 2008, p. 2.

³⁵⁴ Fred Cate, *Privacy in the Information Age* (Washington, 1997), p.p. 67-69.

³⁵⁵ *US Privacy Act of 1974* at www.usa.gov. Accessed on 21 April 2014.

³⁵⁶ NARA, *The Privacy Act* (April 2006) at www.nara.org. Accessed on 24 February 2009.

event of any violations of the Act, a civil suit may be brought against the agency and criminal penalties may be imposed upon the officers or employees of the agency.³⁵⁷

The US Privacy Act of 1974 sought to 'balance the Government need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of privacy stemming from federal agencies' collection, maintenance, use and disclosure of personal information about them. However, the Act applies only to U.S Government agencies and Government contractors operating a system of records on behalf of the Government. It has four main policy objectives:

1. To restrict disclosure of personal identifiable records maintained by agencies;
2. To grant individuals increased rights of access to agency records;
3. To grant individuals the right to seek amendments of agency records maintained on them and upon storing that the records are accurate, relevant, timely or complete;
4. To establish a code of 'fair information practices' that requires agencies to comply with statutory norms for collection, maintenance and dissemination of records.³⁵⁸

Under the administration of President Bill Clinton, a Privacy Working Group was established as part of an Information Infrastructure Task Force, responsible for addressing the privacy issues arising from the exponential growth of electronic information networks. The Group produced a paper entitled, *Principles for Providing and Using Personal Information* in 1995. This document provided principles to deal with the main issues in information privacy at a national and global level. Three main principles were set out on a national level:-

- Information privacy principle – Personal information should be acquired, disclosed, and used only in way that respects an individual's privacy...;
- Information integrity principle – Personal information should not be improperly altered or destroyed...;

³⁵⁷ NARA, *The Privacy Act*, p. 9-8.

³⁵⁸ U.S Department of Justice, *Overview of the Privacy Act of 1974* (2002) at www.usdoj.gov Accessed on 6 February 2009.

- Information quality principle – Personal information should be accurate, timely, complete and relevant for the purpose for which it is provided and used.³⁵⁹

Other principles on privacy on a global level as set out by the Group were the acquisition principle, the notice principle, the protection principle and the fairness principle. Interestingly, these principles were written in the same year as the European Directive on privacy and although the US was not obligated to comply with the Directive many parallels can be drawn to the European principles on data protection.

However, there are a myriad of Acts in the US that seek to address privacy at a national level across various sectors. Unlike the Europeans, Americans appear to very wary of too much central government regulation and the two regions differ significantly on the matter of enforcement. The US regulates at industry level and the score of US Acts that have resulted include, but are not restricted to, the Family Education Rights Act and Privacy Act (FERPA) of 1974, the Right to Financial Privacy Act of 1978, the Electronic Communications Privacy Act of 1986, the Computer Security Act of 1987, the Children’s Online Privacy Protection Act of 1988, the Video Privacy Protection Act of 1988, the Driver’s Privacy Protection Act of 1994, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Fair and Accurate Credit Transactions Act (FACTA) of 2003.³⁶⁰

In spite of all of this legislation which seemingly attempts to cover every aspect of activity within US society, it has been argued that existing legal rights in the US simply do not respond to the need for sanctions against the misuse of personal information.³⁶¹ American law has been viewed as too disjointed, inconsistent, sporadic, confused and wholly

³⁵⁹ Privacy Working Party (US), *Principles for Providing and Using Personal Information* (1995) at aspe.hhs.gov/datacncl/niiprivp.htm. Accessed on 24 April 2014.

³⁶⁰ Information Shield, *US Privacy Laws* at www.informationshield.com/usprivacylaws.html. Accessed on 19 September 2012.

³⁶¹ Joel Reidenberg, E-commerce and Trans-Atlantic Privacy, *Houston Law Review*, p. 725.

inadequate in the face of privacy-invasive technologies and the Internet. This may be as a result of the conflicting interests and tensions that historically exist in US society. Privacy as a human right has been under threat in the post '9/11 world'. Privacy advocates such as James Rule argue that in this environment, 'telephone companies could provide customer information in investigations, telephone conversations could be tapped, employees in the workplace could be searched and secretly filmed, computers could be searched, e-mails could be monitored, trash on the curb could be searched and bank records could be scrutinised.'³⁶²

Joel R. Reidenberg, Professor of Law and Director of the Graduate Program, Fordham University School of Law contends that U.S privacy policy lags far behind and, despite greater public attention, data stalking and information trafficking are norms and the legal provisions do not adequately respond to these practices.³⁶³ He describes the state of American data privacy as appalling and cites examples of plans by Intel and Microsoft to embed and enable components in personal computers that could act as unique identifiers of their owners.

Since September 2001, privacy rights in America have reached a crossroads. Although concerns for privacy remain high, national security issues and the fear of terrorism have resulted in impediments to the privacy rights of U.S citizens and others in the global community.³⁶⁴ As a result, the tensions among countries with regard to the control of personal information are growing. The U.S government is accused of collecting and widely distributing personal data with few privacy limitations, particularly with regard to suspected

³⁶² James Rule, *Privacy in Peril* (Oxford, 2007), p. 144-146.

³⁶³ Joel R. Reidenberg, "E-Commerce and Transatlantic Privacy", Article in *Houston Law Review* Volume 38 (2001), pg. 719.

³⁶⁴ Reidenberg, pg 719.

criminal or terrorist activity.³⁶⁵ In this regard, the most significant piece of legislation intended to obstruct acts of terrorism is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US PATRIOT ACT) passed in 2001 after the September 11th attacks in New York.³⁶⁶ The Act gives authority to the US Federal Government to investigate suspicious financial activities in ways viewed by privacy advocates that lead to the violation of privacy. Is this Act and others that the US has passed in recent times an attack on the principles of privacy? What impact has increased terrorism and heightened national security had on the collection, storage and distribution of records? Events that have taken place in the last two years have brought these questions to the fore and will be discussed in chapters to follow.

Case Studies in the US

Privacy and Healthcare in the US

The Health Insurance Portability and Accountability Act of 1996 referred to as HIPAA law, was enacted by Congress in response to concerns with health coverage, security of medical data and fraud. Before HIPAA, there was no consistency between state and federal requirements for healthcare providers or authority for the enforcement to prevent abuse and fraud in health care programmes. A HIPAA Privacy Standard was instituted in order to establish requirements for disclosing what is called Protected Health Information (PHI). This information is defined as any information on the status of a patient's health, treatment or payments and includes other personal data like the patient's social security number, telephone number and address. The violation of the HIPAA Privacy Standard can result in

³⁶⁵ James Rule, *Privacy in Peril* (Oxford, 2007), p. 144-146.

³⁶⁶ Electronic Privacy Information Centre, *USA Patriot Act (H.R. 3162)* at epic.org/privacy/terrorism/hr3162.html. Accessed on 19 September 2012.

costly penalties and jail terms. However, breaches of that Standard are annually increasing.³⁶⁷

On September 8th, 2011, the New York Times broke the news that there was a major medical breach in privacy at Stanford Hospital in Palo Alto, California. It was reported that personal data on 20,000 patients were posted on a commercial website. The information was said to stay undetected online for nearly a year. That was what was exceptional about this particular breach. The information included names, diagnosis codes, billing charges and account numbers for six months of emergency room service at the hospital. In the 2009 – 2010 *Annual Report to Congress on Breaches of Unsecured Protected Health Information*, four general categories of breaches were identified. These were 1) theft 2) intentional unauthorised access to, use or disclosure of protected information 3) human error and 4) loss of electronic media or paper records containing protected health information.³⁶⁸

The report further stated that theft was the most common cause of breaches. In 2009 alone, 1,468,578 individuals were affected by theft of their protected health information in electronic and paper-based form. Another 483,686 were affected by unauthorised access, use and disclosure, 477,209 by human and technological errors and 11,592 by loss of electronic media and paper records. These figures reflect the areas of key concern in the US health recordkeeping systems.³⁶⁹

³⁶⁷ HIPAA Privacy Standard found at <http://www.all-things-medical-billing.com/hipaa-privacy-standard.html>. Accessed on 21 September 2012.

³⁶⁸ Health Information Technology for Economic and Clinical Health (HITECH), *Annual Report to Congress on Breaches of Unsecured Protected Health Information 2009 and 2010* found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf. Accessed on 21 September 2012, p. 6.

³⁶⁹ Health Information Technology for Economic and Clinical Health (HITECH), *Annual Report to Congress on Breaches of Unsecured Protected Health Information 2009 and 2010*. pp.4-5.

Privacy and the Educational System in the US

The Family Education Rights and Privacy Act (FERPA) of 1974 was passed as a Federal law protecting the privacy of student education records. The Act applies to all schools receiving funds under an applicable programme of the US Government Department of Education. FERPA gives parents some rights to their children's education records and these rights transfer to the child when he or she reaches the age of 18 or attends a school beyond high school level. These students to which rights are transferred are referred to as 'eligible students'. The three main rights afforded the parents of eligible students are 1) the right to inspect and review the student records maintained by the school 2) the right to request that a school correct records which they believe are inaccurate or misleading and 3) the school must seek written permission from the parent or eligible student in order to release any information from the student education record.³⁷⁰ However, FERPA does not mandate schools to have a security or risk management programme to protect student records in place.³⁷¹

In 2010, the daughter of the state Treasurer of West Virginia, Emily Perdue sued Marshall University Board of Governors and her former professor, Laura Wyant, charging that her name and some information about her grades were made public. The civil complaint alleged that on or about 25 September 2009, the employees of Marshall's Board of Governors and the professor improperly released Ms. Perdue's transcript and personal information to third parties without her consent. The attorneys of Ms. Perdue agreed to voluntarily dismiss the lawsuit in exchange for an \$81, 250 settlement.³⁷²

³⁷⁰ US Department of Education, *Family Educational Rights and Privacy Act (FERPA)* found at www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Accessed on 24 September 2012.

³⁷¹ David Sopata, *How FERPA Compares to HIPAA* found at www.infosecisland.com/blogview/17467-How-FERPA-Compares-to-HIPAA.html?amp. Accessed on 24 September 2012.

³⁷² Privacy News From Around the World, *Treasurer's daughter, Marshall University settle FERPA breach lawsuit* found at www.pogowasright.org/?p=16273. Accessed on 24 September 2012.

In October 2011, an even more alarming report was released that thousands of student records were exposed on the US Education Department's direct loans website for seven minutes. The information included social security number, loan repayment histories and bank routing numbers for students.³⁷³ Why this breach is particularly disturbing to advocates of privacy is that the Education Department is the chief enforcer of FERPA and is responsible for regulating the Act on behalf of the Federal Government. Further to this, the Department has been aggressively collecting longitudinal data about students to track their performance and the security of that data is now questionable.

These documented breaches in the regulation and enforcement of two pieces of privacy legislation, the HIPAA and FERPA, are examples in US privacy regime of the types of issues that could arise in the sectoral approach and will be assessed in the chapter's conclusion.



Image 10 Indiana University, Privacy of Medical Records³⁷⁴
protect.iu.edu/privacy/cartoons

³⁷³ Daniel Solove, *Student Privacy in Peril: Massive Data Gathering with Inadequate Privacy and Security* at www.huffingtonpost.com/daniel-j-solove/student-privacy-in-peril-_b_1156907.html. Accessed on 24 September 2012.

³⁷⁴ Image from the Indiana University Public Safety and Institutional Assurance website focusing privacy.

3.5 Data Protection in Canada

The Canadian Government recognised the need for national privacy legislation in the late 1960s and early 1970s when computers emerged as important tools for Government and big business. Canada's constitution guarantees certain privacy rights in the Canadian Charter of Rights and Freedoms. Unlike their neighbours, the Americans, Canada sought to address privacy through comprehensive privacy laws.³⁷⁵ The Privacy Act of 1983 was passed after a Federal government task force produced a paper on privacy and computers.³⁷⁶ This Act applies only to federal government departments and agencies. The central privacy principle under the Act is that personal information under the control of a government institution should not be used by an institution except for the purpose for which it was obtained. Thus, everyone in Canada has the right to apply for access to his or her personal information held by the federal government.

However, the Privacy Act does not apply to private sector institutions and as discussed below, Canada would later pass another federal piece of legislation to deal with the private sector. There was a lack of national data protection standards in Canada. Hence, a committee was set up under the auspices of the Canadian Standards Association (CSA) to devise a set of privacy protection principles that were approved in 1996.³⁷⁷ By 1998, there was another impetus for the Canadian government to re-visit its privacy regime. The EU Data Protection Directive compelled Canada to ensure that its data protection provisions were meeting its criteria of 'adequacy' in order to guarantee protection of the personal information of European citizens doing business with Canada.³⁷⁸

³⁷⁵ *Privacy Act (Canada) 1983* at www.priv.gc.ca/leg_c/r_o_a_e.asp. Accessed on 21 April 2014.

³⁷⁶ Nancy Holmes, *Canada's Federal Privacy Laws Parliamentary Information and Research Service* found at www.parl.gc.ca. Accessed on 26 September 2012.

³⁷⁷ Privacy Principles (Canada) at www.priv.gc.ca/leg_c/p_principle_e.asp. Accessed on 24 April 2014.

³⁷⁸ Colin Bennett, *Private Sector Privacy Reform in Canada: Lessons for Australia* (1997) at www.austlii.edu.au Accessed on 9 February 2009.

However, several policy instruments appeared on the Canadian landscape that influenced their approach to protecting personal data. The Canadian Human Rights Act of 1977 established a limited set of privacy rights which the Privacy Act of 1983 enshrined.³⁷⁹ The Privacy Act allowed Canadians to examine personally identifiable information about them held by more than one hundred (100) governmental agencies.³⁸⁰ It established the Office of the Privacy Commissioner. The Privacy Commissioner acts as an ombudsman with regard to individual privacy protection in Canada. Although the Privacy Commissioner has no powers of enforcement, the office can conduct investigations, administer oaths and if circumstances warrant, bring complaints to the Canadian court system or on behalf of citizens who believe their privacy rights have been violated by government.³⁸¹

The Canadian Privacy Act of 1983, however, did not bring Canada in line with the new international privacy paradigm. A *Model Code for the Protection of Personal Information* was developed by the Canadian Standards Association (CSA). The code emphasises ten dimensions to privacy protection:

1. Accountability
2. Identifiable Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance³⁸²

The code was designed to serve as a model that could be adopted and modified to suit businesses.

³⁷⁹ Office of the Canadian Privacy Commissioner at www.priv.gc.ca/. Accessed on 17 February 2009.

³⁸⁰ Office of the Canadian Privacy Commissioner at www.priv.gc.ca/. Accessed on 17 February 2009.

³⁸¹ Curtis Frye, *Privacy-Enhanced Business* (Connecticut: 2001), p. 68.

³⁸² *Privacy Act (Canada) 1983* at www.priv.gc.ca/leg_c/r_o_a_e.asp. Accessed on 21 April 2014.

On 1 October 1998, a sweeping new privacy law known as the Personal Information Protection and Electronic Document Act (PIPEDA) was passed. The Act came into force in stages from 2001.³⁸³ This was mainly in response to the European Union's Data Protection Directive of 1995 and the need for Canada to meet stringent standards set out by the European Commission regarding the cross-border exchange of personal information.³⁸⁴

A discussion paper in 1998 entitled, the *Protection of Personal Information – Building Canada's Information Economy and Society* was also one of the drivers that led to legislation that established a set of common rules for the protection of personal privacy. Hence, there was the development of a private sector legislative regime. Thus, the Personal Information Protection and Electronic Act (PIPEDA) was enacted in January 2001. This Act established rules governing the collection, use and disclosure of personal information by organisations in the private sector. However, its scope is limited to commercial activities because provinces have exclusive jurisdiction over matters of private property and civil rights.³⁸⁵

PIPEDA came into effect in three separate stages 1) 1 January 2001, the Act applied to the federally regulated private sector 2) 1 January 2002, the Act extended to personal health information and 3) 1 January 2004, included all organisations located entirely within a province. However, where a province has enacted legislation deemed by Order of the Governor in Council as 'substantially similar' to PIPEDA, that province may be exempted from application of the Federal Act. Quebec, Alberta, British Columbia and Ontario (as it relates to personal health information) are exempted from PIPEDA.³⁸⁶

³⁸³ *The Personal Information Protection and Electronic Act (PIPEDA)* at www.priv.gc.ca/leg_c/r_o_p_e.asp. Accessed on 21 April 2014.

³⁸⁴ *The Personal Information Protection and Electronic Act (PIPEDA)*. Accessed on 21 April 2014.

³⁸⁵ Office of Privacy Commissioner of Canada, *PIPEDA* found at www.privcom.gc.ca. Accessed on 28 November 2008.

³⁸⁶ Nancy Holmes, *Canada's Federal Privacy Laws Parliamentary Information and Research Service* found at www.parl.gc.ca. Accessed on 26 September 2012.

Additionally, each province and territory has its own privacy legislation to govern its own governmental authorities. Some provinces have enacted legislation to deal with the privacy of personal health information and the financial sector. The oversight of both Federal Acts is the responsibility of the Privacy Commissioner of Canada but at the level of the province or territory, there are Information and Privacy Commissioners. Information and Privacy Commissioners can be found in Alberta, British Columbia, Yukon, Nunavut, Quebec, Newfoundland, Saskatchewan, North West Territories, Ontario, Prince Edward Island, Manitoba and New Brunswick respectively.³⁸⁷

There is evidence in Canada of tensions in its privacy regime. The Quebec government accused the federal government of exceeding its jurisdiction under PIPEDA in that it interferes with Quebec's constitutional competence in matters of civil rights.³⁸⁸ For this reason, there have been calls to review the Act. A Committee was established from November 2006 to fine-tune the Act to ensure harmonisation with the data protection laws of Quebec, British Columbia and Alberta. After reviewing the provisions for privacy protection in the workplace in the Quebec, British Columbia and Alberta approaches, the Committee felt there was a need to create a separate federal employment model under PIPEDA.³⁸⁹ The Committee also recommended the removal of a controversial provision that was added to PIPEDA in 2002 in response to the events of 11 September 2001 dealing with law enforcement and national security matters that had essentially increased the collection power of the federal government.³⁹⁰

³⁸⁷ Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada* found at www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp. Accessed on 26 September 2012.

³⁸⁸ Nancy Holmes, *Canada's Federal Privacy Laws Parliamentary Information and Research Service* found at <http://www.parl.gc.ca>. Accessed on 28 November 2008, p. 8.

³⁸⁹ Holmes, p. 8.

³⁹⁰ Canadian Parliament, *Protection of Personal Information in the Private Sector* at www.parl.gc.ca/Content/LOP/ResearchPublications/tips/tip102-e.htm. Accessed on 24 April 2014.

The Privacy Commissioner of Canada expressed concerns about the growing number of data breaches occurring in major organisations. She made a call for substantial fines to be imposed to stem the ever-increasing incidents of data breaches. This would only be achieved through strengthening of the Canadian privacy legislation, giving the Commissioner the authority to impose fines.³⁹¹ This may be an indication of the one major weakness of the Canadian privacy regime. It raises the question whether the legislation is sufficiently stringent in ensuring that large, private corporations maintain good privacy practices.

Case Studies in Canada

Privacy and Healthcare in Canada

The Canadian Medical Association (CMA) states that medical breaches are on the rise in Canada. It points to the increase use of portable electronic devices such as computer tablets and mobile devices which lack encryption as one of the causes of privacy breaches. In a survey of 2011, 43.2% of Canadian patients indicated that they would withhold information from the healthcare provider because of concerns with privacy. This would obviously have an impact on the outcome of patient care. The CMA therefore advises that health care providers should not only view privacy as a moral, ethical or legal obligation but a serious part of patient treatment and care. If individuals cannot trust the system, indications are that they would prefer to postpone or totally avoid receiving healthcare.³⁹² This situation has broader implications for the role of privacy within modern societies and requires closer examination.

³⁹¹ Office of the Privacy Commissioner of Canada, News Release found at www.priv.gc.ca/media/nr-c/2011/nr-c_110504_e.asp. Accessed on 29 September 2012

³⁹² Canadian Medical Association, Medical privacy breaches rising found at www.cmaj.ca/content/184/4/E215.full. Accessed on 30 September 2012.

On 1 August 2012, it was reported that an employee in western Newfoundland accessed the medical records of 1,000 patients. This was a week after similar breaches were reported in the largest health authority in Newfoundland and Labrador. Employees were either fired or suspended after discovery of the breaches. The employees were instructed to sign confidentiality pledges and not access any patient records outside their 'circle of care'.³⁹³ The question of whether this response is enough to prevent this type of breach from occurring is valid. Further to this, in March 2012, three urine samples and eight vials of blood with patient names on them were found on a busy St. John's road from the emergency department of the Health Services Centre after being inappropriately disposed of in regular garbage.³⁹⁴

Privacy and Financial Institutions in Canada

Breaches are also taking place in the banking sector. In February 2012, two customers of the Bank of Montreal (BMO) reported that the bank had violated their privacy and trust by allowing sensitive financial information to be accessed by unauthorised people. In the first instance, the monthly account statements of a woman were sent to the home of her ex-husband. The ex-husband took the liberty to go through the details of her account and then contacted her thereafter. It was alleged that he had convinced the BMO to change her address to his. The ex-husband began to threaten her life and demanded money subsequent to the incident. BMO admitted that the changing of the address of the customer was the issue but their lawyers argued that the ex-husband was responsible for his own conduct as it related to her privacy and the subsequent threats to her life. In the other instance, the

³⁹³ CBC News, *Massive breach found at 2nd Newfoundland health authority* found at www.cbc.ca/news/health/story/2012/08/01/nl-western-health-privacy-801.html. Accessed on 29 September 2012.

³⁹⁴ The Toronto Post, *Another privacy breach in Newfoundland* found at thetorontopost.com/news/another-privacy-breach-in-newfoundland/. Accessed on 20 September 2012.

elderly mother of a lady visited BMO to request a copy of her own MasterCard and was mistakenly given copy of her daughter's MasterCard statement instead.

The Assistant Commissioner stated that these incidents are occurring with more frequency in all banks across Canada and believes that training and awareness about privacy for staff is the key solution.³⁹⁵

3.6 Data Protection in Australia

The quest to deal with privacy in Australia has also been described as 'piecemeal and patchy'. Many variants of privacy legislation have emerged across Australia. This model is referred to as the co-regulatory model and is likened in the literature to Canada. The main privacy statute is the Privacy Act also called the Federal Privacy Act. The national Privacy Act of 1988 was established after a decade of proposals.³⁹⁶ It was intended to cover the privacy practices of the federal bureaucracy particularly how Canberra handled the data it collects on citizens who are paying taxes or receiving benefits. The Act also gives individuals access and correction rights in relation to their own personal information held in governmental agencies. In 2000, the Act was extended to include private sector entities.³⁹⁷

This Act initially sought to protect personal information held by Commonwealth governmental agencies. However, in 2000, it was extended to cover the private sector. The Privacy Act extends to a wide range of personal information including health records.³⁹⁸ This is where privacy in Australia gets complicated. The Australian Capital Territory (ACT) is notionally covered by the Privacy Act with the exception of health records which are

³⁹⁵ CBC News, *BMO breached their privacy, customers said* found at www.cbc.ca/news/canada/story/2012/02/03/bc-bankprivacy.html. Accessed on 30 September 2012.

³⁹⁶ *Privacy Act 1988* (Australia) at www.comlaw.gov.au/Series/C2004A03712.

³⁹⁷ Office of the Australian Information Commissioner at www.privacy.gov.au. Accessed on 17 February 2009.

³⁹⁸ Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Sydney, 2005), p. 98.

covered by the ACT Health Records (Access & Privacy) Act of 1997.³⁹⁹ The Northern Territory of Australia has developed its own Information Act of 2002 and enhanced other Acts to include privacy provisions. Queensland had passed the Invasion of Privacy Act in 1972 which was primarily concerned with the licensing of private inquiry agents and the regulation of listening devices. A state Privacy Committee was subsequently established.⁴⁰⁰ The other states including Tasmania, Western Australia and South Australia have issued administrative instructions requiring broad compliance by government agencies with the federal principles.⁴⁰¹

Australia has thus developed a complex privacy regime. Australia has been influenced by business and government agencies in North America and Europe. As with Canada, the EU Data Protection Directive was the harbinger for raising Australian standards for privacy. The national privacy regime encompasses eleven Information Privacy Principles (IPPs) in the Commonwealth Privacy Act of 1988 and ten National Privacy Principles (NPPs) in the Commonwealth Privacy Amendment (Private Sector) Act of 2000. These principles provide the foundation on which privacy provisions across Australia rest. Their influence is evident throughout the various levels of protection.

The Information Privacy Policies (IPPs) can be divided into three broad categories:

- Those which seek to regulate the manner in which governmental agencies collect, store, use and disclose information about individuals;
- Those which allow people access to information agencies keep about them; and
- Those which allow people to request changes to the information.⁴⁰²

³⁹⁹ David Kinley ed., *Human Rights in Australia Law: Principles, Practice and Potential* (NSW, 1998), p. 257.

⁴⁰⁰ Kinley, p. 257.

⁴⁰¹ Kinley, p. 257.

⁴⁰² *Information Privacy Principles* at www.oaic.gov.au/privacy/privacy-act/information-privacy-principles. Accessed on 21 April 2014.

The principles relate to:

1. The manner and purpose of collection
2. Solicitation of personal information from individuals
3. Solicitation generally
4. Storage and security
5. Information relating to records
6. Access to records
7. Alteration of records
8. Checking accuracy before use
9. Use only for relevant purposes
10. Limits on use of personal information
11. Limits on disclosure⁴⁰³

The National Privacy Principles (NPPs) apply to the private sector organisations that collect, use and store personal data. They seek to address ten (10) principles. The principles relate to:

- b. Collection of personal information
- c. Use and disclosure
- d. Data quality
- e. Data security
- f. Openness
- g. Access and correction
- h. Identifiers
- i. Anonymity
- j. Transborder data flows
- k. Sensitive information⁴⁰⁴

Interestingly, section three (3) of the Act clears the way for state/territory privacy legislation when it states that,

It is the intention of the Parliament that this Act is not to affect the operation of a law of state or of a Territory that makes provision with respect to interferences with the privacy of persons and it capable of operating concurrently with this Act.⁴⁰⁵

With the passing of the Privacy Amendment (Private Sector) Act, organisations had to enforce their own codes based on the National Privacy Principles. These codes are approved

⁴⁰³ *Information Privacy Principles* at www.oaic.gov.au/privacy/privacy-act/information-privacy-principles. Accessed on 21 April 2014.

⁴⁰⁴ *National Privacy Principles* at www.oaic.gov.au/privacy/privacy-act/information-privacy-principles. Accessed on 21 April 2014.

⁴⁰⁵ *Privacy Act 1988* (Australia) at www.comlaw.gov.au/Series/C2004A03712. Accessed on 21 April 2014.

by the Privacy Commissioner. The code must provide for an independent adjudicator for handling complaints. If it does not, the Privacy Commissioner becomes the code adjudicator. Any organisation that does not have its own code, must comply with the National Privacy Principles. These principles govern data security, data quality, when information is used and disclosed, identifiers and transborder flow. It has special protection for sensitive information including a person's ethnic origin, political opinions, religious beliefs and membership in a professional or trade association.⁴⁰⁶

Hence, there was the emergence of a number of State and Territory laws, practices and codes of conduct to deal with privacy. Personal information collected by public agencies in New South Wales, the Northern Territory and Victoria are also governed by privacy standards and requirements. The States with the most comprehensive privacy regimes are said to be New South Wales (NSW) and Victoria. New South Wales passed its Privacy & Personal Information Protection Act in 1998. This Act covers the public sector in NSW and established the Office of the NSW Privacy Commissioner. It sets out principles very similar to the federal Privacy Act and the NPPs. The State also passed a Health Records and Information Privacy Act to implement privacy in health records. The State of Victoria passed the Information Privacy Act in 2000 which also sets out the 10 IPPs based on the federal NPPs. An Office of the Victorian Privacy Commissioner was established to administer the Act. They also passed the Health Records Act in 2001 to cover the State's health records.⁴⁰⁷

The layers that exist between Federal, State and Territory laws and regulations have, in some cases, complicated matters relating to privacy. Although in most cases, the laws of the Commonwealth, State or Territory are the same, in instances where there are conflicts or inconsistencies, Commonwealth law prevails. In some sectors, such as health, the providers

⁴⁰⁶ Judy Wallace, *Rights and Freedoms in Australia* (NSW, 1990), p. 22-23.

⁴⁰⁷ Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Sydney, 2005), p. 99-101.

or holders of information are compelled to comply with two sets of legislation at two different levels with two different enforcement regimes.⁴⁰⁸

Section eighty-two (82) of the Federal Privacy Act established a Privacy Advisory Committee with a Privacy Commissioner and six-members appointed by the Governor-General. The role of the Committee is to advise the Commissioner in recommending material for inclusion in the guidelines issued by the Commissioner and to engage in the promotion of community education and consultation regarding privacy. The Commissioner is also required to publish an Annual Report to Parliament.⁴⁰⁹ Before November 2010, privacy was a function carried out solely by the Officer of the Privacy Commissioner. After November 2010, although still the responsibility of the Privacy Commissioner; the function of privacy was moved under the remit of the Office of the Australian Information Commissioner (OAIC).⁴¹⁰

When there is a breach of the Federal Privacy Act, the individual should notify the Privacy Commissioner of his or her grievance and the Commissioner has the authority to investigate the complaint. Thereafter the Commissioner could make a declaration that the individual should be awarded compensation as a result of a breach in privacy. At the State level in NSW, Northern Territory and Victoria, the State Privacy Commissioners have similar authority. However, it has been argued that the amount may not be an adequate deterrent for these types of breaches.⁴¹¹ This raises questions as to how high monetary penalties and/or compensations should be to deter both private and public organisations from breaching privacy.

Case Studies in Australia

⁴⁰⁸ Sally Cameron, *Privacy, Confidentiality and Other Legal Responsibilities*

⁴⁰⁹ *Privacy Act 1988* found at www.austlii.edu.au/au/legis/cth/consol_act/pa1988108. Accessed on 1 October 2012.

⁴¹⁰ Office of the Australian Information Commissioner, *About Privacy* found at www.oaic.gov.au/privacy-portal/about_privacy.html. Accessed on 2 October 2012.

⁴¹¹ Carolyn Doyle and Mirko Bagaric, p. 131.

Privacy and Healthcare in Australia

The healthcare system in Australia has also been subject to increasing privacy breaches in recent times. The Office of the Privacy Commissioner received a number of its enquiries from the health sector. In March 2010, staff of Medicare (Australia) were accused of ‘snooping’ into patient medical records.⁴¹² This happened just before plans to implement a national electronic health scheme. It raised fears from privacy advocates that healthcare officials could not be trusted. Around 400 cases emerged of unauthorised ‘snooping’ by Medicare staff who were investigated and were subsequently disciplined. No details were provided as to the methods of discipline utilised.⁴¹³

The Australian government introduced a Bill in 2010 to establish ‘individual health identifiers’. It later became the Healthcare Identifiers Act and Regulations of 2010. This is very similar to the system introduced in Germany where there would be the use of an ID number to collate patient records in one place so that health care providers could gain access to health care information at one time. However, the challenge is to ensure that the right security controls are in place to prevent unauthorised access to vast amounts of sensitive data.⁴¹⁴ Similar to Canada, when a survey was conducted among Australians regarding how they felt about privacy in the healthcare system, 49.1% said that they have withheld or would withhold information when or if they had a sensitive medical condition due to concerns about privacy.⁴¹⁵

⁴¹² The Australian, *Medicare Privacy breaches shakes e-health legislation* at www.theaustralian.com.au/technology/medicare-privacy-breaches-shake-healthcare-identifier-legislation/story-e6frgax-1225835812144. Accessed on 24 April 2014.

⁴¹³ The Australian, *Medicare Privacy breaches shakes e-health legislation* at www.theaustralian.com.au/technology/medicare-privacy-breaches-shake-healthcare-identifier-legislation/story-e6frgax-1225835812144. Accessed on 24 April 2014. .

⁴¹⁴ ABC News, *Medicare privacy breaches ‘only the beginning’* found at www.abc.net.au/news/2010-03-02/medicare-privacy-breaches-only-the-beginning/347648. Accessed on 1 August 2014.

⁴¹⁵ New London Consulting, *Australia: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* found at

In April 2012, it was reported that there were 56 data breaches for the last financial year in Australia and the Privacy Commissioner was investigating another 59 breaches. The Privacy Commissioner lamented at Privacy Awareness Week (2012) that breaches were on the rise and this was corroborated by security research showing that there was an increase in hacking attacks to steal personal information from websites and on-line businesses. Once again, there is the issue of the increase in breaches being linked to advances in technology that enable determined hackers or 'snoopers' to access electronically stored records. Some high profile breaches occurred with companies such as Google, Sony and Telstra. The legislation in Australia does not dictate that businesses must disclose data breaches as in Europe and the US. The Privacy Commissioner is calling for changes to be made to the legislation towards this end.⁴¹⁶

Some changes have been taking place in the Australian privacy regime in 2014. One important change to note is that the Privacy Principles have been consolidated into thirteen harmonised privacy principles for Australia as a nation. This change may help to strengthen the Australian approach to dealing with privacy.⁴¹⁷

3.7 Data Protection in New Zealand

New Zealand has taken a unique approach to privacy protection. The model developed here is referred to as the omnibus model. New Zealand passed its Freedom of Information law entitled the Official Information Act (OIA) in 1982.⁴¹⁸ This Act falls under the responsibility of the Ombudsman. Under OIA, all government information is declared open unless it should

⁴¹⁶ The Sidney Morning Herald, *One data breach a week: Australia* found at www.smh.com.au/it-pro/security-it/one-data-breach-a-week-australia-20120430-1xulv.html. Accessed on 2 October 2012.

⁴¹⁷ Office of the Australian Information Commissioner at www.oaic.gov.au/privacy/privacy-act/the-privacy-act. Accessed on 3 September 2014.

⁴¹⁸ Office of the Australian Information Commissioner at www.privacy.gov.au. Accessed on 17 February 2009.

be protected. In other words, the Act seeks to address openness of information while protecting privacy simultaneously. Some of stated goals of the OIA that relate to privacy are:

- 'to provide for proper access by each person to official information relating to that person; and
- to protect official information to the extent consistent with the public interest and the preservation of personal privacy.'⁴¹⁹

It was in 1993 that New Zealand then passed a Privacy Act to enhance protections for personal information. The law covers privacy protection in both the private and public sector. It sets out twelve (12) principles to guide behaviour rather than micro-regulate privacy.

The Act incorporated twelve privacy principles similarly to those found in Australia. Principles 1, 2, 3 & 4 govern the collection of personal information. Principle 5 governs the way personal information is stored. Principle 6 gives individuals the right to access information about themselves. Principle 7 gives individuals the right to correct information themselves. Principle 8, 9, 10 and 11 places restrictions on people and organisations regarding who could use and disclose personal information and Principle 12 governs 'unique identifiers' e.g. bank client numbers and passport numbers.⁴²⁰ However, the principles are not prescriptive in nature and allow organisations to design their own information handling policies. It is expected that the agency would be open and transparent about its policies while protecting the privacy of individuals.

Further to this, the New Zealand Privacy Act serves to regulate government data matching.⁴²¹ It authorises the making of codes of practice and in effect modifies the privacy principles to make them more stringent or more lenient to fit a particular case. It mandates

⁴¹⁹ *Official Information Act 1982* at

<http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html>. Accessed on 21 April 2014.

⁴²⁰ Office of Privacy Commissioner of New Zealand at privacy.org.nz. Accessed on 2 October 2012.

⁴²¹ Office of Privacy Commissioner of New Zealand at <http://privacy.org.nz>. Accessed on 17 February 2009.

the Commissioner to monitor and comment publicly on government policies and laws that impact on personal information. It supports openness and transparency in the use and disclosure of information. Additionally, but quite separately, the NZ Courts have developed a privacy tort so that one person could sue another for breach of their privacy.⁴²²

The Privacy Act applies to the handling of all personal information collected and held by government agencies and most businesses. The Act also covers the private sector including major New Zealand owned businesses, sole traders and the local arm of overseas-owned businesses. The legislation is based on twelve Information Privacy Principles (IPPs), similar to the National Privacy Principles (NPPs) originally derived from the OECD Guidelines.⁴²³ The New Zealand legislation established an office of the national Privacy Commissioner.

The New Zealand privacy jurisdiction differs in several fundamental respects from the European Union model. This is evident in the fact that notification of data processing to a supervisory authority is not required. Yet, the NZ Act conforms to European standards by making judicial remedies available for privacy infringements. This includes compensation for persons who suffer loss. The NZ Privacy Commissioner oversees compliance with the legislation, but does not function as a central data registration or notification authority. The Commissioner does not have the power to determine legal rights or liabilities under the Act, except in relation to charging for information.⁴²⁴

The NZ Commissioner has issued seven codes since the establishment of the Privacy Act.

The codes are as follows:

⁴²² Caslon Analytics, New Zealand Privacy Regime found at <http://www.caslon.com>. Accessed on 12 February 2009.

⁴²³ Paul Roth, Remedies under New Zealand Privacy Law Pt. 1, *Privacy Law and Policy Reporter* found at www.austlii.edu.au/journal. Accessed on 9 February 2009.

⁴²⁴ *Privacy Law and Policy Reporter, Remedies under New Zealand Privacy Law* at www.austlii.edu.au. Accessed on 9 February 2009.

- Health Information Privacy Code of 1994
- GCS Information Privacy Code of 1994
- Superannuation Schemes Unique Identifier Code 1995
- EDS Information Privacy Code (Amended) in 1997
- Justice Sector Unique Identifier Code of 1998
- Post-Compulsory Education Unique Identifier Code of 2001
- Telecommunications Information Privacy Code of 2003⁴²⁵

New Zealand appears on the surface to have a well-developed, coherent privacy regime which really consists of two separate regimes operating in tandem. The Privacy Act covers personal information relating to the data subject and the other regime is the freedom of information regime through the Official Information Act (OIA) that covers access to personal information by a person who is not the person to whom the information related. How New Zealand achieves balance between the two regimes is by weighing privacy interests against public interests. Official information is not released when there is a privacy interest. This may be illustrated as seen below. The inner circle which represents personal information is protected.

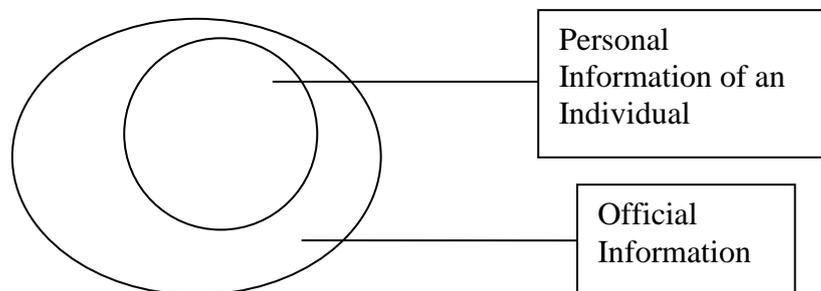


Diagram 1 *New Zealand Approach to Official vs. Personal Information*
produced by the author

This means that the assessment of public interests versus private interest rests with the agency in which a request has been made. A host of questions would need to be asked to assess whether the request encroaches on the right to privacy of an individual. These questions include:

- Is the information personal information?

⁴²⁵ *Privacy Act 1993* (New Zealand) at www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

- Why is the information being held?
- Has the requester identified a public interest reason for disclosure?
- Does the agency see any other public interest reasons? (e.g. accountability of officials or expenditure of public funds)⁴²⁶

The NZ Privacy Commissioner's role is threefold. The chief activity of the Privacy Commissioner is to investigate and conciliate complaints made by aggrieved individuals. Secondly, the Privacy Commissioner can undertake investigations into interferences with the privacy of individuals on his or her own initiative, particularly with high profile disclosures. This is less common. Thirdly, the Privacy Commissioner can inquire into privacy matters and comment on them on his or her own initiative.⁴²⁷ The Privacy Commissioner oversees compliance of the Act but does not function as a central data registration or notification authority as in the European jurisdiction. Decisions regarding the protection of privacy are made through a consultative process between the Privacy Commissioner and the Ombudsman.

Types of official records which have posed some concerns to New Zealanders have been the Electoral Roll, the Register of Motor Vehicles and the Register of Land Titles. Although citizens understand the need to collect this data by the state, fears of abuse of their personal information have been heightened by the increased use of computerisation to record this information.⁴²⁸

Case Studies in New Zealand

Privacy and Healthcare (Personal Accident Insurance) in New Zealand

⁴²⁶ FOI Live 2005 Conference, *The Official Information Act and Privacy: New Zealand's Story* (London, 2005) found at privacy.org.nz/assets/Files/67725421.pdf. Accessed on 2 October 2012.

⁴²⁷ Office of the Privacy Commissioner at <http://privacy.org.nz>. Accessed on 21 April 2014.

⁴²⁸ FOI Live 2005 Conference, *The Official Information Act and Privacy: New Zealand's Story* (London, 2005)

One of the most significant breaches to date in New Zealand took place in August 2011 with the Accident Compensation Corporation (ACC). This corporation was established by the New Zealand Government to prevent injury, to ensure persons get treatment for injuries when they occur and to assist them with getting back to normal life after an injury. The ACC, therefore, collects and assesses a substantial amount of health related and personal information. The nature of the breach was that an email containing information on 6,748 clients of ACC was inadvertently sent to an ACC client. That client's information was among that included in the spreadsheet. The ACC was not aware of the breach until the client eventually met with them in December 2011. The ACC then sent a letter to the client requesting that the information be returned.⁴²⁹ This situation was as a result of human error and again points to a need for careful action on the part of staff.

Privacy and Tax Collection in New Zealand

The Inland Revenue Department (IRD) is responsible for the collection of taxes on behalf of the New Zealand Government. In September 2012, the department extended an apology to New Zealanders regarding a privacy breach that occurred. The personal information of 30 individuals was reportedly released to the public incorrectly. This incident was as a result of a manual mail processing error. The IRD and Office of the Privacy Commissioner are in the process of investigating the breach. Interestingly, the department has blamed the lack of technology as creating the environment for the breach.⁴³⁰ This view supports the argument of this study that technology facilitates breaches in ways that were not possible before. Although breaches could occur in paper-based systems, the ease of retrieval in poorly designed electronic systems can enable undetected breaches.

⁴²⁹ *Independent Review of ACC Privacy and Security of Information* found at www.acc.co.nz. Accessed on 3 October 2012.

⁴³⁰ TV NZ, One News, IRD Apologises for Privacy Breach found at tvnz.co.nz/national-news/ird-apologises-privacy-breach-5107252. Accessed on 3 October 2012.

Country	Legislation	Year	Model/Approach	Code for RM	System of Government
Germany	-Data Protection Act <i>Bundesdatenschutzgesetz</i>	2001	EU Comprehensive	No	Federal
UK	-Data Protection Act (Public & Private Sector)	1998	EU Comprehensive	Yes	Devolved State
Canada	-Privacy Act (Federal) -PIPEDA (Private Sector)	1985 2000	Co-Regulatory	No	Federal
Australia	-Privacy Act (Federal) -Privacy Amendment (Private Sector) Act -Other legislation & industry codes	1988 2001	Co-Regulatory	No Reference to RK in IPPs	Federal
U.S	-Privacy Act (Federal) -Other legislation at sectoral level	1974	Sectoral	No	Federal
New Zealand	- OIA -Privacy Act (Public & Private Sector)	1982 1993	Omnibus	No	Unitary State

Table 2 Data Protection Models in Selected Jurisdictions
produced by the author

3.8 Conclusions

This chapter has provided the context of the development of data protection within the selected jurisdictions; it has discussed the four data protection ‘models’ or more appropriately approaches; it has outlined the key provisions for privacy/data protection within each country and it has considered some major breaches that occurred within each jurisdiction with a special focus on data protection in health care systems.

Some general observations from the findings⁴³¹ on data protection regulation and management across jurisdictions are: 1) In federal systems, data protection regulation becomes complicated at localised levels due to apparent tensions and differences between provincial and central government in the respective countries. Evidence of these tensions

⁴³¹ Data gathered from daily news items, blogs and listservs of privacy professionals globally.

was seen in particularly the US and the Australian context where state-level or territory-level provisions are created for privacy which are not always on par with the federal legislation. This provides a key lesson for the West Indies as it results to issues such as the lack of harmonisation within these jurisdictions. Harmonisation will be a significant factor for a region like the West Indies because of the need to conduct business internally and externally using personal data. This personal data should be equally protected so that its reliability is unquestionable. 2) Issues of trust can arise among some key players in the regulation of data protection as it relates to the ownership of personal information and the best means of sharing that information. Similarly, there is another lesson here because key players within various sectors should be operating using the same standards for protecting personal data. The processes that take place within each sector should be reliable and there should be accountability in actions taken by staff working with personal data. 3) Organisations across all jurisdictions have not been exercising due diligence as it relates to contractual arrangements to ensure that the companies they outsource to store their electronic records and information are in compliance with data protection legislation. This shows that there must be a mechanism for privacy risk assessment and ensuring that the proper vetting of external storage providers cannot be overlooked. Privacy risk assessments are not just for internal processes but should cover what happens when personal data leaves the custody of the organisation. 4) Some workers within organisations are not aware of provisions for data protection at either a national or sectoral level. This finding provides another valuable lesson to the West Indies. It stresses the importance of training and orientation of staff as well as 'refresher' sessions to raise the awareness about data protection/privacy within public and private agencies. 5) Incidents of breaches are caused in many cases by carelessness, negligence or lack of awareness and training leading to human error and 6) malicious intent by staff working with personal data is one of the key factors

leading non-compliance. These findings support the idea that human behaviour is responsible for the majority of breaches. The lesson is that organisations must find effective ways to manage these behaviours through use of guidelines or principles, policies and procedures.

The case studies discussed in the Chapter are significant to this study. They demonstrate that even in the stringent data protection regimes, breaches are happening, in some cases, with alarming frequency. The case studies selected illustrate the typical errors and breaches resulting from poor practices within organisations regardless of sector and jurisdiction. These breaches are similar in nature but the risks are greater in the sectors selected in this studies based on the research. The case studies were derived primarily from news reports in the form of news articles, television and radio reports, with some from official sources such as the websites of Privacy/Data Protection/Information Commissioners. A number of these breach reports are circulated by law offices specialising in data protection and privacy advocates such as the International Association of Privacy Professionals through their daily dashboards.⁴³² The frequency of the news reports and the daily 'dashboard' on breaches globally suggests that these breaches are typical. For more official sources of information on breaches, it is prudent to visit the websites of offices of the Privacy/Data Protection/Information Commissioners to access lists of cases of breaches and may also be possible to access annual reports on breaches. This, however, is not done consistently in all jurisdictions, particularly those which do not have mandatory breach notifications. Both Germany and the UK have the mandatory breach notifications provision in place and so it would be easier to track breaches in these countries. This does not mean that all breaches are reported and so garnering accurate statistics proves challenging.

⁴³² International Association of Privacy Professionals at www.privacyassociation.org.

3.8.1 Assessing the 'Models'

This section specifically assesses the four 'models' for privacy/data protection, namely, the *comprehensive* model as seen in the EU with its Member States, the *sectoral* model as seen in the US, the *co-regulatory* model as seen in Canada and Australia and the *omnibus* model as seen in New Zealand, to determine whether any of these models are suitable in the region of the West Indies.

The first step in this analysis is to consider use of the meaning of the term 'model' as seen in the literature discussed in Chapter 1. *Models*, according to theory in public policy and management, make precise assumptions about a limited set of parameters and variables. Models are therefore used to fix variables at specific settings and to explore the outcomes produced.⁴³³ In the case of the four data protection models, three key variables were identified. These are 1) the regulatory provisions and system(s) of enforcement established within the particular jurisdiction 2) the application and interpretation of those provisions i.e. through use of mechanisms such as technology, policies and procedures and codes of practice and 3) the people who either put the provisions into practice and/or are affected by the provisions and practice. Another key consideration within each regime was the breaches and types of breaches that took place therein. This is important to note when using the term 'model' to mean the standard which something or someone should emulate. When put in that context, the question that then could be asked is whether any of these four models could be held up as a standard or example to be followed by the West Indies?

The four models are indeed four distinct approaches to the public issue of protecting personal information. The *comprehensive* model of the European Union instituted by its

⁴³³ Dr. Khaled F. Sherif, *A Comparison of Frameworks, Theories and Models of Policy Process* found at www.ksherif.com/images/Lecture_10-Comparison_of_Frameworks.ppt. Accessed on 21 October 2012.

Data Protection Directive essentially seeks to regulate data protection of both the public and private sector using a single piece of legislation at national level that explicitly sets out to protect the rights of all citizens across all sectors in the EU Member States. However, it can be seen that this attempt to cover all aspects of data protection has still resulted in a host of regulations and codes being developed at national level to deal with special interests. It is for this reason that the original intent of the Directive could be lost and made more complex. At a national level, the UK has been criticised as weakening the fundamentals of data protection by 'diluting' the EU definitions and introducing other types of legislation that are not compatible with its own data protection law. Germany, the other EU Member State under review, appears to hold to a greater extent the standard established by the EU but still there is evidence of points of weakening at the sectoral level.

What has resulted is that the national interpretation of the EU Data Protection Directive has been clouded by the social, economic, political context at national level. It is also noted that existing legal and recordkeeping traditions may have some influence on how national data protection legislation is implemented. Among special interests groups within the various sectors, industry codes have added another layer of requirements that have led to inconsistencies in how national legislation is interpreted. The Directive itself is the cause of the problem of interpretation in its use of terminology which may differ across Member States. However, it is not practicable to make a broad, high level directive overly prescriptive given that each Member State has its own nuances in their systems of governance. Hence varying interpretations will arise from country to country. This may be the main driver for the European Union to move away from a Directive to a Regulation in

2012 in order to have a more direct influence on dealing with data protection across its Member States.⁴³⁴

The merit of the comprehensive model in the European Union can be seen in its system of regulation and enforcement which are relatively more intelligible and well structured than the sectoral and co-regulatory models. An Information Commissioner sits on the top of the pyramid of monitoring and enforcement and that individual is supported by Assistant Commissioners based mainly on geographic divisions. At the level of the organisation, the Data Protection Officers (DPOs), when employed, are responsible for ensuring that the organisation is compliant with the law and advising with its implementation. These posts are high level posts and in Germany are compulsory. What is striking from a records management perspective is that at the organisational level, records managers in the UK have a Code of Practice which clearly sets out their role as it relates to data protection and it is common to find the role of the DPO and records manager integrated. However, the role of the records manager as it relates to data protection is not as discernible in the German data protection regime and the other jurisdictions reviewed.

The following diagram was created to illustrate the legal effect of the EU Data Protection Directive on citizens in Member States.

⁴³⁴ European Commission, *Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25.1.2012, 2012/0011 (COD) at listservsec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 11 May 2014.

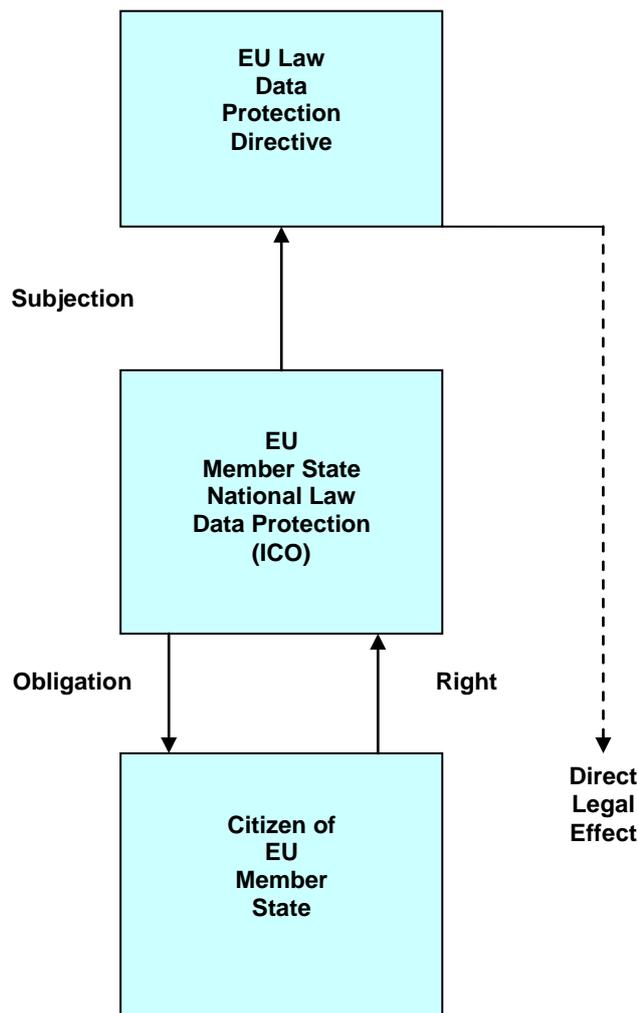


Diagram 2 The Legal Effect of the EU Data Protection Directive
Adapted by the author

The sectoral model as found in the United States developed as a result of the avoidance of an omnibus, centralised, governmental regulation for data protection. In the US, although there is a Privacy Act that serves the Federal Government and private organisations administering systems of records for government, there is a host of legislation, some of which is incompatible, at state and sectoral level to govern privacy at state level and within private organisations. In addition, there are numerous regulations to accompany the pantheon of laws. This approach is aptly described as patchy and complex and has implications for recordkeeping. Why? In this environment, it is very difficult for an individual

to navigate the laws and decipher which authority is relevant to their circumstance. There is no centralised or 'one stop' body of monitoring, regulation or even to provide advice to the citizen in the event of a breach. Legal counsel in dealing with privacy is inescapable. The records management programme may be the only saviour for the organisation when faced with a law suit. A good records management programme would not only protect the organisation but the individual from poor recordkeeping practices that would lead to breaches.

At an organisational level in the sectoral model, the role of the records manager would be even more critical and would need to be clearly defined as it relates to dealing with privacy issues in recordkeeping. A designated privacy professional is not always employed by private companies and there are no regulations making it mandatory. Where there is no clearly identifiable officer with accountability for regulating privacy, the risk of breaches increase and the organisation as well as its staff and clients are subject to unwarranted exposure of the personal information held therein. A single company may be caught in the 'cross hairs' of legislation and it may be challenging for it to keep track of changes in the legislative landscape, particularly those that relate to how they manage their personal information.

The gaps in the sectoral model and its incompatibility with the EU comprehensive model has caused a large rift between the US and the EU as it relates to the sharing of information across borders particularly in light of globalisation and the increased use of technology. The two regions sought to address their differences by entering into a 'Safe Harbor' agreement in 2000. This agreement was designed to allow the transfer of data into the US in cases

where the transfer would not meet the EU standard for 'adequacy'.⁴³⁵ However, concerns for the US handling of personal data have not abated and with its heightened sensitivity to national security, privacy may be under threat more than since the World Wars. At a glance, this model or approach to privacy/data protection does not augur well for jurisdictions that seek to conduct business with the EU and other jurisdictions that emulate the EU approach.

The Canadian and Australian Government have been said to have adopted the co-regulatory model in regulating privacy. They have established a variation of the European Union data protection model. Under this approach, industry and government work together in a systematic way, industry drafts and enforces privacy protection but an oversight agency is provided. Historically, Canada and Australia have had a similar path of development and have both faced the challenge of creating national policy within federal systems with shared responsibility for the private sector.⁴³⁶ This is reflected in their approach to dealing with privacy.

Australia, like Canada, seems torn between the North American and European models for privacy protection. In Australia, the amalgamation of approaches has resulted in what can be described as plural privacy regimes. This entails a combination between a unified national system (Commonwealth), state government systems and major territories systems. There is heavy reliance on industry self-regulation as seen in the US codes of practice, which has been developed at industry level and endorsed by the Federal Privacy Commissioner. However, the merits to such a complex network of industry codes, federal, state and territorial law are questionable.

⁴³⁵ Linklaters, *Technology, Media and Telecommunications News, Germany – Is the Safe Harbor Agreement Still Safe?* found at www.linklaters.com/Publications/Publication1403Newsletter/20100317/Pages/Germany%E2%80%93IsItTheSafeHarbor.aspx. Accessed on 23 October 2012.

⁴³⁶ Colin Bennett, *Private Sector Privacy Reform in Canada: Lessons for Australia* (1997) at www.austlii.edu.au Accessed on 9 February 2009.

In spite of all the codes developed to deal with privacy, in 2012, Australia earned a reputation for being the most intrusive government in the Western world. An article in the Globalist Report accuses Australia of spying into the lives of its citizens even more than the US Government. It states more than 17 governmental agencies including the Australian Tax Office and Medicare have been spying on citizens since 2010 by accessing telephone and Internet data records without a warrant threatening privacy on a grand scale. The Australian law enforcement authorities have claimed that terrorism is the cause for their interception of personal data.⁴³⁷ However, the US has regained its position as the top government for spying on its citizens as seen with the recent debacle on the NSA's activities previously discussed in Chapter 1.⁴³⁸

The New South Wales Council for Civil Liberties expressed its concern about the collection and use of personal data by agencies to the Australian Law Reform Commission. It suggested that the Privacy Law should be amended to create a tort on privacy and a tort on intrusion.⁴³⁹ Then privacy would be dealt with as a civil wrong and citizens would be in a position to sue for an injunction to prevent the continuation of the breaches to their privacy or for monetary damages. This form of privacy protection that seeks to prove emotional harm, which was first introduced by the Americans Warren and Brandeis, may not adequately cover all types of breaches that may occur with personal data in records in the computer age.

⁴³⁷ Andrew Puhanic, *Australian Government Now Spies on its Citizens More than the US Government Does* found at www.theglobalistreport.com/australian-government-spies-on-its-citizens. Accessed on 24 October 2012.

⁴³⁸ Fox News, *Spying on Congress – NSA Scandals gets even worst in 2014* at www.foxnews.com/opinion/2014/01/09/spying-on-congress-nsa-scandal-gets-even-worse-in-2014. Accessed on 21 April 2014.

⁴³⁹ New South Wales Council, *Submission to the Australia Law Reform Commission Inquiry on Privacy Legislation* found at www.nswccl.org.au/docs/pdf/ALRC%20Privacy%20Submission%202007.pdf. Accessed on 24 October 2012.

Disclosure of breaches in privacy is not mandatory and there have been calls for changes in the legislation in this area. This measure may be used as a deterrent to such rampant breaches. In addition, compensation to victims is low in relation to the severity of the breach. Increasing the penalties paid by organisations for breaching privacy provisions is another measure that may help to reduce the amount of breaches in this jurisdiction. Another issue is that complex maze of privacy provisions results in retarding the response to complaints. The NSW Council for Civil Liberties contends that it can take months for the Privacy Commissioner to deal with a privacy matter.⁴⁴⁰

The Canadian privacy regime, although similar to Australia in its co-regulatory approach, is slightly less complicated than Australia. The Canadians have legislation for federal agencies in the form of the Privacy Act and private agencies in the form of Personal Information Protection and Electronic Documents Act (PIPEDA) and a central body for regulation and enforcement under the Office of the Privacy Commissioner of Canada at the top level. However, at provincial level, the privacy issue becomes somewhat muddled as each province has its own privacy legislation and sectoral provisions. This resulted in the need for the federal Act to be amended in a quest to harmonise across provinces. Provinces such as Quebec historically are suspicious of the Federal Government's intentions and do not accept any pronouncements without question. This points to weaknesses in the privacy regime as the rifts between federal powers and province powers may be the cause of some breaches that have occurred with records in the various systems. This situation makes the Canadian privacy regime unduly unstable and demonstrates how political and cultural variables could impact on the implementation of privacy.

⁴⁴⁰ Australian Government - Australian Law Reform Commission, *Privacy Law and Practice* at www.alrc.gov.au/inquiries/privacy. Accessed on 25 April 2014.

The New Zealand approach to privacy is different from all the other jurisdictions and deserves closer examination mainly because of its apparent simplicity. The NZ Government has taken an omnibus approach which encompasses both the public and private sector under one piece of legislation and is hinged on the concept of openness. In this model, it is accepted that all records are opened to the public under the OIA but those containing personal data are closed⁴⁴¹ and subject to the Privacy Act.

This approach has the benefits of not being overly complicated and because it is omnibus, it does not have several layers of regulation as the other models. Of course, New Zealand does not have to grapple with the tensions of a federal system. However, the main concern for this approach would be leaving the assessment of whether a matter affects an individual in the hands of an agency or company. Essentially, this is what occurs with the NZ approach to privacy. Citizens are expected to trust in the administration of privacy, leaving the choice of openness or closure of records to the state and to private organisations. However, the report breaches to the Privacy Commissioner who has the authority to carry out investigations and the matters could be brought before the Human Rights Tribunal; so there are provisions for handling grievances.⁴⁴²

3.8.2 Assessing the Mechanics of the Models

When investigating the mechanics of models for privacy/data protection in the selected jurisdictions, significant areas of concern are revealed from a records management perspective. Some of which is seen in the case studies within each jurisdiction and the others gleaned from interviews and observation. Some of the issues include the apparent increasing need for privacy/data protection due to the existing tensions between the main

⁴⁴¹ The term 'closed' in archives and records management refers to when access to a record/document is prohibited.

⁴⁴² *Privacy Act 1993* (New Zealand) at www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

'actors' in privacy regulation; the impact of cultural, historical, political and social factors on the meaning and interpretation of 'privacy'; apparent flaws in some systems of monitoring and regulation as it relates to records; the need for sanctions that reflect the severity of breaches; the need for employee awareness and training particularly in the handling of records with personal information; the need to conduct thorough privacy risk assessments and audits in recordkeeping systems; the impact of advancing technology and/or lack of technology but, important to this study, the understated role of the record managers in the implementation and management of privacy protection within the public and private sector organisations.⁴⁴³

Nevertheless, a look across all the jurisdictions has shown that there is common ground as it relates to the core principles that underpin informational privacy and data protection. Even in a jurisdiction as under regulated as the United States, the core values are apparent and the view of privacy as a human right is shared. The main differences relate to the manner in which the public policy to protect personal information is regulated. Where some jurisdictions see the need for omnibus national legislation and several layers of monitoring and control, others take a 'softer' approach by providing guidelines and industry codes which are not mandatory. In the end, managing privacy/data protection seems exceedingly challenging in all environments due to its very nature.

Unquestionably, there is a need to generate records containing personal data for the efficient running of a society but how those records are treated are dependent on two main variables. The two main elements involved are 1) the automation i.e. the control technologies and 2) people i.e. workers and end-users working within the systems.

⁴⁴³ The findings on the mechanics are mainly based on interviews, site visits and observation to assess how data protection is interpreted, implemented and managed at the lower levels.

Across all jurisdictions, the impact of advancing technology on privacy/data protection particularly as it relates to the creation, distribution and storage of records is irrefutable. Although a universal definition for privacy cannot be distilled across the jurisdictions, the same concern for informational privacy is evident. The issue here is how rapid advances in technology have enabled increased breaches of privacy/data protection. The enabling technologies include, but are not restricted to, Wide Area Networks (WANs) with growing numbers of end-users, powerful databases, websites, social media, the advent of cloud computing and the increasing use of tablets, smart phones and laptops. Interestingly, the breaches are not always as a result of malicious intent but a substantial amount of breaches also result from human error in using the available technologies.

Security measures have thus become even more critical in today's environment. Citizens across the various jurisdictions have expressed their concern for the apparent lack of security found in high profile public and private organisations that interact with their personal data in their automated recordkeeping systems. In paper-based, manual systems, a document could be locked in filing cabinet or a vault and only accessed by the persons who were in possession of a physical key. In the automated environment, the 'key' to accessing electronic records could be unlocked by individuals possessing the technological 'savvy' and usually this would be done with malicious and/or harmful intentions. In all jurisdictions, there is evidence of instances of unencrypted files on lost laptops, tablets or smart-phones, intentional or unintentional, unauthorised access to personal data in highly confidential databases, personal data being leaked by use of social media and inadequately secured websites are but a few of the situations that have been highlighted by the press and have reached governmental levels of discussion and debate.

It was also noted that the media houses, which in themselves constitute one of the most feared groups as it relates to privacy/data protection across the globe, have been the first and most active groups in exposing or 'whistle blowing' breaches in privacy/data protection in recordkeeping systems. They fuel the fears of the citizenry but at the same time reflect what matters to the populace.⁴⁴⁴

Another similarity that may be identified is the increased expectations of citizens/clients/customers towards how their personal information should be handled or treated by public and private entities. In the case of public agencies, citizens seem to understand and accept that there is a need for government to collect and capture relevant information on their personal circumstance to carry out and improve services but they also hold to question the security of that information and expect that it will not be abused to their disadvantage or detriment. This is even more pronounced in societies like the United States where too much governmental or federal intervention into the lives and affairs of citizens is seen as a fundamental disregard for their rights as outlined in the US Constitution and Bill of Rights.⁴⁴⁵ Ironically, this historical and cultural reality has been the main reason behind the lack of strong centralised regulation of privacy by the US Government. There are varying degrees of concern in other federal jurisdictions like Germany and Canada but ultimately, citizens expect that governments would not be unnecessarily intrusive when collecting, storing and using their personal data and that information would be safeguarded from unwarranted access.

In regulating privacy across the five jurisdictions, some tensions between the 'actors' are apparent. At a macro level, tensions exist between the states, provinces or territories and

⁴⁴⁴ See Section on the Press and Data Protection, p. 295.

⁴⁴⁵ US Bill of Right, www.constitution.org/billofr_.htm. Accessed 3 September 2014.

the central or, in some cases, federal governments. This is glaring in the US in particular but can be seen in Canada, Germany and Australia. Hence, multiple systems of monitoring and regulation have been developed and at times can lead to lack of clarity for the key stakeholders in navigating the various regulations at the central and local levels. The UK and Germany are less complicated in this regard being subject to the EU Directive. Their infrastructure for regulating data protection appears to be more coherent and understandable. However, in Australia, where multiple levels of protection exist, the regulation of privacy can be described as patchy and complex and can result in tensions between the main actors.

At a micro level, tensions exist between the various 'actors' operating within the various sectors as seen with Germany and its healthcare sector. Some groups view themselves as more qualified to access highly confidential personal data over others that may have to interact with the same records. For example, medical doctors in Germany expressed disapproval with insurance companies being the main holders of medical information in the healthcare system. The intent was to make the system more efficient with the main players being able to access the personal data of an individual in the same location. However, some groups see themselves as more trustworthy and capable than others in protecting privacy on a national scale.

Another important question that arises is, is privacy more likely to be breached in a private organisation than a public one? The findings have shown that due to the advances in technology, public and private organisations are equally guilty in not ensuring that all appropriate steps are taken to protect an individual's privacy. Although the tendency may be to link breaches to private companies, the same kinds of causes for breaches are occurring in public bodies answerable to governments and their citizens.

What is evident is that all types of organisations across all sectors need to implement the right measures to properly manage privacy in their recordkeeping systems. The environments are similar with both public and private companies working in 'hybrid' environment that use both paper-based, manual systems in tandem with automated systems. Some of these key measures include conducting regularised privacy risk or impact assessments and audits of all systems. The training and awareness of staff is crucial even with the best policies and procedures in place. New staff would require orientation to deal with the issues that could arise with handling records containing personal information of internal and external customers.

Another area that requires consideration is the issue of the weight of sanctions for breaching data protection. Sanctions, which are either criminal or civil in nature, vary across the jurisdictions. The European Union stance on sanctions in its Member States since its 2012 proposal for a Regulation is that sanctions imposed by data protection authorities should be increased to up to EU€250,000 for less serious breaches and up to EU1,000 000 for serious breaches.⁴⁴⁶ As seen earlier in the Chapter, this issue is being reviewed in jurisdictions such as Canada and Australia which have been discussing increases on sanctions as a means of deterring breaches. Whether the increasing of sanctions would reduce the number of breaches across jurisdictions is yet to be determined because these proposals have not yet taken effect. However, a lesson can be learnt about establishing effective deterrents through penalties from the implementation stage. If these are too low, sanctions will be overlooked or ignored and bad practices among public and private organisations will persist. Sanctions must have 'teeth' and produce a 'chilling effect' to be effective.

⁴⁴⁶ European Commission, Press Release Database, *Progress on EU data protection reform now irreversible following European Parliament vote* at europa.eu/rapid/press-release_MEMO-14-186_en.htm. Accessed on 11 May 2014.

After analysing the models and cases of breaches, this study posits that records management can play a vital role in upholding the provisions for data protection/privacy at an organisational level. Privacy will need to be addressed taking a balanced approach, not only looking at systems of regulation and enforcement at the top levels but strengthening the management and control of private records and personal information at the lower levels with attention being paid to the behaviour of individuals, processes and working groups within the various functional areas and organisational systems. Collaboration between professions and disciplines to problem-solving and finding workable solutions to data protection is also necessary. Therefore, the following chapter fully explores and describes the inherent relationship between data protection and records management. It also examines how this relationship should be integrated with other functional areas within organisations.



Image 11 Cartoon on Privacy Impact Assessment
www.behance.net/gallery/Privacy-Cartoons/3754298⁴⁴⁷

⁴⁴⁷ Image by Chris Slane, a New Zealand editorial cartoonist on privacy.

SECTION THREE
CONCLUSIONS AND RECOMMENDATIONS

4. CHAPTER 4

THE RELATIONSHIP BETWEEN DATA PROTECTION AND RECORDS MANAGEMENT (RM)

In the previous chapter, it was seen that the existing models for data protection within the selected jurisdictions focused on a high level or macro approach when dealing with data protection/privacy regulation, enforcement and management. However, it is evident from the breaches reported that this approach has not effectively dealt with data protection in practice at an organisational level. The breaches revealed that bad practices such as indiscriminate dumping of personal information and human error such as accidentally posting personal information on the Internet have been occurring in organisations. This study asserts that public and private entities are on the frontline of the data privacy issue because they create and receive, distribute and maintain records of their clients/customers and their own staff in order to conduct daily business.

The persistent issues with informational privacy should be dealt with at all levels combining sound data protection legislation and enforcement with sensible pro-active measures in public and private sector recordkeeping systems involving all the key stakeholders. Further to this assertion, if the data protection issue is effectively tackled at organisational level, there would be an overall national reduction in breaches. How then can understanding the relationship between data protection and records management (RM) bring about much needed improvements to dealing with data protection at the organisational level?

This chapter examines and describes how records management is related to and could potentially resolve some of the key issues of managing data privacy/data protection. It opens by exploring and introducing a new RM approach that provides a framework for identifying records that are subject to data protection and discussed the main reasons for

their selection. In addition, a hierarchy or classification of privacy protection for records found within a typical organisation is provided. The chapter shows how data protection strategies could have been incorporated to prevent the types of breaches such as those described in the previous chapter and explores whether records management can be considered best placed for ensuring sound data protection management now and in the future. Finally, it provides some key mechanisms to prevent breaches in recordkeeping systems and discusses the implications of data protection in managing archival records for the society at large.

4.1 A New RM Approach for Data Protection: What Makes Personal Records *Truly* Personal?

In any given organisation, there are records containing personal data about ‘living, identifiable’ people. Yet, it is at times difficult to assess when a record can be considered a personal record or whether every record containing some form of ‘personal data’ is indeed personal. The clear identification of records which are subject to data protection based on definitions for what is ‘personal data’ is critical to the management of those records. This action, referred to as *attribution* in the EU model, essentially means when personal data is linked to a ‘data subject’ in order for data protection principles to take effect.⁴⁴⁸ Defining ‘personal data’ has been opened to wide interpretation across all jurisdictions and, as a result of case law, has become even more imprecise.⁴⁴⁹ Some jurisdictions have not paid a great deal of attention to the concept of a ‘data subject’ or the idea of multiple data subjects in a given record as seen in the EU model but rather focus on the information itself

⁴⁴⁸ European Commission, *Proposal for the Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* found at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 27 December 2012.

⁴⁴⁹ An example of case law that has blurred the meaning of ‘personal data’ can be found in the UK *Durant vs. Financial Services* (2003) where the issue of multiple data subjects in a single record arose. This led to the need to identify the ‘primary data subject’.

to determine if it can be traced to an identifiable person or persons. The problem here is that the quantity or quality of the information on an identifiable person is not prescribed by law and has been difficult to measure. To illustrate the point, one could query, is a name of an individual in a record enough to make that record attributable to that person? In many cases, it is not. This then leads to the question, what makes a personal record truly personal?

In order to address this question, it would be useful to examine the legal definitions of 'personal data' in the models under review. A look at these definitions may shed some light on why it is so challenging to define and identify what are personal data/records among organisational records based on data protection legislation. This following table presents that information:-

DP/Privacy Model	Definition of 'Personal Data'
EU Comprehensive Model	Any information related to an identified or identifiable natural person ⁴⁵⁰
Canadian Co-Regulatory Model	Information about an identifiable person that is recorded in any form ⁴⁵¹
Australian Co-Regulatory Model	Information or an opinion on an individual whose identity is apparent or can reasonably be ascertained from that information or opinion ⁴⁵²
US Sectoral Model (Federal Privacy Act)	No clear definition provided. <i>Act instead defines 'record' as any item, collection or grouping of information about an individual that is maintained by an agency</i> ⁴⁵³
NZ Omnibus Model	Information about an identifiable person; and includes information related to a death maintained by the Registrar-General. ⁴⁵⁴

Table 3 Definitions of 'Personal Data' in Selected Jurisdictions

Produced by the author

These definitions are not useful or conclusive in determining what makes a personal record truly personal or attributable to an individual. They do not provide the data controllers/processors any guidance in identifying records subject to data protection. The only common thread here is that a person must be identifiable but the definitions prove too broad as to what kind of information and how much of that information is involved. Implicit in these definitions is that there must be enough details in a record that would enable a user to see a glimpse into the life of an individual in the 'snapshot' of the record. Therefore, the concept of the 'life story' in a record will be used in this study to mean any personal details about an individual that allows a user to learn about and/or re-construct aspects of an individual's personal life. This may include details about where the person was born,

⁴⁵⁰ A broader definition is being proposed in the 2012 EU Regulation to 'any information related to a data subject'. This would allow for the determination to be made on a case by case basis.

⁴⁵¹ *Privacy Act (Canada) 1983* at www.priv.gc.ca/leg_c/r_o_a_e.asp.

⁴⁵² *Privacy Act 1988* found at www.austlii.edu.au/au/legis/cth/consol_act/pa1988108. Accessed on 1 October 2012.

⁴⁵³ *US Privacy Act of 1974* at www.usa.gov. Accessed on 21 April 2014.

⁴⁵⁴ *Privacy Act 1993 (New Zealand)* at www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

ethnicity, educational background, marital status, credit history, political affiliation, medical history and more. The capacity to re-construct 'life stories' of individuals from a record usually is not the original intent behind the creation of the record but is inherent because of the *evidential* and *informational* nature of records.

Central themes in records management can be applied in the concept of the 'life story'. The *authenticity* and *integrity* of the personal record must be maintained over time. This would mean that the systems used to manage the records from their creation to their final disposition must preserve all the characteristics of records. The characteristics of records as stated in records management are that they must be accurate, complete, understandable, authentic and reliable to be considered true records. Therefore, personal records would need to meet this standard. It is also accepted in records management that records are *evidential* and *informational* by nature.⁴⁵⁵ They provide evidence of activities and they inherently provide information by communicating the context, ideas and opinions of a subject at particular point in time and in a particular space. The personal record therefore must be able to provide evidence of the activities of an identifiable individual and/or information about that individual within a particular context.

This study is the first to suggest that the record or data can only be defined as personal if there is enough content about an identifiable person for the user to become aware of aspects of the personal life, status, condition, opinions, relationships, interactions and transactions of an individual. For example, a comment made by a board member and recorded in the minutes of a board meeting may only be considered personal if he or she mentions details about his or her own involvement, status, relationship, interaction and/or

⁴⁵⁵ Elizabeth Shepherd and Geoffrey Yeo, *Managing Records: A Handbook of Principles and Practice* (London, 2003), pp. 10-12.

transaction with the topic under discussion or similar details about another identifiable individual. Ultimately, in defining the personal record, it is less challenging to determine that personal details such as names, address and other status information are 'personal data' than classifying the aspirations, motivations, feelings and/or opinions of a person as personal. The latter still falls within the realm of personal data by law and if disclosed without consent can lead to the embarrassment or harassment of an individual.

When assessing what makes a personal record truly personal, record-keepers could utilise a simple approach that would enable the measurement of personal details in the content of the record. This method is illustrated below in Figure 1.2.

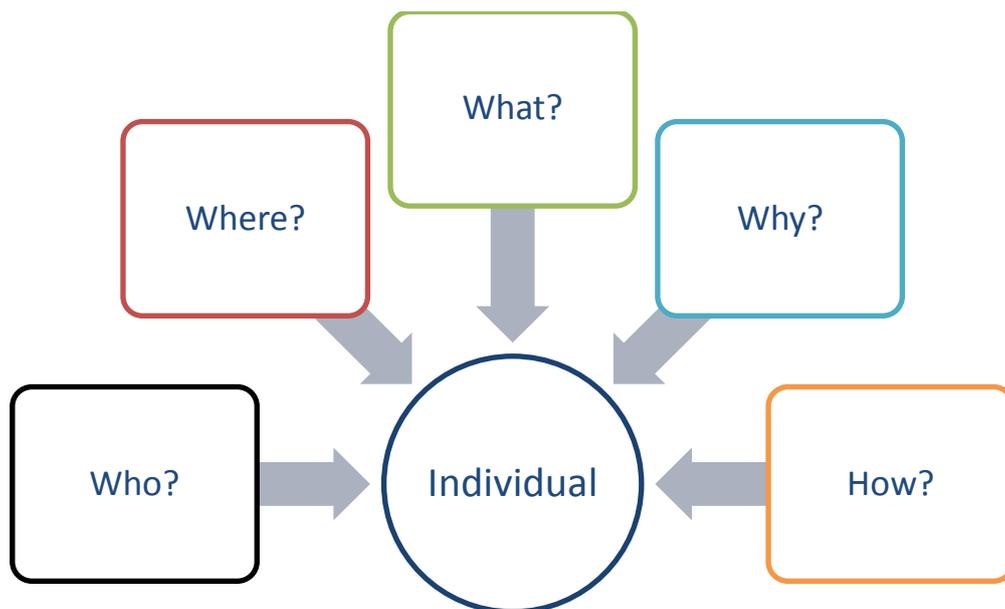


Diagram 3 Five Elements of a Personal Record
produced by the author

1. **WHO? (Identity)** – includes name, unique identifier, community and nationality
2. **WHERE? (Space/Time)** – includes geographical location and/or temporal placement
3. **WHAT? (Relationship(s))** – includes status, interrelationship(s), bond(s)
4. **WHY? (Ideology)** – includes cultural, political or historical influences, beliefs, values, motivations
5. **HOW? (Behaviour)** – includes actions, reactions, attitudes, emotions

Key Questions

Who? (Identity) – Does the record indirectly or directly provide the name of an individual or allow for an individual to be identifiable?

Where? (Space & Place) – Does the record provide current contact details/location of an individual?

What? (Relationship) – Does the record reveal the status/relationship/interaction/transactions of an individual?

Why? (Ideology) – Does the record reveal the opinions/motivations/intentions/aspirations of an individual?

How? (Behaviour) – Does the record reveal methods/actions employed by an individual to deal with a matter relating to that individual?

All or some of the elements may exist in a single record. However, the most important element for the record to be subject to data protection is *identity*, as personal data must be traceable to an identifiable individual. That is unquestionable as all definitions in the existing legislation state that very clearly across jurisdictions. An address on a record has no personal meaning unless it is linked to a named individual. Note that identity may not take the form of a name but a unique identifier, such as a Personal Identification Number (PIN) as seen with Germany. A PIN would make the individual identifiable if the information can be further linked to a name. For a record to be considered truly personal, more than one of

these elements must be present in order for it to be meaningful and reveal some aspect of the person's life story. The details when put together would provide *context*. A list of names alone has no meaning to a user unless it is placed within a particular context. A list of names of persons who defaulted on loans would have meaning as it gives the context to why the names are there. As with the study of Diplomats discussed in Chapter 1, the understanding of records go far beyond the medium, a form and content but the consequences in which they were created.

The structure or form that records containing personal data take is also telling or revealing. The record captures information based on its format and its function. If it is free form like a diary, journal, letter or email, the details captured would generally tend to be more comprehensive including not only a name and contact information but including a state or condition, intent, opinions and/or expectations. If the record takes the format of a form, the data captured may not be as wide ranging. The records format in itself would provide some context and may implicitly provide the background to the actions/transactions of the individual. For example, an entry form for a competition at a department store suggests that the individual or associate may have had to purchase an item in that store in order to enter. The details captured in the form give part of the life story but the form having been completed provides evidence that the individual or associate completed a transaction at the store giving background to their actions. Again, we see here the form was not designed to create a life story but inherent in the record are intangible details about a person's activities/life.

4.2 Implementing the 'Life-story' Approach in RM Programmes

One of the aspects of recordkeeping that is highlighted when dealing with data protection/privacy in records is the need to place the concern for the lives of individual people at the fore when processing records containing personal data. This study suggests that traditionally records managers/archivists have been heavily engaged with needs of organisations and the society at large and so they have not focused on the needs of people who are the 'data subjects' in records. The idea is that the 'life-story' of an individual or a group of individuals could be present in the records that records manager/archivists handle from day-to-day. Records managers/archivists, therefore, need to re-examine their thinking and approach to records dealing with records that may contain telling details on the lives of people.

When seeking to implement the 'life-story' approach to deal with data protection/privacy in RM programmes, records managers/archivists should first take into account the mission and vision of their organisation so as to understand what types of records containing personal data should naturally accumulate across all functional areas, regardless of format. After this assessment is made, it should be followed by careful planning to systematically deal with any issues that could arise with managing the life-story of clients and staff from record creation to final disposition. The following section broadly outlines the key steps that should be taken, regardless of the type of organisation, when seeking to implement a 'life-story' approach to data protection/privacy in records:

Step 1 Conducting a Comprehensive Inventory

Records manager/archivists should conduct a comprehensive Inventory of all records created, received, distributed and stored by their organisations, both in electronic and paper-based formats, across all functional areas. This is always the first step in properly

establishing a well-functioning records management programme. The records containing personal data can only be identified when all record holdings are known.

Step 2 Identify Personal Data in Records – Record Groups/Series level

As was discussed in the previous section, a critical part of data protection management is to identify records containing personal data. In this step, record groups containing high concentrations of personal data that could lead to the identification of identifiable individuals and the reconstruction of their life-stories are identified. A high-level classification for the protection of records is provided later in this chapter e.g. personnel/client files.⁴⁵⁶ Classification allows for the systematic and logical grouping of records to facilitate consistent capture, retrieval and disposition. The identification of record groups containing personal data would enable records manager/archivists to take a high level approach to addressing data protection by designing classification schemas that isolate and 'flag' (highlight) records containing personal data at secondary level or series level so that the right measures regarding access, security and retention could be applied. Below is an example of part of a functional classification schema which addresses data protection/privacy by highlighting the records series under the primary heading of 'Human Resources' that contain the highest concentration of personal data:

HUMAN RESOURCES	300
Human Resources – General	
Human Resources – Policies and Procedures	
Human Resources – Reports and Statistics	
Human Resources - Benefits & Pensions	
Human Resources - Employees	
Human Resources - Job Descriptions	
Human Resources - Vacancies	

⁴⁵⁶ See pg. 256 for Hierarchy of protection in classes of records containing personal data.

Table 4 Sample of Records Classification Schema with 'Flagged' Records Series for DP
Produced by the author

Step 3 Identify Personal Data in Records – Documents/Item level

Records manager/archivists should also be prepared to deal with the identification of personal data captured at document or item level that could lead to the identification of living individuals and reveal parts of their life-story. In any organisation, there will be records that contain personal data that may be found in unexpected categories. Records manager/archivists, in these instances, will need to examine records page-by-page using the 'life-story' approach to identify information that is truly personal in nature and subject to data protection or privacy legislation so that appropriate measures are taken to protect this type of information recorded therein. e.g. Minutes of the Board of Trustees.

It is recommended that records practitioners carry out both high level as well as low level identification of truly personal data to ensure that breach to data protection and privacy are reduced significantly.

Step 4 Employ Measures for Data Protection in Records

After identification of the life-story in records, records practitioners should employ the most appropriate measures for protecting personal information from unwarranted access or unsuitable disposition decisions such as prolonged retention of records which should be destroyed. This Chapter provides the measures that should be used in RM programmes.⁴⁵⁷

Step 5 Document and communicate decisions and actions

Records managers should document decisions and approaches taken to address data protection/privacy in the organisations' recordkeeping systems and communicate the plan

⁴⁵⁷ See pg. 246.

of action to all members of staff. This could be done as part of orientation programmes for new staff members and awareness seminars or workshops for existing staff members.

Life-story Approach - The Cost of Implementation

When seeking to implement the life-story approach in an RM programme, it is important to consider how this approach impacts on the cost of operations. The RM/archivist must first seek senior management approval and would need to justify the objectives which relate to the need to safeguard personal data and acquire the funds required to meet the objectives. The areas where additional resources would be needed are staffing, communication and training, hardware and software, space management and equipment. A concern raised in more than one interview is that the funds for implementing a data protection approach are 'not easily acquired' especially in organisations where budgets for information management are small or have been cut.

In a RM system that is predominately paper-based, costs may not be as high as a system which relies heavily on automation. Electronic document and records management systems (EDRMS) are subject to higher costs because of the need to upgrade hardware and software periodically to combat obsolescence. The EDRMS also requires sophisticated support from IT personnel to deal with server issues and 'back-up' procedures. IT resources usually reside outside of the RM function and, in some cases, the differing priorities and perspectives can make collaboration a challenging experience. However, automated systems make it easier to manage data protection and implement the 'life-story' approach in a systematic way from the creation to the final disposition of records and information. In an automated environment, personal data could be identified, accessed securely, 'flagged' for action and disposed of using a properly designed system with EDRMS functionalities.

The following is a break-down of budgetary requirements for the implementation of the life-story approach:

a) Staffing - A skilled individual, who may be the RM/Archivist, should be assigned the responsibility to coordinate and oversee the management data protection and implement the approach. If the organisation is financially sound, a Data Protection Office working in conjunction with the RM and other supporting personnel trained in records management and data protection may be employed.

b) Communication and Training - A good communication and training strategy is required. This includes the design, marketing and distribution of material that thoroughly explains the approach as well as policies and procedures for data protection management are absolutely critical to successful implementation.

c) Hardware and software

The budget should include the costs of adequate computer systems and an EDRM software that meets international standards (DoD 5015.2 or MoReq2 model requirements for managing electronic records)⁴⁵⁸. There are emerging privacy protection software packages on the market that may be investigated. Wherever automation is used, adequate strategies for upgrading as well as to deal with disaster management and long term preservation should be considered.

d) Space management, Environmental controls and Equipment

Equipment that would be required includes fire-proof safes or vaults, appropriate cabinets and shelving for the proper storage of records containing personal data. Space management considerations include ensuring that the records are adequately safeguarded in locked rooms or vaults and the location of records is clearly documented. The physical integrity of

⁴⁵⁸ DoD 5015.2 records management directive or standard may be accessed at www.defense.gov/webmasters/policy/dodd50152p.pdf and the MoReq2 model requirements may be accessed at moreq2.eu/moreq2.

records containing personal information should be maintained with the appropriate environmental controls such as air-conditioning and de/humidifiers as required. Fire detection and suppression as well as anti-intrusion systems are recommended. Organisations may also invest in shredders or incinerators to ensure the secure destruction of records no longer needed. These standards are typically met in any good records management programme.

4.3 The 'Life-story' Approach and Modern Records and Archives Theories

Modern archival theorist Geoffrey Yeo speaks of records as *persistent representations* of activities. Representations are said to be 'things that stand for something.' Yeo argues that records essentially 'stand for' activities and are persistent because they have the capacity to endure beyond the immediate circumstance leading to their creation. He further states that the activities represented by records are gone but that the record allows us a picture of them.⁴⁵⁹ If one accepts this idea, then personal records represent the activities of an individual and leave behind a picture of their circumstance at a point in time and, in some instances, depending on the type of record, their thoughts, feelings and motivations. Yeo surmises that representations are not perfect.

In the concept of the 'life story' approach, the record as a representation allows the user of the record to reconstruct some aspects of the person's life story and based on the data protection principle of accuracy in personal data, the life story reconstructed should be as accurate as possible. As an example, a personnel record on an individual in context can reveal a great deal of detail of the activity of an individual in the context of doing his or her job within an organisation. Another interesting dimension is that the personal record may

⁴⁵⁹ Geoffrey Yeo, *Concepts of a Record (1): Evidence, Information and Persistent Representations*, *The American Archivist*, Vol. 70 (Fall/Winter, 2007), pp. 334-343.

also simultaneously create a picture of life within the organisation and the influence of the organisation within society at large.⁴⁶⁰ Hence, there is a 'continuum of representation' in the personal record. A single personal record can have several representations or meanings according to who interrogates it and the reasons behind that interrogation.

Eric Ketelaar has offered another useful perspective that is compatible with the 'life story' approach as it relates to the societal meaning of personal records when he contends that records don't tell stories, people tell stories.⁴⁶¹ The story reconstructed about an individual by the user may differ according to the user. Although the same information is provided in the record, different users may draw distinct conclusions of the life story of an individual based on the time and space in which they exist. Ketelaar further suggests that records are 'memory texts' for the construction of memory and several memories co-exist at the same time in a 'memory continuum'.⁴⁶² The time/space element to the construction of life stories is also affected by the changing meaning of what is personal. As the concept of privacy is ever changing, in some instances, what was private or personal twenty years ago is no longer private and personal today. For example, some types of private information that may have been discussed or shared within the confines of a group of family or friends are now placed in a publicly accessible space through social media sites such as *Facebook* or *Twitter*. As time passes and memories about an individual fade, the record stands alone and the accuracy of the personal data would serve well beyond the life of the individual in the telling of his or her life story. This would have implications for the new types of personal records that people create about themselves using social media. Before entering personal

⁴⁶⁰ Based on experience as a trained archivist/records manager.

⁴⁶¹ Ketelaar, Eric, 'Archival Temples, Archival Prisons: Modes of Power and Protection', *Archival Science* 2: 221–238, (2002), p. 233.

⁴⁶² Ketelaar, Eric, 'Sharing: Collective Memories in Community Archives', Published in: *Archives and Manuscripts* 33 (2005), p. 3.

information on a social media site, an individual would have to carefully consider how he or she would like to be thought of or remembered as this record will be opened to interpretation by anyone that could access it as time passes.

Hence, data protection becomes even more significant when examining the long term implications for the keeping of records and archives. It can serve to protect the dignity and identity of an individual throughout his or her life and beyond his or her existence. A further discussion on personal records as it relates to societal value is undertaken in the section dealing with archives. When private papers are accessioned by the archives, a more detailed and sometimes intimate life story could be reconstructed about the data subject because more than one representation of their activity may exist in a single collection/*fonds*. These representations would indeed be persistent because they are deemed archival and be held indefinitely within the repository. Personal records as 'persistent representations' must be considered vis-à-vis a new principle being developed in the EU data protection regime, that is, 'the right to be forgotten'. This principle emerged as a result of concerns of the capabilities of advancing technologies to create, use and maintain records as well as the concern about the new records being created by individuals about themselves using social media. The 'right to be forgotten' is in conflict with the idea of records as 'persistent representations' because of the capabilities of advancing technology and so this is dealt with in the following chapter.

4.4 Key Records Management Concepts and Data Protection

When the key concepts in records management are analysed, the relationship between data protection and records management becomes even clearer and the synergies that exist between the two pursuits, more apparent. This section reflects on the breaches of the previous chapter on data protection models to show how principles that underpin records management could be incorporated into data protection management. It would also help to assess whether the 'life story' idea is feasible in the established discipline of records management.

The Life-Cycle Concept

A major concept in the field of records management is the 'life-cycle' concept. The idea for this concept was first developed in the US by Theodore Schellenberg who spoke of the 'life-span' of a record in a manner similar to a biological organism.⁴⁶³ The concept states that records are born (created or received), live and get older (used, distributed and maintained) and finally die (final disposition). Records were later said to move through three main stages in their life-cycle from a *current* stage to a *semi-current* stage and finally to *non-current* stage. This progression is usually illustrated in a linear fashion or in a loop or circle.⁴⁶⁴

Although this concept has been challenged and has received serious criticism by records professionals up until the present, the life-cycle concept is widely accepted and in use in established traditional records management programmes around the globe. The concept is mainly useful when dealing with paper-based, manual systems where there is the physical movement of paper records employing manual processes. What is apparent across the jurisdictions is the lack of systematic management of records and information from their

⁴⁶³ Theodore Schellenberg, *Modern Archives: Principles and Techniques* (Chicago, 1956).

⁴⁶⁴ Elizabeth Shephard & Geoffrey Yeo, *Managing Records: A Handbook of Principles and Practice* (London, 2003), pp. 8-12.

creation and receipt until their final disposition. If records management programmes were fully operationalised in the organisations within the selected jurisdictions, many of the breaches could have been avoided. How?

One contemporary version of the 'life-cycle' concept speaks of five major stages, namely the *creation* stage, the *distribution and use* stage, the *storage and maintenance* stage, the *retention and disposition* stage and the *archival preservation* stage.⁴⁶⁵ At each of these stages, records are physically moved from the active space which could be a registry, a records office or office of creation, through to low-cost secondary storage in a records centre where they are appraised for destruction, retained for later review or deemed to have enduring value and sent to an archives repository. Controls for privacy/data protection could be instituted to safeguard personal data found within these organisational records through a well-functioning, purpose-designed records management programme using the life-cycle concept. How could this be accomplished? Below is a look at how data protection management could work within each stage:⁴⁶⁶

- 1) The **Creation** stage (**Identification**) – At this first stage records are created or received, registered, captured, indexed and classified using manual processes or within an electronic document and records management system (EDRMS). Record types that contain personal data should be identified from the outset and classification schemes in which they are placed should be designed to take into account how they should be treated throughout their entire life-cycle. Grouping like record types together in a functional classification scheme is the recommended approach. Further to this, choosing the right classification would be critical to the

⁴⁶⁵ Mary Robek et al, *Information and Records Management: Document-Based Information Systems* 4th Edition (California, 1995), pp. 5, 6.

⁴⁶⁶ Robek et al, pp. 5, 6.

protection of these records. If the records are placed in the wrong classification, particularly in an EDRMS system, this would increase the risks of breaches because they would be subject to the wrong access rights and privileges as well as inaccurate retention and disposition scheduling.

In keeping with data protection principles, records with personal data should be processed fairly and lawfully. This broadly is understood as ensuring that all aspects of upholding the law and protection of the rights of the 'data subject' are upheld. It also means that even the design of the document in which the information is captured should not mislead the user so that the individual knows exactly how that data captured will be used by the 'data controller' and gives consent for any sharing of that information before it is placed in the system. In addition, personal information collected should be adequate for the purpose intended and not excessive.

- 2) The ***Distribution and Use*** stage – This stage is where records are circulated either manually or electronically to those who are required to use them to take necessary action. In an electronic recordkeeping environment, workflow processes may be employed to automatically move records through the established steps in the process to make decisions or to produce an end result. Data protection management is crucial when providing access to records containing personal data at this stage. If the right measures are not employed as it relates to access rights and privileges, the personal information could be accessed by unauthorised persons intentionally or unintentionally and could become subject to unwarranted use as seen in the Canadian breach in the Bank of Montreal and the UK breaches in local councils.

In keeping with the data protection principles, personal information should be accurate and up to date. It is therefore the obligation of the data controllers to ensure that any information in their recordkeeping systems is current and that the information is up-to-date. This may be accomplished by periodically checking the records in the systems that relates to 'living and identifiable' people. Inaccurate information can lead to the organisation impinging on the rights and privileges of a data subject. The organisation will be ineffectual at good decision making when using inaccurate data and this would result in poor management of the affairs of its clients/customers.

- 3) The ***Storage and Maintenance*** stage – At this stage, records are held and stored in paper-based, manual systems such as filing cabinets, shelving or vaults or in searchable databases using EDRM systems. Records containing personal data should be held securely to prevent unwarranted access and use. This may be as simple as locking filing cabinets or placing in safes or vaults. In an electronic environment, the appropriate security levels should be instituted and audit trails showing usage of records made available to key administrators. The provision of security and management of risks to records with personal data is critical to compliance with data protection laws.

The principles of data protection speak to ensuring security measures when maintaining personal data. Another area to be considered is personal information accessed remotely using smartphones, tablets and laptops. Encryption of that data would be useful measure to protect that data in the event of theft. Records with personal data should never be left unattended in any format. Personnel working with these records should be carefully selected and confidentiality agreements

signed as an added measure. This action may have helped to prevent the breach in the US at Marshall University as discussed in the previous chapter. However, note that those who intend to break the law still have the ability to do so even with this best practice in place.

- 4) The ***Retention and Disposition*** stage – This is the stage where through a process of appraisal, the final fate of records are decided. At this stage, records may be retained for a prescribed period for evidential purposes and reviewed later. They may be destroyed because they no longer have any value to the organisation or they may be deemed archival because they inherently have enduring value either for evidential or informational purposes. The establishment of appropriate retention periods and secure destruction of records with personal data is necessary to avoid the risk of data protection breaches. Attention should be paid to how records containing personal information that are no longer valuable to an organisation are disposed of and destroyed. Secure destruction as practiced in records management programmes could have prevented the breach which occurred in Scottish Borders Council with the records found in the recycled bank in the supermarket car park.

In keeping with data protection principles, records containing personal data should not be kept longer than is necessary. This would mean that from the outset, the records management in conjunction with the office of creation should determine how long a record with personal data should be kept in the system based on the stated purpose and intent of the record. The record should not be retained for use for any other purpose without the consent of the data subject. If the records are archival to the organisation and are to be retained for research purposes, further measures have to be taken in order to protect the personal data therein.

5) The **Archival Preservation** stage is the stage where there should be the provision of controlled access to archival records containing personal data. This is further discussed later in this chapter.

The following diagram was designed to illustrate how privacy management could be incorporated into the life-cycle concept.

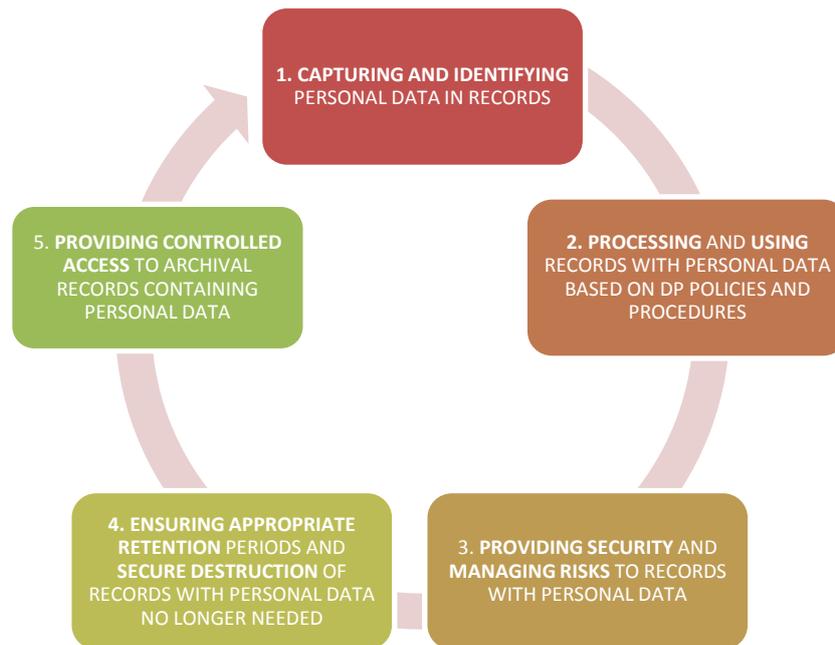


Diagram 4 Life-cycle Management of Data Protection for RM
produced by the author

The Records Continuum

Australian records managers and archivists adopted another concept that was developed by Australian archival educator Frank Upward and further expounded on by Sue McKemmish in the mid-1980s.⁴⁶⁷ This concept is called the ‘Records Continuum Model’. The Continuum model is being used in Australia as a metaphor to getting records management to support environments that are built around electronic communication.⁴⁶⁸ A ‘records continuum’ as defined in the Australian Standard 4390 is ‘a consistent and coherent regime of

⁴⁶⁷ Frank Upward, Modelling the continuum as paradigm shift in recordkeeping and archiving processes, and beyond – a personal reflection, *Records Management Journal*, Vol. 10, No. 3, December 2000, p. 115.

⁴⁶⁸ Upward, p. 116.

management processes from the time of creation of records (and before creation, in the design of recordkeeping systems) through to the preservation and use of records as archives.' This definition suggests an ideal and seamless integration for documents, records and archives management. This model is based on four dimensions supporting an evidence-based approach to the management of records, particularly electronic records.⁴⁶⁹

In the first dimension, the records continuum model identifies accountable acts and creates reliable evidence as a trace of such acts by capturing information about transactions. In the second dimension, recordkeeping systems manage 'families' of transactions and records series. In the third dimension, a seamless recordkeeping scheme embraces the multiple systems and 'families' of records of an entity. The records captured are used to carry out the functions of the organisation but they may simultaneously have archival value to an individual and/or the organisation. In the fourth dimension, a collaborative recordkeeping establishment under the guidance of a suitably empowered public recordkeeping authority serves the needs of the total society. The records have meaning beyond their purpose of creation within an organisation and could represent and preserve societal or collective memory.

The records continuum is about an integrated control.⁴⁷⁰ There is therefore no 'artificial' separation of the stages of 'life' of a record but rather a seamless flow or integration of the purpose and meaning from before a record comes into existence to its final disposition. This view of records existing in multiple contexts concurrently is seen by some practitioners as more realistic than the linear life-cycle concept. How could this concept be related to data

⁴⁶⁹ *An integrated approach to records management: the records continuum model's purpose-oriented approach to records management changes the role of records management changes the role of recordkeeping from reactive to proactive*, *Information Management Journal*, Information Management Journal 3 July 2001. p. 1, p. 2.

⁴⁷⁰ *An integrated approach to records management...*, *Information Management Journal* 3 July 2001, p. 1.

protection/privacy? The following diagram was created based on an original diagram of the Records Continuum concept by Frank Upward to illustrate where data protection concerns arise within the records continuum.

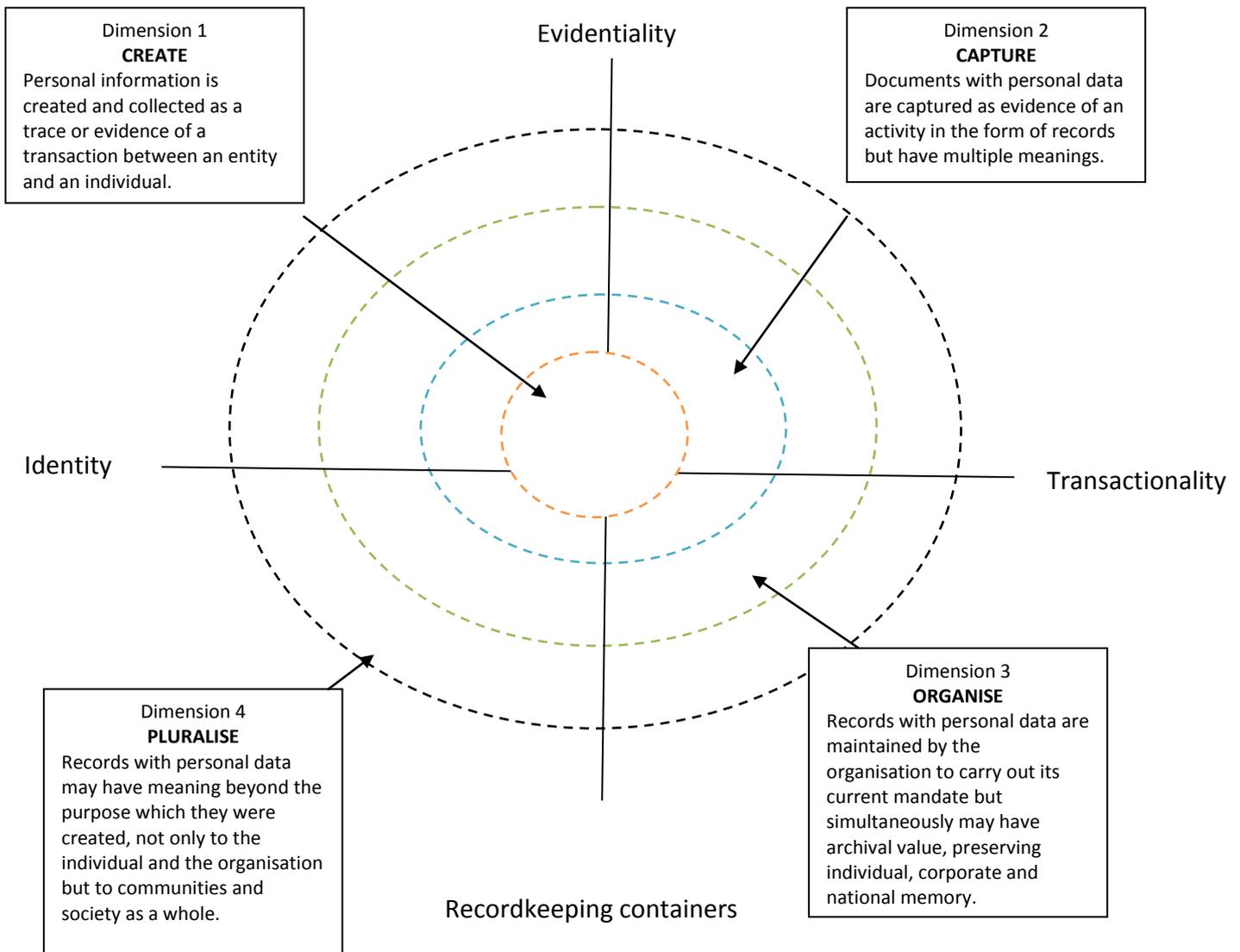


Diagram 5 Frank Upward's Records Continuum and Personal Data
adapted by the author

In using the Records Continuum model to show the relationship to records management and data protection, it is important to note that this model is more a philosophical model than a practical one. It seeks to deal with integrating past, present and future uses of records in the same time/space. It also addresses the role of the records manager vis-a-vis

the archivist. The concept supports a shift in archival practice where rather than waiting until the end of the life-cycle of the record to include the archivist in the process of recordkeeping; archivists are involved from the day of creation because records could be deemed archival even before they are created. Here is how the protection of personal data in records can fit into this approach:

Dimension 1 – In the first dimension, an individual interacts with an entity for a specified purpose and in doing so a trace of evidence is left behind. This trace may take many forms. It could be a paper-based document, an electronic form, a telephone conversation or an image. The transactions between an organisation and an individual (actors) should be clearly identified by the archivist/records manager as these activities would result in the creation of records as by-products. This is particularly critical in an automated environment where individuals may interact with recordkeeping systems directly by filling out an on-line form for submission in an electronic recordkeeping system. The personal information required to carry out processes must not be excessive and the form of the instrument used for capture should be designed to meet legal requirements for data protection. Individuals should know why their information is being collected and give consent for that information to be used for any other purpose if necessary in keeping with privacy/data protection principles.

Dimension 2 – In the second dimension, the trace evidence of the activities of an individual only becomes a record when it is captured and becomes static. All the characteristics of the record must be there for its authenticity and integrity to be irrefutable. Records containing personal information are captured in recordkeeping systems which allows for them to be placed in context and their structure and content are maintained. The archivist/records manager should ensure that these records are placed correctly in a well designed functional classification scheme which should be built with the management of personal data taken

into consideration. Those record types which contain personal data should be grouped together so that the appropriate retentions could be applied.

Dimension 3 – In the third dimension, records are maintained for operational purposes but can simultaneously carry archival meaning to the organisation and/or the individual. Records with personal data reflect the relationship between the organisation and individual clients/customers. The organisation is accountable for how these records are maintained and stored both manually and electronically. They are also responsible for ensuring that these records are secured and safeguarded from unwarranted access to not only protect their integrity but the individual from the abuse of their personal information. Records must be properly organised to show their content, context and structure in this dimension of the continuum.

Dimension 4 – In the fourth dimension the records, which were created for a particular purpose within an organisation, also may simultaneously have meaning for communities or groups and society at large. The provenance of the records should be clear and in the event that the personal data is captured in organisational records, appropriate steps taken to safeguard it when providing access to the wider community who would become privy to the information in an archival repository. A balance must be struck between giving the society what it needs to understand the subject and protecting the privacy of an individual.

Personal Data and the Records Continuum Axes

Evidentiality Axis – The trace of activity of individuals becomes captured as evidence for business use but simultaneously provide a glimpse into the actions, beliefs, values, goals and aspirations of the society at large. This allows for memories to be created and preserved at multiple levels i.e. at an individual level, an institutional level and community level. Hence,

the records can be interpreted and re-interpreted according to the user(s) over time. They would serve to corroborate the life-story of the individual over time.

Transactionality Axis – The purpose of the records containing personal data is multiple in nature. The records were created for business use to fulfil a particular function e.g. a certificate to represent the successful completion by an individual of a course of study at a higher education institution. The records take on new purpose as the function changes from a primary business need to a research need. The certificate reflects the organisation's role in education and more broadly the achievements of individuals collectively within that society.

Recordkeeping Containers Axis – The records containing personal data are maintained within organisational recordkeeping systems for active use but in the 'post-custodial' world, these records are also archival records and access may be given to some aspects of the records in the context of research. This is where controls for data protection/privacy would need to be applied. In the office of creation, only those with the authority to access the records should be permitted access but in the context of archives, strategies to protect the personal data from unauthorised access by communities outside the organisation would need to be employed.

Identity Axis – This is a critical axis when it comes to dealing with personal records. The individual connects with his or her personal records because they reflect and represent their actions and life-story. Yet, there are other identities and/or communities that may be identifiable in the same records. There is the organisation's identity as the creator of the records as they reflect their activities and role in society. There could be collective identities of groups, associates and affiliations of the individual reflected in her or her personal

records e.g. graduation classes, trade unions, political parties and social clubs. These multiple identities exist from the point of creation.

Having a sound understanding of the key RM concepts is the basis on which proper data protection management strategies could be established in RM programmes. The following section will offer a proposal designed by the author and based on observation and experience on how to develop a classification system for managing records containing personal information.

4.5 Developing a Data Protection Classification System for Personal Records

This study asserts that there are four main record types or classifications within a typical organisation that are subject to data protection legislation. These are 1) personnel records 2) client records 3) accounting records and 4) general administration records. In many organisations, these records are being stored in paper-based as well as electronic formats. The methods of storage and use would have implications for the mechanisms chosen to manage informational privacy/data protection.

Personnel Records and Data Protection

Personnel records are those records that contain the principal information about the staff members of an organisation. Personnel records support business needs by providing information necessary to making the best use of the organisation's human resource in the most effective and efficient manner.⁴⁷¹ They also serve to protect the rights and privileges of staff as it relates to payment of salaries, conditions of service, leave, training, promotions and pensions. Personnel records are the most likely records of the organisation to contain the most sensitive personal data and they are subject to informational privacy and data

⁴⁷¹ International Records Management Trust, *A Study Programme: Managing Personnel Records* found at www.irmt.org. Accessed on 2 November 2012.

protection legislation. The personal data that may be found with a single personnel file are as follows:-

- i. Personal details – Name, address, emergency contact details, date of birth, sex, national insurance number, tax information, educational background, qualifications, trade union affiliation, religion, political affiliation and work experience;
- ii. Employment history – details on recruitment, date of employment, promotions, post, job description/job title;
- iii. Terms and conditions of service – Salary, hours of work, leave entitlements, personal health insurance, other benefits e.g. housing, car and entertainment allowances;
- iv. Details on periods of absence – illness (medical certificates and reports), lateness, annual leave, maternity/paternity leave, dependent’s leave and compassionate leave;
- v. Accident reports – Details of work-related accidents; health & safety records
- vi. Training – details on training received and professional development;
- vii. Disciplinary Action – Details on disciplinary action/legal matters;
- viii. Termination of Employment – Details on termination of employment when applicable.⁴⁷²

Across all jurisdictions examined in the study, it was noted that a further effort was made to deal with privacy in personnel records because of their special nature. For example, the US Government under its Government Accountability Office passed a code entitled, ‘Privacy Procedures for Personnel Records’ in accordance with the Federal Privacy Act. The code applies to all Federal agencies.⁴⁷³ Other jurisdictions have similarly sought to specifically address personnel records with policy and procedures in keeping with their national privacy/data protection legislation.

⁴⁷² Adapted from the Advisory, Conciliation and Arbitration Service (ACAS), *Personnel records and recordkeeping* found at www.companieshouse.gov.uk/about/gbhtml/ca_gba3.shtml#two. Accessed on 12 November 2012.

⁴⁷³ US Government, Government Accountability Office, *Privacy Procedures for Personnel Records* found at law.justia.com/cfr/title04/4cfrv1_02.html. Accessed on 9 November 2012.

Records managers may directly or indirectly interact with personnel records, particularly in centralised recordkeeping systems. Usually, personnel records would be administered by officers in human resource sections/departments of an organisation. However, in a centralised system, the records manager, if present, would be the one to design the classification scheme to categorise personnel records under the human resource function and that would enable the right access and security measures to be put in place. In an electronic records management system, series and sub-series could be used to isolate highly sensitive records types, such as medical reports, into their own 'container' or sub-folder, thereby enabling even more sophisticated security, retention and access privileges. Human resource personnel are not fully equipped to design these recordkeeping systems and therefore the records manager should not be excluded from this process. This would be a step towards 'carving out' a role for records management in the protection of privacy.

In decentralised or devolved systems, where personnel records are directly managed by the Human Resource department, records management policies and procedures should still be in place and should be adopted. The involvement of the records manager in the design of the system is still required. This would ensure that privacy/data protection mechanisms are employed to deal with personnel records both in paper-based, manual systems and automated systems.

Client Records and Data Protection

Another related category of records that contain personal data and, in some instances, highly sensitive personal data is client records. The level of sensitivity would be dependent on the nature of the business of the organisation. For example, medical institutions would naturally accumulate large concentrations of sensitive personal data in the form of medical records or 'notes' on each individual patient that include medical history, any procedures

that may have been undertaken and the results. A client record generally contains the most important information about an individual who receives service(s) in some form from a professional, a company or an organisation. It documents the transactions between the client and the professional, company or organisation and may contain all or some of the following information:-

- i. Personal data – Name, address, emergency contact details, date of birth, sex, national insurance number, information for tax purposes;
- ii. Service History – Start of service, type and purpose of service, length of service, other details on service;
- iii. Account Information – Account number, banking information, insurance information (where applicable), billing and payments, credit report;
- iv. Grievances - Details on any complaints from either party;
- v. Results/Outcome - Reports or details on how issues were resolved;
- vi. Termination of Service – Details on the termination of a service.

This study regards *personnel* and *client* records to be at the highest level on the pyramid of privacy protection because of the highly sensitive level of the personal information that is contained therein. In accordance with the privacy/data protection legislation existing in all the reviewed jurisdictions, exceptional attention would need to be paid to how these types of records are treated in both manual and automated systems.

Accounting Records and Data Protection

Accounting records may be defined as those records which contain the principal information about the assets, liabilities and financial transactions of a professional, company or organisation which are required to be kept to disclose the financial position at any point in

time and for auditing purposes.⁴⁷⁴ Many professionals, companies and organisations are creating, distributing and storing accounting records in both paper and electronic form particularly with the use of accounting software packages that enable the implementation of searchable databases. These records are also subject to data protection legislation as they usually contain personal data. There is some overlap between accounting and personnel/client records but these records generally stand alone in recordkeeping systems and may not be linked to personnel/client records. This study regards accounts records at the second tier in the level of privacy protection required. The accounting records subject to data protection include, but are not restricted to⁴⁷⁵:-

- i. Deeds of Covenant/Gifts from Donors
- ii. Legacies
- iii. Payroll/Calculation of Payments/Refunds
- iv. Life Assurance
- v. Correspondence related to contracts
- vi. Records of complaints and investigations
- vii. Deeds of title
- viii. Details re: current pensioners, pension scheme/Expression of wish – next-of-kin
- ix. Claims correspondence
- x. Travel accounts
- xi. Vendor files
- xii. Banking records
- xiii. Forgery & fraud cases

⁴⁷⁴ Companies House, *Accounts and Accounts Referencing Date – GBA Companies Act 2006* found at www.companieshouse.gov.uk/about/gbhtml/ca_gba3.shtml#two. Accessed on 12 November 2012.

⁴⁷⁵ Adapted from Buzzacott, *Retention of Accounting Records* found at www.buzzacott.co.uk/uploads/insights/Buzzacott%20Insight%20Retention%20of%20Account%20UpdateU.pdf. Accessed on 12 November 2012.

- xiv. Trustee/Directors Minutes and Decisions
- xv. Major financial agreements

Any financial record types that would disclose personal information on 'living, identifiable' individuals should be isolated in the recordkeeping system using a well designed classification scheme and retentions applied based on legislation both related to financial records and privacy/data protection regulations within the particular jurisdiction.

General Administrative Records and Data Protection

General administration records contain information about the general management of an organisation and relate to many aspects of the operation and mandate of the organisation. Some general administration records contain personal information about the directors, staff, clients/customers and/or donors. General administration records that may contain personal data include, but are not restricted to⁴⁷⁶:-

- i. Strategic plans
- ii. MOUs and Agreements
- iii. Operational plans
- iv. General correspondence
- v. Special projects
- vi. Records of donors
- vii. Complaints Logs
- viii. Visitors books
- ix. Legal Opinions
- x. Minutes & meeting records
- xi. Policies & procedures documents

⁴⁷⁶ Based on records management experience.

- xii. Requests for information
- xiii. Reports – staffing/annual/audits/management
- xiv. Disaster preparedness & recovery plans
- xv. Incidents & unusual occurrences reports
- xvi. Inspection & security reports
- xvii. Telephone records
- xviii. Postage records
- xix. Permit records
- xx. Key and badge records

There may be several other records types found under general administration that contain small amounts of personal data. It would therefore be prudent for the data controller/processor to ensure that this information is identified so that it may be dealt with using appropriate measures. The following diagram was created to illustrate the hierarchy of levels of protection of records type containing personal information.

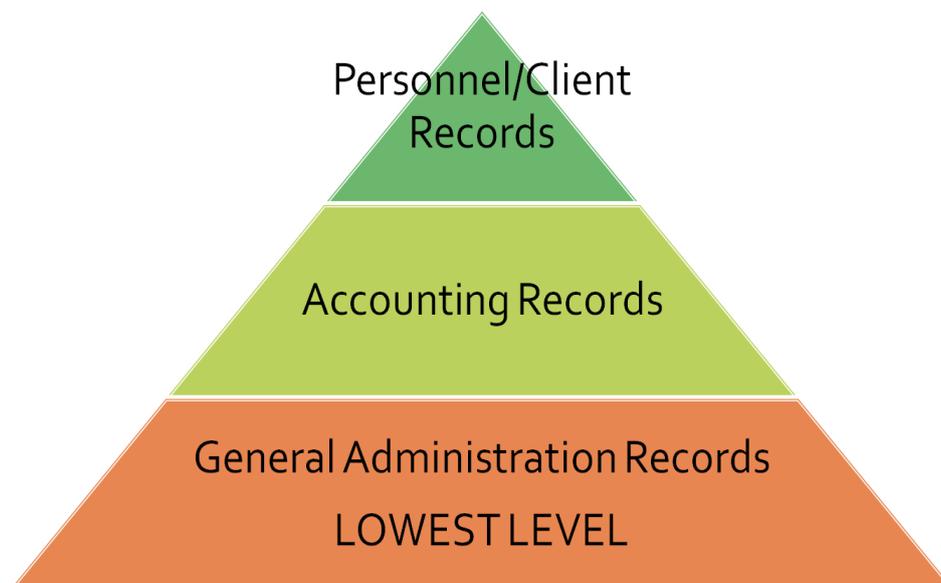


Diagram 6 Levels of Privacy Protection for Organisational Records
produced by the author

The protection of personal data in records within the four broad record categories under review, i.e. personnel, client records, accounting records and general administration records, could be illustrated in a pyramid as seen in Diagram 6. General administration records having the lowest percentage of personal data and are usually the largest amount of records in any given organisation so they are the bottom of the pyramid of data protection. Personnel and client records which contain the highest percentage of personal data and, in many cases, highly sensitive personnel records are at the highest level of privacy/data protection pyramid. Accounting records are at the middle point as they do contain some personal data and at times overlap with personnel and client records. Some of the data found in accounting records may be documented in aggregate i.e. a manner that individuals are not identifiable (anonymised) so that data would not be subject to data protection.

Other Key Considerations

Other concerns that have arisen with privacy and recordkeeping in the workplace relate to the retention and monitoring of telephone records, the capturing of recordings of employees on closed circuit televisions (CCTV), which also relates to bodily privacy, reviewing electronic mail sent by employees from company email accounts as well as web browsing histories. The use of social media to track the activities of employees and clients/customers is now adding a new dimension to the privacy problem and will be explored in the following chapter. In recent times, these actions have resulted in legal action being taken by employees who successfully proved that their privacy was breached.

There have been developments and debates about the use of CCTV surveillance which is employed extensively in the societies under review. Images captured are also forms of records as they provide evidence of activities, even more compelling than written documents. Images are considered to be 'personal information' in privacy/data protection

legislation globally. This type of information also needs to be taken in context to have meaning. If an image is removed from its context, this can 'open the door' to misinterpretation. As seen in the UK and New Zealand, data protection principles apply to the capture and use of images of individuals. Persons must be informed of the presence of CCTV by proper signage. Individuals can request to view an image of themselves unless they have agreed otherwise. Images must be complete, accurate and not excessive i.e. only captured when necessary. The images of individuals as with all personal data can be abused and can lead to harassment and/or embarrassment if not properly managed.

Across the jurisdictions under review, guidelines have been produced to ensure the proper use of CCTV surveillance particularly in workplaces. New Zealand has very clear guidance and a checklist that covers having a clear plan for CCTV and selecting the positions for the cameras.⁴⁷⁷ In Australia, the use of CCTV as a measure for crime prevention is being debated with claims that it may be in contravention of privacy law.⁴⁷⁸ There is cause for concern for privacy advocates as to the intrusiveness of cameras. The UK is recognised as a leader in this area having CCTVs on every high street and many other public areas. There is a code of practice for CCTV use in the UK which is a very comprehensive document which seeks to counteract the abuse of CCTV in public spaces.⁴⁷⁹ However, these guidelines are not legally binding.

Modern cameras have unimaginable capabilities and the most recent development has been to attach cameras to drone flying machines that enable images to be captured in

⁴⁷⁷ Privacy Commissioner of NZ, *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations* found at privacy.org.nz/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations. Accessed on 30 January 2013.

⁴⁷⁸ The Sydney Morning Herald, *Council CCTV Use May Break Privacy Law* found at www.smh.com.au/it-pro/government-it/council-cctv-use-may-break-privacy-law-20121016-27p2r.html. Accessed on 30 January 2013.

⁴⁷⁹ Information Commissioner's Office, *CCTV Code of Practice* found at www.ico.gov.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx. Accessed on 30 January 2013.

positions that were not possible before. Initially, this type of technology was used for military purposes but there is now a market for them to the general public. Google has invested in drone technology to be used for Google Maps, raising more concerns about the loss of privacy.⁴⁸⁰ James Rule in his work, *Privacy in Peril: How We Are Sacrificing A Fundamental Right for Security and Convenience* argues that today's 'advanced' societies need more 'actionable' personal information, that is information deemed reliable enough to carry out decision-making.⁴⁸¹ This has deep implications for the privacy of citizens even within their own homes and has already had legal repercussions globally.

Ultimately, awareness and education will be paramount to ensuring that these forms of records are created, stored and used in keeping with data protection principles. Archivists and records managers must be pro-active as privacy advocates within their organisations and seek to raise awareness about the consequences of unchecked surveillance resulting in personal records.

4.6 Data Protection Terminology Relating to RM

Processing

The term 'processing' has special meaning in the EU model for data protection. That meaning, however, is not clearly defined and has been subject to vast interpretation among EU Member States. *Processing* can be understood to mean that records and information has been captured and stored or that some action is being taken on the records and information containing personal data. The UK Act defines processing as a 'means of obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the

⁴⁸⁰ Geek.com, *Google buys flying camera drone, is Google Maps about to get much clearer?* found at www.geek.com/articles/gadgets/google-buys-flying-camera-drone-is-google-maps-about-to-get-much-clearer-2010089. Accessed on 31 January 2013.

⁴⁸¹ Rule, James, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (Missouri, 1981).

information or data.’⁴⁸² All of these actions to records and information take place when dealing with the management of records within an organisation. Therefore, it naturally follows that records management should be concerned with understanding the parameters of data protection legislation as it relates to the creation, receipt, distribution, use and maintenance of records containing personal data.

One of the issues raised in the previous chapter is the question of whether manual processing of information is less effective for reducing breaches in data protection than automated processing. One of the observations made from the cases of breaches is that in both instances, the human factor is present and the chances of human error occurring in the processing of personal data remains unavoidable. However, further research is required to determine whether the chances of breaches are higher or lower in automated environments. With paper-based, manual systems, errors with personal data being inaccurate or not properly distributed can easily be attributed to the workers. In an automated environment, errors or wrongful access may be external as a result of viruses, poorly designed systems or glitches in the software.

Relevant Filing System – UK Interpretation

Another term relevant to records management is ‘relevant filing system’. This term in the EU context, has been interpreted by the UK DP Act as ‘any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose i.e. a computer. The set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular

⁴⁸² *Data Protection Act 1998* (UK) at www.legislation.gov.uk/ukpga/1998/29/contents.

individual is readily accessible⁴⁸³ This is yet another vague definition which has been controversial and has been affected by court decisions.⁴⁸⁴ It is intended to mean that only those documents from which specific information about individuals can be easily extracted would be subject to data protection. Records managers and archivists therefore would need to assess whether the records and information allow for personal information on individuals to be readily extracted when working in the UK context. For example, if an accumulation of documents in a file about an individual does not allow for a user to readily identify specific information about that individual even if the file has the individual's name on the cover, it would not be subject to UK data protection. However, this interpretation of the EU Directive is not the same across Member States where a more direct approach is upheld. Files with personal data are subject to data protection without the conditions described in UK law.⁴⁸⁵ It means that the records manager must have a clear understanding of term in his or her jurisdiction and how to apply it in practice.

The manner in which records are arranged and classified in a recordkeeping system could enable unauthorised persons to discover personal data. The alphabetic arrangement of records using either a dictionary or encyclopaedic arrangement may be recognisable and easily decoded by a user not familiar with the system. It may be more challenging for an unauthorised person to decode a numeric or alpha-numeric system where subjects such as the names of identifiable person are not apparent by the coding. It may be wiser for archivists and records managers to utilise numeric and alpha-numeric systems when

⁴⁸³ *Data Protection Act 1998* (UK) at www.legislation.gov.uk/ukpga/1998/29/contents.

⁴⁸⁴ See Judgement between Michael John Durant and Financial Authority Case No: B2/2002/2636 at www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf. Accessed on 11 May 2014.

⁴⁸⁵ See German Federal Data Protection Act (BGBI.I 1990 S.2954) which refers to a 'data file' at www.iuscomp.org/gla/statutes/BDSG.htm. Accessed on 11 May 2014.

arranging records with large amounts of personal data such as personnel or client records to reduce the likelihood of breaches by unauthorised persons.

4.7 Records Management Programmes and Data Protection

Organisations through their records management programmes can efficiently and effectively protect themselves and their employees from breaches of privacy/data protection laws. Records management programmes traditionally refer to the systematic management of recorded information held by an organisation and/or business entity. These programmes deal with the total management of records from their creation to final disposition and in doing so they also take into account compliance with any existing legal and regulatory frameworks.

Further to this, records management programmes are designed to ensure that organisations uphold their obligations to their clients/customers and to society at large under themes of transparency and accountability. Therefore, it is the view of this study that records management programmes are rightly placed to balance the efficient operation of an organisation with the protection of the rights and privileges of the individuals that interact with that organisation. This would apply both in the public and private sector. The proper management of privacy/data protection can therefore be tackled using every element of a records management programme that may include all or some of the following components:-

- An active records management programme
- A semi-active records management programme
- A records management training programme
- A disaster preparedness & recovery programme
- A vital records programme

- An archives management programme
- An electronic records management programme
- A micrographics programme
- A records retention & disposition programme
- A forms management programme
- A reprographics programme

The measures that could be employed within some of these components of a records management programme are discussed later in the chapter.

4.8 Developing Policies and Procedures in RM Programmes for Data Protection

Records managers and archivists would need to re-work the policies and procedures that govern their RM programmes to incorporate data protection management. These policies and procedures should be supported by senior management (data controllers) to ensure that they are adhered to by users of the RM systems. They should address the following areas:-

- The legal requirements for privacy/data protection
- Role and responsibilities for privacy/data protection management
- Security of records containing personal data including disaster preparedness & recovery
- Access and reproduction for records containing personal data
- Transfer of records containing personal data
- Retention and destruction of records containing personal data
- Mechanisms for privacy risk assessments and audits
- Mechanisms for handling breaches and complaints regarding data protection

- Training and orientation for staff in data protection requirements for recordkeeping⁴⁸⁶

Procedures which accompany the policies should be in keeping with data protection principles throughout every stage of 'life' of the records.

As was seen in the case studies of the previous chapter, not having clearly written policies could result in careless behaviour or even innocent mistakes due to lack of understanding and awareness. Clearly written policies and procedures would serve as a protection for the organisation as well as its stakeholders from data protection breaches. Policies and procedures should not only be written but properly communicated throughout the organisation. A sound communication strategy should target not only new members of staff via orientation but all levels of all staff. This would ensure that all parties are fully aware of their roles and responsibilities as it relates to privacy/data protection management regardless of the jurisdictions in which they operate.

When developing policies and procedures for data protection management in RM programmes, a checklist of key questions could be asked to ensure that data protection requirements are being met. It would be useful to also use these questions to guide the process of developing the most appropriate measures for safeguarding records containing personal data from identification of records even before they are created to their final disposition. The questions are presented in Table 5 which was produced by the author.

⁴⁸⁶ Based on interviews with Records Managers in the UK context.

Forms Management/Records Creation

- What personal data is being requested and why?
- Is the information requested appropriate for the purpose (fair and lawful)?
- What types of records would result from this process?
- Will this information be useful for another purpose?
- Has a fair processing statement been included in the form?

Records Capture

- Will this information be captured in a paper-based or electronic form?
- Which offices would need to interact with this information after it is captured?
- Who is the official owner of this record?
- Is the information accurate and up-to-date?

Records Classification

- Which functional area uses these records?
- Which series/sub-series should these records be placed in order to be subject to the right access/security privileges and retention period?

Records Storage

- In what format should the records be stored?
- If electronically, is there a robust audit trail in the system?
- Who has administrator rights to audit trails?
- Is there an established procedure to deal with access and security?
- What strategies will be used for migration, back-up, disaster preparedness and recovery of records containing personal data?
- If information is transferred to a third party, is there an appropriate contract in place to protect records containing personal information?

Records Use

- How will the records be transmitted/distributed?
- Which officers in particular need to access the records to carry out their function?
- What mechanisms will be employed to protect personal information in the records from unauthorised access internally and externally?

Records Disposition

- How long should records containing personal data be retained to meet data protection requirements?
- What methods of transfer will be used to safeguard records with personal data?
- What methods of destruction will be used?
- Who will manage this process?

Archival Preservation

- Which records containing personal data have enduring value to the organisation and society at large?
- How will personal data be safeguarded when access is provided to a record? (e.g. under a Freedom of Information (Fol) request)
- Is written consent sought to open records for research?
- Should the record be kept closed to prevent breaches in data protection?

Table 5 Checklist to meet Data Protection Requirements in RM Programmes
produced by the author

This table shows a high level checklist for establishing data protection management in records management programme. These questions should be asked as the first step to implementing data protection at the higher levels of records classification schemes. The suggestion here is to use this checklist to categorise records at series and sub-series level as subject to data protection. It is recommended that implementation should start from the general to specific; in other words, from the top downwards. However, to ensure that there are absolutely no breaches, as a second step, records must also be examined and classified at the lower levels, that is, at file and document level.

4.9 Key Data Protection Measures in RM Programmes

There are tangible and practical solutions to the informational privacy problem that should be undertaken as part of a viable records management programme. Many of these solutions require the skill set of trained and experienced archivists and records managers to be successfully carried out. However, it is important that archivists and records managers do not work in isolation of other professionals and stakeholders. The legal and IT professionals in particular would assist records professionals with making these measures sure-footed and 'fool proof'. Some of these measures are already in use in organisations visited and observed by the author. However, the recommendation here is that all of these measures should be employed in tandem within the same organisation for maximum effectiveness. The measure introduced for the first time by this study is highlighted. The recommended measures are as follows:-

a) Inclusion of Fair Processing Statements/Notices – In keeping with the principle in data protection legislation that states that personal data should be processed fairly and lawfully, it is important that at the stage of records creation, data controllers/processors provide a fair processing statement or notice to the data subject. This statement will serve to inform

individuals of the intent behind the use of their personal information and the organisation's commitment to ensuring that any personal data collected is treated fairly and lawfully.⁴⁸⁷

b) Purpose-built Classification Schemes - Records managers should seek to arrange records to facilitate quick retrieval and comprehensive control of records containing personal data by designing sound classification schemes. Classification schemes should therefore be used as the foundation on which data protection strategies are built by grouping record series containing personal data in logical, functional categories. This would enable the right controls to access and security to be assigned at records series level across all functional areas as well as the implementation of appropriate retention periods that comply with data protection legislation.⁴⁸⁸ This idea has been discussed in Chapter 4.⁴⁸⁹

c) Privacy Risks Assessment Survey for Records – Records managers should carry out regularised privacy risks assessment surveys for records throughout the organisation. These surveys would enable a thorough assessment of the risks to recordkeeping systems which hold records containing personal data. It would help to determine the effectiveness of measures put in place to prevent breaches in these systems. After which improvements could be made that would address weaknesses and failures.⁴⁹⁰

⁴⁸⁷ See sample *Student Fair Processing Notice* from the Institute of Education in London, UK at www.ioe.ac.uk/about/documents/About_Policies/Data_Protection_for_Students.pdf. Accessed on 13 September 2014.

⁴⁸⁸ This recommendation requires testing as a pilot project in an organisation for a final conclusion to be drawn. The author is currently conducting a pilot within her Higher Education Institution, The University of the West Indies, Cave Hill Campus, Barbados in the Archives and Records Management Programme and has agreed to assist the Gallery Records Manager at Tate Britain in London with a similar project. The results will be published as future work.

⁴⁸⁹ See pp. 232 for classification schema with data protection management.

⁴⁹⁰ See sample *Privacy Risk Assessment Questionnaire* from American institute of Certified Public Accountants at www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/PrivacyServices/Pages/Privacy%20Risk%20Assessment%20Questionnaire.aspx?action=print. Accessed on 13 September 2014.

d) Establishing Robust Audit Trails – Audit trails should be established to track the movement of records both in paper-based and electronic systems. This would involve the capture of metadata that would show who saw the record; who modified the record; on what date was the record accessed; who printed the record; who removed the record from the system or who attempted to destroy, alter or illegally export personal data from the record (electronic).⁴⁹¹

e) Conducting Regularised Audits – Records managers should carry out regularised audits of the records and the recordkeeping system(s). This is part of monitoring and evaluating the effectiveness of the records management programme in general but allows them to keep track of the need for changes and improvements to ensure compliance with all legal requirements. It also means conducting checks of the records themselves to ensure that information recorded in them is accurate and there is no duplication of that information in multiple forms in the recordkeeping system. Records managers will also be able to determine where new approaches to dealing with concerns such as privacy could be developed.

f) Developing a Security Matrix/Access Control Matrix – Developing an ‘air-tight’ security matrix also known as an access control matrix is critical to the protection of records containing a personal data particularly in electronic document and records management systems (EDRMS). Records managers need to map the use of records in the system throughout every work group in the organisation and give the right security clearance to only those officers in the workflow processes who are authorised to access the records containing personal data. In the paper world, it would be as simple as ensuring that only

⁴⁹¹ See publication on *Audit Trails* from US Department of Commerce Computer Security Division at csrc.nist.gov/publications/nistbul/itl97-03.txt. Accessed on 13 September 2014.

authorised individuals have the keys to filing cabinets or vaults with records containing personal data.⁴⁹²

g) Using Redaction Methods – The use of redaction can allow sensitive information to be visually blocked from unauthorised persons while enabling them to view requested information. Software programmes are utilised to carry out this task with electronic documents. In the traditional paper world, when supplying 'hard-copy' data, the records manager would need to manually cross out or in some way darken personal information on any data subject to data protection before supplying it to the requester.⁴⁹³

h) Using Aggregate Data – Aggregate data can be derived from a process of taking different elements of information from different sources to create a summary form of data. This method of using data is a good strategy to protect personal data as the data is anonymised. Aggregate data is good for research into trends over time and should be used wherever possible.⁴⁹⁴

i) Anonymisation and Pseudonymisation – The anonymisation of data more specifically refers to the rendering of information in a form that individuals are no longer identifiable and is an effective strategy in avoiding the risk of inappropriate disclosure. Pseudonymisation is a concept where the name of an individual is replaced by pseudonyms or an artificial identifier to prevent an individual from being singled out. This strategy is being favoured in the EU model. One must also seek to manage the risk of *re-identification*

⁴⁹² See publication on *Assessment of Access Control Systems* from US Department of Commerce, National Institute of Standards and Technology at csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf. Accessed on 13 September 2014.

⁴⁹³ See sample redaction software from Oracle at docs.oracle.com/database/121/ASOAG/redaction.htm#ASOAG594. Accessed on 13 September 2014.

⁴⁹⁴ Aggregate data is further explained by Geek Interview on *Aggregate Data* at www.learn.geekinterview.com/data-warehouse/data-types/aggregate-data.html. Accessed on 13 September 2014.

where anonymised or pseudonymised data could be used to re-establish the real identity of an individual particularly in web environments.⁴⁹⁵

j) Use of Encryption – The use of encryption as a security measure to protect sensitive data is highly recommended when storing records containing personal data electronically. Encryption scrambles data into a form that is unreadable to unauthorised users of the system. It is particularly useful when using portable devices to access data remotely in the event of theft.⁴⁹⁶

k) Training and Orientation of Staff – Training and orientation of staff in records programmes is absolutely crucial to maintaining a well ordered, well-functioning enterprise-wide programme. Records managers should incorporate training and awareness about data protection legislation and policies and procedures in the training programmes for staff at all levels. This could be undertaken through collaboration with HR through induction programmes or by routine awareness seminars conducted by the records manager on a group by group basis. The importance of training cannot be over emphasised when seeking to protect personal data created, received, distributed and maintained by the organisation.⁴⁹⁷

The measures provided here are meant to be preventive. The most effective way to deal with privacy/data protection is to take pro-active steps to combat the risks of breaches in the organisation. Records managers should not wait to be guided by other professionals in

⁴⁹⁵ The measures of Anonymisation and Pseudonymisation are relatively new and are being explored in the EU regime. The impact of these measures require further research over a long term period as it relates to preserving the integrity of records and information.

⁴⁹⁶ Encryption is further explained by Symantec article, *Introduction to Encryption* at www.symantec.com/connect/articles/introduction-encryption. Accessed on 13 September 2014.

⁴⁹⁷ The author will be working in conjunction with ARMA International, a professional association for records managers and archivists, to design and produce training materials for practicing records managers and archivists. She is currently part of a standards group of ARMA International designing an international standard on private information for records managers worldwide (August 2014).

dealing with privacy in recordkeeping systems but seek to use their inherent understanding of these systems to devise a plan to deal with privacy/data protection.

I) Roles and Responsibilities for Data Protection

Another area that should be addressed is identifying who in the organisation should be responsible for data protection. In fact, there are stakeholders in the organisation that should be directly involved in the management of data protection. It is recommended that representation from Human Resources Management departments, IT and Legal departments should be included in the pursuit of sound data protection. Each of these professionals has valuable skills and knowledge, which may include institutional memory that could assist with the development of strategies and measures to deal with the management of data protection. However, it is also recommended that one high-level officer be designated to coordinate and oversee data protection management. Managing data protection is a very time consuming and labour intensive job. This was evident based on interviews conducted with data protection and compliance officers in a variety of organisations. However, the question may arise as to whom is best in the organisation to carry out this function.

The post, under the EU model, is usually referred to as the Data Protection Officer. In some jurisdictions, it is referred to as the Data Privacy Officer. In Australia, many references are made to records keepers in the Information Privacy Principles (IPPs) in the legislation which gives explicit instructions to record-keepers in the organisation regarding their role and responsibility in informational privacy management.⁴⁹⁸ The UK has been the most forward thinking in defining a clear role for archivists and records managers having formulated a

⁴⁹⁸ Australian Government, *Privacy Act 1988* (Current) found at www.comlaw.gov.au/Details/C2012C00414. Accessed on 13 December 2012.

Code of Practice for Archivists and Records Managers under the Data Protection Act of 1998.⁴⁹⁹ We have also seen globally the proliferation of Privacy Officers and Compliance Officers who have been hired to take on this responsibility.⁵⁰⁰ Other organisations refer these matters to their legal counsel when a problem arises.

This study asserts that records professionals such as archivists and records managers should be considered best placed to coordinate data protection management because of their combined knowledge of 1) the organisational structure 2) the organisation's culture 3) workflow processes 4) regulatory frameworks 5) background and administrative history of the organisation 6) the mission and vision of the organisation 7) what are the official records of the organisation 8) how the organisation's recordkeeping systems work 9) how to design classification schemes and retention schedules and 10) the informational needs of the organisation over time.

Although legal professionals traditionally have dealt with privacy matters in the organisations globally, they do not possess the range of knowledge about the informational assets of the organisation like the archivist and/or records manager. It may be best to establish a team of the key stakeholders that would consult and collaborate on data protection but someone has to coordinate the effort and take a leading role in the development of strategies. In cases where another professional is designated for this role, it is crucial that he or she liaises with the organisation's archivist/records manager as well as other stakeholders when designing enterprise-wide policies and procedures for data protection.

⁴⁹⁹ The National Archives, *Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998* found at www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf. Accessed on 12 December 2012.

⁵⁰⁰ International Association of Privacy Professionals found at <https://www.privacyassociation.org>.

The UK Code of Practice offers some good insight into the role and responsibilities for archivists and records managers as it relates to data protection. The Code's introduction clearly states that archivists and records managers need to understand data protection to ensure that their handling of information complies with the Act. The Code provides sound guidance for practicing archivists and records managers and in some areas is highly prescriptive. The guidelines for records managers deal with the acquisition and processing of personal data; the development of records management policies, procedures and systems; records centre operations; inventorying personal data systems; maintaining accuracy of personal data; dealing with data subjects access to personal data and the transfer of personal data outside of the European Economic Area (EEA). Guidelines for archivists⁵⁰¹ also relate to the acquisition and processing of data but this is distinct from records management; dealing with records appraisal; accessioning of archival records; inventorying personal data systems; maintaining accuracy of personal data; data subject access to personal data; third party access to personal data; compiling finding aids for archival materials with personal data; the business use of archives; the security of personal data and the transfer of personal data outside the EEA.

However, given the dynamics of the Act which is ever evolving and the impact of rapidly advancing technology on recordkeeping, it would be wise for archivists and records managers to continually keep abreast of any changes in the Act itself that would affect recordkeeping. A code of practice is not mandatory and unlike the Australian situation where the instructions are built directly into the law in the form of IPPs, UK archivists and records managers are not obliged to follow the guidance in the code. Yet, a clearly written code is a useful tool and would assist archivists and records managers in understanding key

⁵⁰¹ The National Archives, *Code of practice for archivist and records manager under Section 51(4) of the Data Protection Act 1998* (Surrey, 2007), p. 4.

terminology as well as other aspects of the law that may be complex. The best approach to providing a code of practice is to continually review and monitor the need for changes to keep it relevant and up-to-date. Given the rapidly changing environment, a review and update should be undertaken every five years.

One of the arguments of this thesis is that archivists and records management have been engaging in activity from the beginning of their profession that is now being incorporated in data protection management programmes. This area of responsibility is therefore not at all foreign to the discipline of records and archives management and should be seen as complementary to the work already being undertaken in RM and archives programmes. Hence, the exclusion of these professionals in the quest to protect data of all kinds would be a 'backward step' for an organisation. Senior management should seek to have meaningful discussions with the records and archives management team before deciding on the best compliance strategy for managing data protection.

The cost of compliance also has to be given some consideration. There are resources required when seeking to implement data protection management. The organisation would need to evaluate whether its existing structure could accommodate the measures as discussed in this Chapter. The resources needed include staffing, hardware and software. It may also include employing experts for the implementation process, change management and training along with training/promotional materials. However, the benefits of instituting a strategy for data protection compliance outweigh the initial investment because of the nature of the issue. These measures serve to protect lives and so every individual in the organisation will benefit from well designed systems to safeguard personal information.

4.10 Data Protection and Archival Administration

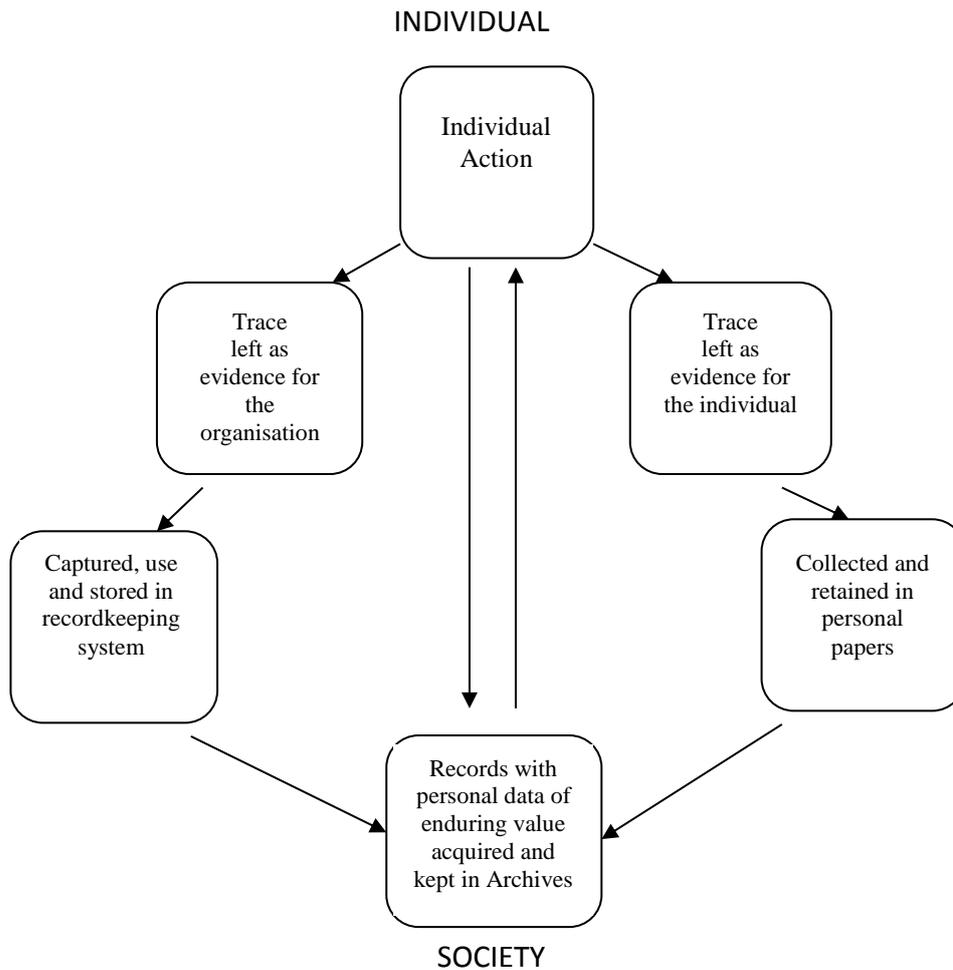


Diagram 7 The Passage of Recorded Personal Data into the Archives
produced by the author

Ultimately, newer theories on recordkeeping recognise that there must be less focus on the physical record and more focus on the context, purpose, intent, interrelationships, functionality and accountability of the records and their processes of creation.⁵⁰² A broader view of the meaning of records and archives has been developed. A closer look at the interaction between the citizen and the state and the impact of the actions of the state and also of private enterprise on society is being undertaken. This interaction is illustrated in the preceding diagram. It is in the Archives that this relationship is pronounced as a result of the research that is carried out therein. Records are no longer just tools for administration but

⁵⁰² Terry Cook, *What is Past is Prologue: A History of Archival Ideas Since 1898 and the Future Paradigm Shift*, *Achivaria*, Association of Canadian Archivists 43 (Spring 97).

represent the fundamental nature of society. Archives have been described as ‘of the people, for the people and by the people.’ How can information ‘about the people’ be protected within the research driven environment of the Archives?

Records managers may have an immediate concern with data protection because they deal with active and semi-active records which contain personal information on ‘living, identifiable individuals’. However, archivists need to be concerned with data protection because they may inherit records with personal information on people that are still alive.⁵⁰³

Archival records, which are records of enduring administrative, legal, fiscal, cultural, historical and intrinsic value, represent the fundamental nature of a society and serve to provide glimpses into the past and lessons for future generations. Archivists are required to do ‘a balancing act’, assisting researchers while protecting individual privacy.⁵⁰⁴ Archivists are for all intents and purposes the ‘guardians’ of valuable evidence and information in records and ‘knowledge providers’ for current and future research. Archivists are charged with preserving the characteristics of society, both good and bad, in order to assist researchers with understanding the why, what, when and how. It is important that their core function is not forgotten when looking at the issue of data protection.

Diagram 7 illustrates the passage of recorded personal data into the archives which begins as a result of individual action. A person interacts with an organisation as part of a process and leaves behind evidence of that activity. The evidence is captured in the form of a record which is used and maintained in an organisation’s recordkeeping system and is also collected and retained by the individual. Archival institutions may acquire material with

⁵⁰³ The National Archives, *Code of practice for archivists and records manager under Section 51(4) of the Data Protection Act 1998* (Surrey: 2007), p. 3-4.

⁵⁰⁴ Judith Schwarz, *The Archivist’s Balancing Act: Helping Researchers While Protecting Individual Privacy, Privacy and Confidentiality* ed. Menzi Bernd-Klodt, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005), p. 82.

personal data from both sources. Records with personal data may be transferred to the Archives as part of an established retention schedule in a records management programme or from an individual by way of deed, gift or purchase. What steps then should archivists take in dealing with data protection in archival records or historical papers?

Researchers increasingly demand unrestricted access to records and have high expectations of what archivists should allow them to view in pursuit of novel and undisclosed information. Personal information contained within archival records, particularly in the case of prominent personalities within society, holds a very strong appeal to the average researcher. Archivists therefore must examine their policies and procedures to ensure that this type of information is protected. They must also review key archival processes and incorporate sound data protection strategies to deal with data protection management.

The societal role of the archives and archival records have been debated and discussed in the writings of modern archives theorists including Hans Booms,⁵⁰⁵ Eric Ketelaar,⁵⁰⁶ Randall Jimerson⁵⁰⁷ and Terry Cook⁵⁰⁸. All agree that archives are there to serve the needs of society as guardians of collective memory and the human experience. Archives have been said to be of the people, by the people and for the people. The theorists also recognise that archivists have to balance a complex set of activities in order to best serve the societies in which they operate.

There are three main areas that archivists should pay close attention to when seeking to comply with data protection: appraisal, accessioning and providing access. The act of

⁵⁰⁵ Hans Booms, Hermina Joldersma and Richard Klumpenhower, 'Society and the Formation of a Documentary Heritage: Issues in the Appraisal of Archival Sources', *Achivaria* 24 (Summer, 1987).

⁵⁰⁶ Eric Ketelaar, 'Archival Temples, Archival Prisons: Modes of Power and Protection', *Archival Science* (2002).

⁵⁰⁷ Randall Jimerson, 'Archives Power: Memory, Accountability, and Social Justice', *Archival Science Commons* (Chicago, 2009).

⁵⁰⁸ Terry Cook, 'What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm', *Achivaria* 43 (Spring, 1997).

appraisal has been recognised as one of the most powerful acts of the archival profession. Appraisal can be described as the process of identifying records and materials to determine whether they have sufficient archival value to be acquired and accessioned. The selection process is not a scientific one and very weighty decisions have to be made as it relates to choosing the records that would best serve the needs of society now and in the future. A critical part of the process is that archivists consult with record creators in the case of 'living' organisations to gather background information on the administrative history, organisational structure and use of records to inform their appraisal decisions. Archivists would then need to carefully review records containing personal data bearing in mind that these records with their life-stories may be key to providing solutions to societal problems over time. Further to this, archivists should be accountable for their actions as it relates to how they treat and make accessible records to stakeholders and the society at large. In societies where there are National Archives Advisory Boards or Councils, with representation from various interest groups within society, the actions of archivists should be well documented, communicated and supported by these stakeholders. In the absence of Advisory Boards and Councils, archivists should keep good records of their appraisal decisions. Accessioning is the process of physically and legally taking custody of records and materials into an archival repository. Access is the ability to retrieve archival records and materials through the creation and use of finding aids, indexes and other tools.⁵⁰⁹ Archivists would need to ensure that the conditions of deposit and other legal requirements are clearly documented and understood by the depositor, the researcher and themselves as it relates to how personal data therein should be treated. Table 6 would assist archivists with putting data protection requirements into these day-to-day processes.

⁵⁰⁹ Society of American Archivists, *Glossary of Archival and Records Terminology* found at <http://www2.archivists.org/glossary>. Accessed on 11 February 2013.

Appraisal	<ul style="list-style-type: none"> - Identify records containing personal data - Establish provenance - Identify what research interests could be satisfied by records containing personal data based on archival values
Accessioning	<ul style="list-style-type: none"> - Document details on the conditions of deposit as it relates to any access and reproduction restrictions on records containing personal data - Find out the time limits placed on restricted materials containing the personal data of 'living, identifiable' individuals - Isolate restricted materials intellectually, without disturbing 'original order' wherever possible
Access	<ul style="list-style-type: none"> - Institute formal guidelines for access to records containing personal data in Access Policies - Arrange and describe records containing personal information in a manner which makes them clearly identifiable - Provide clearly written finding aids with statements on any restrictions on the materials - Defend decisions to close materials on the basis of the existing legislation - Provide clear data protection guidance to researchers even placing a copy of the legislation in the search Room area - Design declaration forms for users of material containing data protection statements - Carefully post any materials containing personal data on websites and databases employing measures such as redaction and encryption wherever necessary - Find out whether there are any legal restrictions when responding to queries outside your jurisdiction

Table 6 Activity Table for Archivists dealing with Data Protection
produced by the author

The protection of personal data is even more challenging in an archive as the institution will inherit or receive a cross section of record-types that may contain varying degrees of

personal data. This would mean that from the early stage of appraisal of the records, the archivist must closely examine and identify which records would be subject to the data protection legislation. On the positive side, as data protection only covers 'living, identifiable' people, this would narrow the window of time that would be of concern to about one hundred years. As it relates to data protection, the archivist would then have to focus on the records less than about one hundred years old to identify data subjects. On the negative side, because of the nature of personal data as so pervasive, colonising particularly private papers, the archivist would have to examine records at 'item level' in order to ensure that personal data is not missed and unauthorised access provided to researchers. It may not be practical for archivists to carry out this task at the stage of processing but it would have to be dealt with on a 'request-by-request' basis when providing reference services. Then the right mechanisms can be employed to protect personal data. Some attempt should still be made to address the issue even at the stage of arrangement and description so as to not mislead researchers into thinking they could have full access to the information.

The UK DP Act, as well as other legislation globally, speaks to 'research exemptions' which allow for archival repositories to retain records containing personal data indefinitely for research purposes under 'the relevant conditions' (UK).⁵¹⁰ 'The relevant conditions' relate to the data not being processed in a way that would cause harm or distress to a living individual. However, it should be clear that the principles of data protection as set out in the legislation still would apply in archival administration and should not be taken for granted or ignored. Archivists in general have a wider role to play within society. They go beyond an administrative function as keepers of societal memory. In training, archivists must be made

⁵¹⁰ *Data Protection Act 1998* (UK) Section IV at www.legislation.gov.uk/ukpga/1998/29/contents.

aware that information found in private papers is equally important to the future advancement of society and therefore should be made accessible wherever possible to those who need it. In recent times, there has been a thrust towards 'community archives' and this endeavour results in bringing in even more records containing personal data in the form of oral history interviews and similar personal accounts into the archives to complement existing holding and fill in the gaps. Avoidance of the issue of data protection is not an option. There is indeed a conflict of interest in society's need to access information and the 'right to privacy' that the archivist must consistently navigate.

Even with the best design policies, procedures and guidelines, archivists will face pressures from interest groups who study sensitive subjects, such as political victimisation, gay or lesbian rights or gender and sexuality, to provide access to undisclosed personal data. Sound judgement will be needed to avoid breaches.

The issue of evidence of accountability of the archivist also comes to the fore. The balance between protecting the individual's right to privacy and providing tomorrow's society with the information it requires to deal with sensitive topics is a delicate balance. If one accepts that archives have a wider societal value and the absence or inability to see information can hinder the advancement of society, the decisions that archivists make today, even in the face of current data protection legislation, require intense consideration. As the meaning of privacy changes, the legislation will change and archivists would need to think beyond the immediate context. Personal information stored in archival repositories may become unlocked in the face of changing legislation. The legislation will also remain steps behind the technology and the way how people use and access information will constantly be altered particularly in a digital world. Aspects of how these technological changes will impact recordkeeping and archives will be discussed in the following chapter.

4.11 Conclusion

This chapter has provided a new concept for the identification of personal records; shown how data protection management could be firmly incorporated into records management principles; discussed how a records management programme could have prevented the breaches such as those described in Chapter 2; proposed a hierarchy of privacy protection for organisational records; stated the types of records that could be subject to data protection by functional area; shown how data protection affects archival records; discussed roles and responsibilities for data protection management and recommended mechanisms for data protection management in records management programmes.

Records containing personal data form a significant part of any organisation's information assets. Records managers/archivists are often at the heart of the organisation as it relates to how its informational assets are managed. Safeguarding of records and information has always been at the centre of the work done by these records practitioners. However, in the changing compliance landscape records practitioners need to realise that their role has become weightier than before and seek to re-examine and re-think their formulation of policies and procedures bearing in mind the requirements of data protection principles. The legislation on data protection will always lag behind the technology used to create, distribute and store records. However, a sound records management programme with all the elements and measures discussed in this chapter should enable an organisation to stay ahead of the ever-changing legislation. Records practitioners should take whatever steps are necessary in their programmes to ensure the physical and intellectual security of the records containing personal data.

One definition for records management states that it is 'the systematic application of scientific controls on recorded information required in the operation of an organisation's business'.⁵¹¹ Records management, therefore, is concerned with ensuring that organisational information is timely, accessible, accurate, authentic, usable and complete. Records management is the only professional discipline concerned with an organisation's total information resources. A broader view of records management states that its main objectives of records management are based on 1) service 2) profit or cost-avoidance and 3) social responsibility.⁵¹² Privacy and data protection as a public policy fit naturally into the social responsibility aspect of records management. This aspect relates to the attainment of organisational goals in accordance with moral, ethical and legal codes of the society in which the organisation operates. The objective would be to ensure that privacy/data protection as a human right and legal provision is respected and complied with by records managers and archivists in the management of the information assets within their care.

Since the 1950s, records management has been acknowledged as a profession and scholarly pursuit. In recent times, key principles in the regulation of privacy/data protection and related information rights legislation, such as freedom of information, became integral to records management and in doing so result in protecting the organisation from breaches within the compliance environment. Data protection is humanistic in its scope as its main objective is to protect individuals from harm, inconvenience, embarrassment, and/or unfairness by safeguarding the confidentiality and integrity of personal data contained within records through regulation and mechanisms.⁵¹³ Whilst records management focuses closely on business processes within an organisation the overall result of protecting the

⁵¹¹ Mary Robek et al, *Information and Records Management: Document-Based Information Systems* 4th Edition (California, 1995), p.5.

⁵¹² Mary Robek, (California, 1995), p. 5.

⁵¹³ Ricks, Swafford & Gow, *Information and Image Management: A Records Systems Approach* (Ohio, 1992), p. 478.

personal data contained within the records of internal and external customers of the organisation is to the benefit of the people who interact with the organisation on a very personal level.

Organisations that institute total records management programmes put measures in place that incorporate the main principles of data protection into their recordkeeping systems.

Ricks, Swafford & Gow in their text, *Information and Image Management: A Records Systems Approach*, demonstrated how a well established records management programme guarantees the right conditions for privacy/data protection.⁵¹⁴

- 1) **Openness.** There is a policy of openness about the organisation's personal recordkeeping policies, practices, and systems; there are no secret systems.
- 2) **Individual access.** An individual about whom information is collected and maintained by the organisation in individually identifiable form should have the right to see and copy that information.
- 3) **Individual participation.** An individual should have the right to amend or correct the substance of the personal information maintained by the organisation.
- 4) **Collection limitation.** Internal collection of personal information should be limited to necessary information.
- 5) **Use limitation.** Internal uses of personal information should be limited to those who have a need to know.
- 6) **Disclosure limitation.** External disclosures of personal information should be limited.
- 7) **Information management.** The recordkeeping organisation should bear affirmative responsibility for establishing reasonable and proper information management policies and practices to assure that its collection, maintenance, use and dissemination of information about an individual are necessary and lawful and that the information itself is current and accurate.
- 8) **Accountability.** A recordkeeping organisation should be accountable for its personal recordkeeping policies, practices and systems.

⁵¹⁴ Ricks, Swafford & Gow, (Ohio, 1992), p 478.

It is clear from the above that data protection principles were present in records management programmes before they were explicitly set out by legislation. Yet, the issue privacy/data protection has not been comprehensively addressed in the discipline of records management. This study therefore represents the first attempt to bring all the elements together in a comprehensive way.

In the last ten years, there has been a shift in focus in the discipline of records management to risk management as a result of the highly litigious environments in which organisations, both public and private, operate globally. This is evidenced by the previous chapter which highlighted the result of breaches in data protection alone. There have been other scandals that have rocked the business world internationally such as the Enron debacle⁵¹⁵ that have brought about sweeping changes in the perception of records management and a new interest in the impact of law on records management and archival administration. Understanding the legal provisions that exist is the only way to ensure compliance and protect records managers and their organisations from the risk of breaches.

Further to this is the concept that records management fall under the umbrella of risk management. Risk management for records is still in its infancy in development as a broad concept. It however provides a basis for the relationship between records management and data protection. Victoria Lemieux in her study *Managing Risks for Records and Information* asserts that records and information underpin every business transaction in the organisation and that any risk to the adequacy of records and information poses a threat to the effectiveness of the organisation with regard to the fulfilment of its objectives.⁵¹⁶

⁵¹⁵ The Enron scandal of 2001 resulted in the collapse of America's seventh largest company which lied about its profits as well as falsified and concealed information, including records containing personal information on its investors, politicians and employees, even shredding records during an investigation into its state of affairs.

⁵¹⁶ Victoria Lemieux, *Managing Risks for Records and Information* (Kansas, 2004), p. 2.

Lemieux describes records and information risk management as the management of any risk to the business arising from some inadequacy in an organisation's records and information.⁵¹⁷ Implicitly, it can be reasoned using this concept that the risk of non-compliance with data protection principles could inhibit an organisation's effectiveness as well as result in legal ramifications that could have devastating effects on the organisation. Recordkeeping debacles with major companies such as Arthur Andersen and Enron prove that inattention to records accountability issues can be disastrous.

Ultimately, the main activities for RM practitioners in regulating privacy/data protection may be summed up in the following three points:-

1. Ensuring that data protection responsibilities are clearly identified and assigned.
2. Providing records and archives management services with clearly written policies and procedures that define how personal data are to be processed.
3. Ensuring that when obtaining personal information, their methods of collection, storage, destruction and provision of access complies with data protection legislation.

Guarding personal data is not only a legal issue for RM practitioners but also an ethical one. The *Code of Professional Responsibility for Records Management* as developed by ARMA International states that 'records and information managers [should] affirm that the collection, maintenance, distribution and use of information about individuals is a privilege in trust: the right to privacy of all individuals must be both promoted and upheld.'⁵¹⁸ The International Council of Archives in its *Code of Ethics* for archivists states, 'archivists should respect both access and privacy, and act within the boundaries of relevant legislation'.⁵¹⁹ Hence, the responsibility of the RM practitioner to understand privacy legislation and adopt measures to protect personal data held within public and private organisations is unquestionable.

⁵¹⁷ Victoria Lemieux, p.2.

⁵¹⁸ ARMA International, *Code of Professional Responsibility for Records Management* at www.arma.org.

⁵¹⁹ International Council on Archives, *Code of Ethics* at www.ica.org.

Records practitioners have an obligation to the society that they serve to ensure that their organisations are 'above board' in their dealings with citizens. They should see their role as critical to protecting the delicate balance between organisational/societal need and preserving the rights and privileges of individuals. Every record containing personal data could have a positive or negative effect on the life of a person or persons mentioned therein. As was discussed, the concept of the 'life-story' would help with the identification and attribution of records to living, identifiable people. This is the most challenging area that needs to be addressed. Once the records containing personal data are clearly marked then and only then can the appropriate steps be taken to safeguard them. People's lives can be adversely affected when their personal data is abused.

Records managers and archivists are critical in finding solutions to data protection. The issue of data protection which will not go away but will become increasingly challenging as the technologies made available to the masses become more enabling. Technology is still driving the need for privacy but in a different way from in the 1960s. The technology in the new millennium is far more pervasive, far-reaching, boundless, personal and custom-built than at any other time in human history. This has led to more intrusive practices that should put privacy advocates, records managers and archivists on their guard. The following chapter examines aspects of dealing with data protection and records management in a digital world.

5. CHAPTER 5

DATA PROTECTION AND RECORDS MANAGEMENT IN A DIGITAL WORLD



Image 12 Internet Privacy⁵²⁰
browertech.wordpress.com/category/internet-privacy

The seamless movement of information from desktop computers to personal data assistants (PDA) including smart-phones and tablets poses unimaginable risks to the unwarranted disclosure of personal information. Biometrics, including the proposed implantation of microchips into individuals to monitor their movements within the workplace, intrusive technologies such as closed circuit television (CCTV), the use of Hypertext Transfer (or Transport) Protocol (HTTP) cookies, radio frequency identifiers (RFID), global positioning satellites (GPS), drone cameras and spyware, the use of storage area networks (SAN) and the advent of 'cloud-computing' that allows virtually unlimited amounts of information to be stored remotely, all affect informational privacy and in turn have serious implications for recordkeeping and records management. This study, which represents a single abstraction

⁵²⁰ Image taken from Jennifer Brower's (PMP) Tech Blog.

in space and time within this dynamic environment, will explore the impact of the new technologies on the creation, maintenance and use of personal records.

The use of social media by organisations, both public and private, including *LinkedIn*, *Facebook*, *YouTube* and *Twitter*, is a growing trend that poses new challenges to the issue of privacy and recordkeeping. Some questions under review are, do citizens understand and acknowledge the impact of new technological trends on records related to them? Have the expectations of citizens appeared to have changed as it relates to what records containing personal data are collected by agencies? What would be the role of records managers and archivists in the new digital age as it relates to personal data? Are new skills and theories required for coping with these challenges? How would the 'life-story' concept apply in this environment?

Finally, the chapter ends with a close look at the newly proposed regulation by the European Union called 'The Right To Be Forgotten' which is intended to replace the Data Protection Directive.⁵²¹ The chapter considers the intent of the law, its feasibility and how it is perceived to assess its value from a recordkeeping perspective. Is the 'right to be forgotten' in conflict with the records management goals of retaining evidence, democratic accountability and preserving collective memory for the society at large? The chapter examines whether the technology in general creates a crisis with data protection in principle and in practice.

⁵²¹ European Network and Information Security Agency, *The Right to be Forgotten between Expectation and Practice* found at www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten. Accessed on 25 February 2013.

5.1 Being Remembered: The Records 'Life-story' in a Digital Age

Technology has changed how individuals are remembered. The new types of records created as a result of technology 'remember' people in life and beyond. To go a step further, information and communication technologies have made it virtually impossible for individuals to be forgotten. In the past, people and/or organisations that retained information about them would have the majority of their personal information in the form of paper-based documents or records. Some of these may have been physically retained in registries, records centres or archives with controlled access. Some recordkeeping systems were so poorly designed that it would be nearly impossible to retrieve all or some of the information and the context about an individual's life may have been lost over time. Hence, an individual's life-story or aspects of his or her life-story may be forgotten over time in manual environments. How has this changed? How do new digital records 'remember' an individual?

New forms of records including email, instant messages and those created on social media such as *Facebook*, *Twitter* and *LinkedIn*, result in very large amounts of information being retained and the creator may not have full control on what is disposed of over time. From a technical standpoint, the very nature of the transmittal of these records means that duplication happens in more than one place which may be a server, portal or database. For example, when an email is sent the copy of the email is kept in the 'Sent Items' on the desktop, laptop, tablet or smartphone of the sender as well as the server of the organisation of the sender. In turn, a copy is received in the 'Inbox' on the desktop, laptop, tablet or smartphone of the receiver and the server of the organisation of the receiver. Further copies may exist if the message was sent using search engines such as Google or Yahoo

which use data centres to store and backup messages.⁵²² The same applies to messages sent through social network sites.

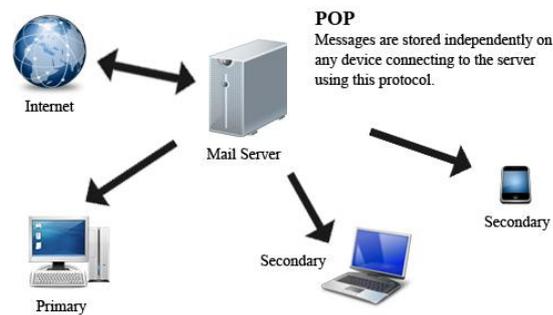


Image 13 Diagram of Email Path from a POP Server⁵²³
www.vimm.com/wp-content/uploads/2012/05/POP_diagram-email.jpg

In these environments, it is challenging to determine who has ownership of the information/record and the creator or data subject may not be able to fully control how their personal data is used or shared. Social media moguls like *Facebook* have found themselves facing questions from privacy advocates as well as in legal situations with the European Union over concerns about data sharing, data marketing and data storage.⁵²⁴ There are multiple ‘owners’ of personal data in this situation; the creator, who may be the organisation or the data subject, the site where the information is captured and re-distributed or a third party ‘data broker’ used by the site may all claim to be the owner of the information. This makes managing privacy and accountability for managing privacy very difficult.

One of the most disturbing features of today’s technology has been the lack of control of privacy by the user/data subject. The capacity of modern technology to track movement and behaviour for marketing and other purposes have left users clueless as to how to switch

⁵²² Google.com, *The Story of Send* found at thenextweb.com/google/2012/05/15/wonder-what-happens-when-you-send-an-email-google-tells-all-with-the-story-of-send. Accessed on 8 March 2013.

⁵²³ Image taken from Vivid Image, a company that offers online marketing services.

⁵²⁴ Lawyers.com, *Lawsuit targets Facebook privacy issues* at <http://communications-media.lawyers.com/privacy-law/lawsuit-target-facebook-privacy-issues.html>. Accessed on 21 April 2014.

these features off. The tracking of people and their activity is being conducted at many levels in today's society. For example, some department stores and supermarkets use software at the cashier with the capacity to monitor each customer, who are uniquely identified by a customer identification number and shopper's cards, to track their preferences. Customer data is being collected and stored without much consideration to the implications for privacy. There is the question of how robust is the security and the methods for disposition of the personal data after the purpose for its collection is completed. This can mean that individuals' transactions, actions, affiliations, purchases, entertainments choices, belief systems, interests, hopes and aspirations can be accessed without their knowledge and consent on a 24 hour, 365 day basis ultimately resulting in the ability to reconstruct an individual's life-story in detail.

Apple Inc. as a company has faced criticism and legal consequences as a result of what is seen as its flagrant disregard for privacy in recent times. It has been accused of using native applications for tracking the movement of users using identifier technology called unique device identifiers (UDIDs).⁵²⁵ It was discovered that the firm kept a log of location data on Apple device owners without permission and a US judge ordered the company to reveal more about their technology after death threats were received by a user.⁵²⁶ Similarly, Google has been required to defend its position on privacy repeatedly.

Additionally, individuals themselves are creating their own personal records that detail every aspect of their lives from what they eat for breakfast to where they go to dinner and everything in between. The First Lady of the US commented that, 'everybody's kitchen table

⁵²⁵ CNNMoney, *Apple probably isn't cracking down on native app cookie tracking – yet* found at money.cnn.com/news/newsfeeds/gigaom/articles/2013_02_26_apple_probably_isnt_cracking_down_on_native_app_cookie_tracking_yet.html. Accessed on 11 March 2013.

⁵²⁶ TechnoBuffalo, *Death Threats and Privacy: A Judge Orders Apple to Reveal More Info in Tracking Lawsuit* found at www.technobuffalo.com/2013/03/08/apple-tracking-privacy-lawsuit. Accessed on 11 March 2013.

conversation is now accessible to everybody else so there is a national [and international] conversation about anything'.⁵²⁷ This reinforces the point that matters that were privately discussed in the homes among families and friends are, as a result of the social media environment now discussed and debated openly, not only on a national level but on a global scale. The world has become so much smaller in the sense that topics and issues go 'viral' in a matter of seconds and an individual could be embarrassed and defamed within the time it takes to upload a video on *YouTube*. For example, in a BBC news report, a PR executive lost her job over a racist comment she made on *Twitter* which went 'viral'⁵²⁸ on the Internet.⁵²⁹ This is the reality of the instant impact of sharing personal information in the digital world.

Therefore, individuals must be aware of how the technology is impacting on their privacy. They have to think carefully about how they wish to be remembered by society at large and what aspects of their lives they want to be in the public domain. The records they create on themselves became part of their 'memory continuum' and are part of what is referred to in IT as their 'digital footprint'. Individuals, just like organisations, should take measures to protect themselves and their families. It may be a matter of life or death as tracing their whereabouts is made simple with apps such as *Google Earth* which uses global positioning technology.

Another new activity being carried out by individuals on a day-to-day basis is 'life-logging'. This is the act of an individual creating a life-story on him or herself for future reference by essentially tracking his or her every movement or activity using all the available technologies. This technologies include, but are not restricted to, digital photography,

⁵²⁷ Huff Post Entertainment, *Michele Obama on Oscars Criticism: 'Absolutely Not Surprising'* found at www.huffingtonpost.com/2013/03/01/michelle-obama-oscars-criticism_n_2788512.html. Accessed on 11 March 2013.

⁵²⁸ 'Viral' is a term used to describe when an item posted on the Internet spreads rapidly worldwide.

⁵²⁹ BBC News, PR Officer loses job over racist *Twitter* comment at www.bbc.co.uk/news/world-us-canada-25484537. Accessed on 21 April 2014.

capturing audio or video and creating a searchable links to his or her 'digital footprint' on *Facebook*, *Twitter* and *LinkedIn*. Undoubtedly, this kind of all-embracing accumulation of personal data into a single space using software as a platform would open an individual to many risks of breaches of their privacy and can lead to unwanted occurrences such as identity theft. The matter of 'identity theft' as a security risk will be further discussed in this chapter. It also means from a recordkeeping perspective that these individuals are creating records as 'persistent representations' of themselves, good or bad, that would exist well beyond their death.

As it relates to the life-story concept, the more elements that exist on a person in the record, the more detailed the life-story that could be re-constructed. This is the concern for privacy advocates and individuals including superstars as they realise that the press is becoming more and more intrusive in various aspects of their lives. Examples of this can be seen in two famous law suits, one involving Catherine Zeta-Jones, a Hollywood star and the other involving Princess Catherine, wife of Prince William of the British Royal family.⁵³⁰ In both situations, images were captured and published without consent. Images of individuals caught on camera do not alone constitute an invasion of privacy but it is the singling out of an individual that may be considered a breach of their privacy.⁵³¹ This illustrates that even superstars who, in some cases, have an arsenal of bodyguards and other types of security are left vulnerable to intrusive devices which capture their private information. This matter is being addressed, particularly in the EU Data Protection model, as it relates to CCTV. Records, regardless of form, which highlight a particular individual in a manner where that individual is clearly identifiable singularly is indeed a breach of privacy/data protection and

⁵³⁰ Mirror, Kate Middleton Topless Pictures: *Place says invasion of privacy is "grotesque and totally unjustifiable" and evokes memories of Princess Diana* at www.mirror.co.uk/news/uk-news/kate-middleton-topless-pictures-palace-1323761. Accessed on 25 April 2014.

⁵³¹The outcome of the case involving Catherine Zeta Jones may be read in a BBC report entitled, *Zeta Jones Privacy Case Ends* found at news.bbc.co.uk/2/hi/entertainment/2843999.stm. Accessed on 16 March 2013.

heavy fines have been imposed on photographers and other media related personnel in recent times for these types of breaches. There are now more ardent calls for press regulation to manage this issue.

The Press and Data Protection

The regulation of the press as it relates to privacy and data protection is a significant issue. This study has presented the issue of balancing access to records and information with protecting the private information of individuals. However, there is another balancing act required in modern societies, which is, balancing freedom of expression with protecting private information of individuals. Media houses such as newspaper agencies, television and radio stations collect and accumulate vast amounts of personal data. The priority of media houses is to inform the public about news stories which include the sharing of personal data. This activity has led, in some cases, to inappropriate methods of gathering and disseminating private information on individuals.

The matter came to the fore in the UK context in 2011, after a phone-hacking scandal emerged involving *News of the World* newspaper. The newspaper was convicted of intercepting voicemail messages of royal aides.⁵³² Lord Justice Leveson was appointed by the British Prime Minister, the Right Honourable David Cameron, to investigate the scandal. He was assisted by a panel of six independent assessors to examine the culture, practices and ethics of the press and, in particular, the relationship of the press with the public, police and politicians. The Inquiry produced a four volume report which addressed themes such as freedom of the press and democracy, the responsibilities of the press, criticisms of press culture, practices and ethics and conclusions and recommendations for future regulation of

⁵³² BBC News, Q&A: *News of the World Phone Hacking Scandal* at www.bbc.com/news/uk-11195407. Accessed on 13 September 2014.

the press.⁵³³ The UK Information Commissioner's Office responded by producing draft guidelines for data protection and the media.⁵³⁴ These draft guidelines demystify the requirements for the media as it relates to their obligation to uphold data protection legislation. The press is required to comply with data protection legislation.

This study recognises that there are many aspects of the privacy problem that relate to the sharing of knowledge for democratic and security reasons. The issue of the media and its role in protecting private data is not an easy one to navigate given the demands of an information-driven world. The technologies are increasingly enabling and the legislation does not update quickly enough to match the capabilities of the technology. Added to this phenomenon are rapid changes in human social behaviours which appear to fuel the activity of the press. As more information is created revealing more details about the personal life of individuals in accessible ways such as with the use of social media sites, that information is exploited by the press to create or sensationalise news stories. Conversely, the press also serve as the biggest 'whistle-blowers' who could help to protect the public/individuals from wrongly acts. Therefore, this topic deserves to be thoroughly investigated across the jurisdictions as part of future work to more fully appreciate its depth. In the case of the West Indies, extensive research would need to be conducted to assess the role of the press in threatening and conversely, protecting privacy.

In reality, the amount of data being collected and stored on individual people in a multiplicity of ways i.e. data replication, makes it extremely difficult to control how an individual will be remembered. One may choose to erase unflattering images and other

⁵³³ The National Archives, *An inquiry into the culture, practices and ethics of the press: report [Leveson]* at [webarchive.nationalarchives.gov.uk/20140122145147/http://www.levesoninquiry.org.uk](http://www.levesoninquiry.org.uk). Accessed on 13 September 2014.

⁵³⁴ ICO, *Data protection and journalism: a guide for the media* (draft) at ico.org.uk/news/latest_news/2014/~media/documents/library/Data_Protection/Research_and_reports/data-protection-and-journalism-a-guide-for-the-media-draft.pdf. Accessed on 13 September 2014.

information of oneself in one form but it may continue to exist in another form or in duplicate in unknown locations. There is actually no means at present to totally 'sanitise' or 'alter' the way one is remembered. The best approach is to attempt to control as much as is humanly possible what information is personally created as well as continuously track the information that may be stored on oneself on the Internet and other 'storehouses' in the form of data centres and databases. A simple exercise is to 'Google' oneself and examine closely all 'hits' containing your name and/or other means of identification that appear to relate to you as an individual. Some websites such as *Spock* are known people-search engines that 'harvest' information and conduct 'deep web' searches on individual people to assist persons in finding them wherever in the world they may be. This is indeed a frightening prospect in times of cyber-crime and cyber-bullying which are not adequately dealt with in the various data protection regimes.

5.2 Electronic Records and Data Protection

From the outset, the move for data protection was augmented by the concern that fast growing technologies with rapidly increasing capabilities were being used by governmental and private entities to manage records and information. However, in the new millennium, the ability to create, manipulate, distribute and store records and information has increased ten-fold. Agencies are now armed with the latest in hardware and software with dedicated information technologists whose main role in the organisation is to find new and innovative ways to incorporate the use of technologies in every possible task in the day-to-day operations. The days of the sole use of paper-based, manual systems are quickly passing and electronic recordkeeping is the new gold standard with electronic records as the format taking the lead in many aspects of the governance of society.

In the selected jurisdictions, it was seen that citizens generally accepted the use of technology for the improvement of services but remain wary of the management of that technology as it relates to the protection of their personal data against misuse by unauthorised people. As a result, many privacy watchdog groups have been formed and privacy advocates are on the rise. Citizens appear to be more comfortable in recent times with the utilisation of technology but still mistrust the intent behind its use by governments and organisations as well as the increasing intrusiveness. In the past, there was a fear of the manipulation of personal data internally within an organisation. Today, the fear is based more on the interconnectivity of the information databases/storehouses which now have a global reach through wide area networks, the Worldwide Web and 'cloud-computing'. Electronic recordkeeping has been very appealing to some in leading companies and that information is being shared and stored in far-flung locations around the world in unprecedented ways. A large percentage of the records are created and maintained as part of e-government, e-commerce, e-banking and financial, criminal and judicial, travel, health and social and educational systems. Many of these records contain personal data and therefore are subject to data protection.

It must be noted that not all systems containing personal information are records management systems. There will be many databases in a given organisation that retain information about identifiable people but do not have the functionalities of a records management system to ensure that that information is captured, classified, stored securely and properly disposed of. This would mean that personal information in this environment would be even further under threat of manipulation, unwarranted access or even destruction because of the nature of these software packages. There is a special focus on collaboration and work-groups which would enable end-users to retrieve, update and

refresh data in a quick, dynamic manner. However, if there are no records management controls at play, information could be just as easily be changed, altered or destroyed. In this situation, the owners/creators of the data would need to pay even more attention to security measures and audit logs to ensure that there is no unauthorised access to the data.

5.3 Electronic Personal Data and Security

The topic of security of personal data in an electronic environment is quickly becoming the most topical issue dealt with around the globe. The elements in records that make them attributable to an identifiable person can be created, captured, manipulated and distributed more easily in an automated environment than ever before. This was evident in Chapter 2 in Germany where technology is used to capture key personal and sensitive data in the health card system. However, the risks of unauthorised access are far greater when personal data is stored in databases on shared networks on remote servers. Security is critical when personal data can be entered, altered and transmitted by multiple users operating in separate entities. In the case of Germany, the actors involved with storing and using the personal data were the doctors (hospital), insurance agents (insurance company) and the pharmacist (pharmacy) and if the right controls and measures were not placed within each separate and distinct entities/spaces, the possibility of breaches could have a 'mushroom effect'. Simply put, the bigger the network, the bigger the risks. One organisation may take all the right steps including training and sensitising their staff. However, that may not be the case with the other two involved even though they are dealing with the same information. Cyber-attacks including hacking and virus attacks are the greatest external threats to personal information stored in automated environments. Hacking is a skill that is continually developed by highly talented technologists who learn to override firewalls and other protective mechanisms used to protect electronic information. Daily, important government

and private databases are subject to malicious software infiltrations and other forms of cyber-attacks. The US Government spends billions on an annual basis protecting its Pentagon and other arms of its government from cyber-attacks from terrorist cells and allegedly other governments. University and other higher education sites which contain vast amounts of personal data in the form of staff and student records are also attacked with frequency.⁵³⁵ Some high profile persons were hacked including, Michelle Obama (First Lady of the US), Joe Biden (Vice –President of the US) and Jay-Z (international rap star), having their personal information placed openly on the Internet as recently as March 2013.⁵³⁶

An internal threat to electronically stored personal data is the act of tampering with types of records as well as unauthorised access by staff with malicious intent or as a result of errors as discussed in Chapter 2. This undermines the integrity of electronically stored personal data and its authenticity becomes questionable. The accuracy of personal data in an automated environment can be more challenging to maintain than in the paper-based, manual environment. This data can be very vulnerable in the wrong environment resulting from badly designed systems. In addition, if the wrong strategies for migration and conversion of data are employed, electronic personal records could lose critical metadata and become irreparable or irretrievable. The information may even be corrupted and therefore will not reflect the actions and transactions that have taken place, affecting the rights and privileges of an individual. These are but some of the main issues that would impact on the privacy/data protection in the digital world.

Some governments and organisations promote self-service portals where customers have access to their own data. Customer data in the portals are open to hacking and are

⁵³⁵ E-Hacking News, *Breaking News* found at <http://www.ehackingnews.com>. Accessed on 18 March 2013.

⁵³⁶ ABC News, *Obama: Looking Into Celeb 'Secret File' Hack* found on abcnews.go.com/US/michelle-obama-joe-biden-celebrities-personal-information-allegedly/story?id=18707707. Accessed on 18 March 2013.

vulnerable to unauthorised access. Organisations would need to ensure that the data is consistently updated to avoid inaccuracy and breaches to data protection legislation. These records may be integrated with other related systems and lay bare substantial amounts of details on identifiable individuals. For example, governments may integrate national registration information with motor licensing information. Similarly, travel information held in Immigration databases may be integrated with criminal justice and/or police records in an attempt to deal with international crime.

Identity theft is a very relevant concern in the fight to protect privacy. Identity theft also known as identity fraud is a crime which involves the stealing of the personal information of an individual to deceive for economic gain. This type of crime is rampant in today's environment as persons seek to unlawfully accumulate material goods or other benefits from others without their consent. Additionally, there is the crime called 'phishing' where hackers steal email addresses and personal details to carry out email scams. The authorities try to identify and find hackers by using Internet Protocol Addresses (IPs), which can track the person to a general location like a region or a country. However, clever hackers could hide or re-route their IP addresses to mislead authorities.

The EU group of data privacy regulators have deemed IP addresses to be personal data. It argues that when an individual can be identified from an IP address, that constitutes personal data. This view is opposed by Google which contends that IP addresses only reveals the location of a computer, not an individual user. There is a further argument that most individuals would utilise the same computer so that makes an IP address attributable to them independently.⁵³⁷ This point has to be acknowledged as the ability to identify an

⁵³⁷ The Washington Post, *IP Addresses are Personal Data, EU Regulator Says* found at www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html. Accessed on 19 March 2013

individual from an IP address would be a critical element in classifying that information as personal data.

Modern day storage devices are becoming smaller and more portable making them extremely vulnerable to theft. Even with the best encryption technology, technologically savvy individuals can easily override security features to access sensitive personal data. These devices include laptops, tablets and smart-phones which are essentially mini-computers. It was recently discovered that Android phones could be breached by freezing them.⁵³⁸ Care and attention is needed by executives who carry data on storage media including flash drives and compact external drives when travelling. The storage capacity is so vast that an entire organisation's records, including highly sensitive personal data, may be carried in this form. There are legal implications for taking this information outside the jurisdiction in which it was created as it may no longer be subject to stringent data protection regulations depending on where in the world it is stolen.

5.4 'Cloud-Computing' and Third Party Storage across Borders

'Cloud computing' is the latest trend in off-site data storage. Cloud computing essentially is the practice of storing and accessing data over the Internet instead of local storage on a computer hard drive or server.⁵³⁹ This means that an organisation's or private personal data could be stored anywhere in the globe, usually through third party storage. *Google, Apple, Microsoft, Amazon* and *Dropbox* all offer cloud computing as a service to customers. Thus, cloud computing has been recognised as posing a range of risks to informational privacy. Australia and NZ Privacy Commissioners have responded to this by offering guidance to businesses to avoid the risks associated with 'cloud computing'. The National Archives of

⁵³⁸ BBC News Technology, *Frozen Android Phones Gives Up Data Secrets* found at www.bbc.co.uk/news/technology-21697704. Accessed on 21 March 2013.

⁵³⁹ PC Magazine, *What You Need to Know About Cloud Computing* found at www.pcmag.com/article2/0,2817,2372163,00.asp. Accessed on 19 March 2013.

Australia have even prepared a checklist for archivists and records management entitled, 'Records Management and the Cloud'.⁵⁴⁰ What are the main privacy concerns when storing records in the 'cloud'?

Cloud computing adds a new dimension to being remembered or remembering in a digital world. In cases where attention is not paid to the terms and conditions of third-party storage, the creator of the record and/or the data subject could completely lose control of the personal data stored on him or herself. In the case of an organisation, the integrity of the records stored off-site must be upheld and protected to ensure that the authenticity of the records is not compromised. Records in the 'cloud' must meet the same requirements and standards as records in other storage.⁵⁴¹ Again, the matter of ownership of information must be very clear in this situation.

From a records management standpoint, it would be prudent to carry out privacy impact assessments when deciding on this as a strategy. The use of 'cloud computing' could be a solution when working in disaster prone regions as a way to ensure that records are not damaged or destroyed. However, the pros must outweigh the cons and the best approach taken to safeguard all stakeholders must be taken. Contractual agreements must be 'air-tight' ensuring that the rights and privileges are clearly outlined. All data inclusive of personal data in the 'cloud' must be also governed by the right privacy policies and procedures.

Further to this, records managers using the 'cloud' technology in their programmes must be conversant with privacy/data protection legislation not only in their jurisdiction but any

⁵⁴⁰ The National Archives of Australia, *Records management and the cloud – Checklist* found at www.naa.gov.au/Images/Cloud_checklist_with_logo_and_cc_licence_tcm2-41355.pdf. Accessed on 19 March 2013.

⁵⁴¹ See InterPares (RIC) study on *Records in the Cloud*, a collaborative study led by the School of Library and Information Studies at the University of British Columbia at recordsinthecloud.org.

other jurisdictions in which the company they choose operates within. These companies must be viewed as third party custodians of data and should be handled with extreme caution any organisation's records. Custodianship does not have to translate to access. Measures must be employed to ensure that employees working for the third party custodian cannot breach trust by accessing information without authorisation. The risks remain very high.

Personal information that is typically stolen includes social security numbers, credit card information, credit report information, and bank account information. A prime example is in September 2014, it was reported that the iCloud service owned by Apple was breached using usernames and passwords to hack into the iPhones of celebrities. Their personal photographs were taken and published on the Web.⁵⁴² Apple denied that hacking of the iCloud took place but the risks involved in the use of cloud computing were exposed.⁵⁴³ The following section will look at the records types containing personal information that are generally created, used and maintained in electronic format.

5.5 Identifying Electronic Records Types with Personal Data

The types of electronic records containing personal data and captured by organisations have increased exponentially. Personal data is needed to carry out many types of services being offered to citizens from healthcare, to education, to travel. Today's organisations thrive on databases and networks that store vast amount of data on individuals for transactional, security, historical, cultural, political, administrative, legal and fiscal purposes. Electronic

⁵⁴² Forbes, *iCloud Data Breach: Hacking and Celebrity Photos* at www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos. Accessed on 13 September 2014.

⁵⁴³ Yahoo! News, *Apple denies iCloud breach let hackers take iPhone hostages* at news.yahoo.com/apple-denies-icloud-breach-let-hackers-iphones-hostage-123055818.html. Accessed on 13 September 2014.

records may reveal details about the 'life-story' of an individual and could include the following record types illustrated in Table 1.4 designed by the author.

<i>Sector/Systems</i>	<i>Some Key Electronic Records Types with Personal Data</i>
E-Government	National Registration information, Personal Identification numbers, Vehicle Licensing records, Land Registry records, Income Tax, Electoral records, Population Records (Births/Deaths/Marriages/Wills/Deeds)
E-Commerce/E-Banking & Finance	Credit Cards, Debit Cards, Credit Reports and E-Contracts
Healthcare/Social Services	Medical records, Health E-Cards, Pharmaceutical records, National Insurance records, Social Security number/records
Education	Student records, Employee records, Identification card systems, Library records
Crime & Justice	Police records, Court records, Prison records, Judgements and other types of legal records
Security	CCTV records, drone cameras footage, digital cameras including those in smart-phones and tablets
Travel	Visas, Passport records, Biometric records
General	Email, Telephone messages, Instant messaging (text/bbm/Whatsapp)

Table 7 Sample of Key Electronic Record Types with Personal Data

The table demonstrates how personal records are created using a multiplicity of formats into day's digital world. Personal records are also more pervasive and persistent than ever before as discussed in Chapter 3.

5.6 The EU 'Right to be forgotten'

The European Commissioner first attempt to address directly data protection in electronic communications and the Internet was its Directive on Privacy and Electronic

Communications (2002/58/EC) enforced on 12 July 2002.⁵⁴⁴ However, its most recent proposal for a new regulation which was introduced on 24 January 2012 that is the focus of this section. This will be referred to as the General Data Protection Regulation.⁵⁴⁵ The regulation, for all intents and purposes, is being considered as the way forward as it relates to the regulation of data protection in Europe. It seeks to build consumer's trust in the use of online environments for economic purposes. One way it hopes to do so is by addressing the complete erasure of an individual's 'digital footprint' or the 'right to oblivion' of personal data stored and collected in Europe on an identifiable individual upon his or her request. One of the key principles behind the regulation is 'the right to be forgotten' which is based on the premise that people should be in control of their personal information to the extent where they are able to request that any trace of their personal data be removed when it is 'no longer necessary for the purpose it was collected'.⁵⁴⁶ This raises questions about the desirability as well as feasibility of the proposed regulation. Do individuals in today's environment want to be completely forgotten? Is this even technically possible? What impact would this have on recordkeeping systems?

The 'right to be forgotten' appears to be a direct response to advances in technology that have created challenges with ensuring the security of personal information online. It is well intentioned as it seeks to protect individuals in today's digital environment but its feasibility is highly questionable and it does not appear to be desirable.⁵⁴⁷ This is evidenced by the fact that the date for adoption of the regulation with its proposal has not yet occurred and the

⁵⁴⁴See *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* at www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/data-protection-privacy/directive-2002-58-ec.

⁵⁴⁵European Commission, *Proposal for a General Data Protection Regulation* COM (2012) 11 at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 21 April 2014.

⁵⁴⁶European Commission, Article 17, Preamble (53) found at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 3 April 2013.

⁵⁴⁷Stanford Law Review, *The Right to be Forgotten* at www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten. Accessed on 21 April 2014.

debates and discussions continue.⁵⁴⁸ In a previous section, this study addressed all the ways that individuals have been creating records on themselves and the fact that technology has changed the way one is remembered. However, in the digital age, it appears that individuals are less concerned with being forgotten and spend more time creating and expanding their 'digital footprint' as it relates to the social, political (activist) and/or professional aspects of their life-story. This is evidenced by the amount of users on *Facebook*, *Twitter* and *LinkedIn*. *Facebook* states that it reached 1.01 billion active global users by the end of 2012.⁵⁴⁹ Many individuals that are not on *Facebook* are creating life-stories in other digital forms and sharing them on the Internet.

Where there is unease by individual users is with the handling and security of personal information related to their financial position and the benefits that go along with their status in society. Yet, they want to leave their mark on society and be remembered for their activities, associations and achievements as shown by the statistics of Internet usage. The new technologies allows individuals to do this in an unprecedented way and so 'the right to be forgotten' completely may have appeal for a few. The US demographic for social media use shows the large percentage of users between the ages of 18 and 54. The table below by technology consultant company Pingdom, shows statistics of online use of social media sites in 2012 based on the age of individuals in the survey.

⁵⁴⁸ European Commission, *Data Protection Day 2014: Full Speed on EU Data Protection Reform* at europa.eu/rapid/press-release_MEMO-14-60_en.htm. Accessed on 1 February 2014.

⁵⁴⁹ Yahoo Finance, *Number of active users at Facebook over the years* found at finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html. Accessed on 3 April 2013.

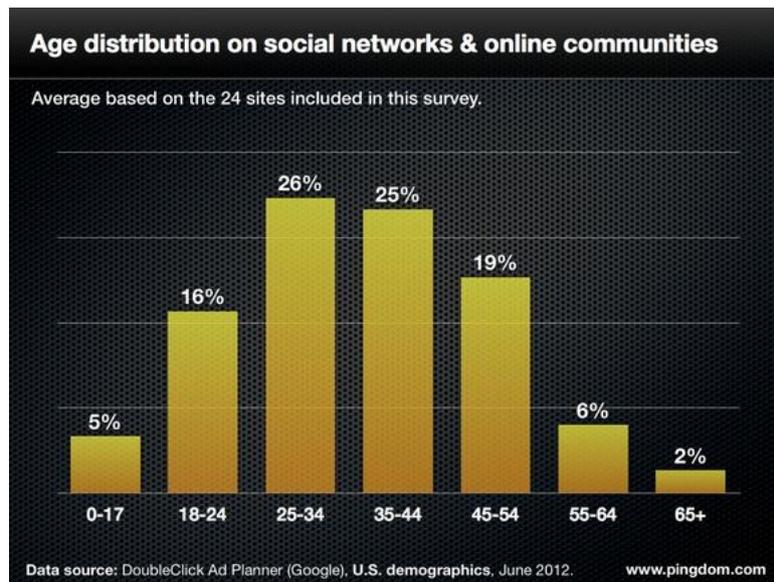


Image 14 Age Distribution on Social Networks & Online Communities (US)⁵⁵⁰
www.pingdom.com

The attempt by the European Commission to curb unwarranted access to personal data through the principle ‘the right to be forgotten’, especially given that people want some part of their life-story to remain, is realistically impossible. The regulation offers a few exemptions to total erasure where it states that further retention can be allowed for historical, statistical and scientific purposes; public interests and the right to freedom of expression.⁵⁵¹ However, it does not take into account that there may be a need to preserve some personal data for reasons of accountability which is one of the main objectives of good recordkeeping. Total erasure of personal data when no longer necessary for the purpose collected means that evidential and informational value of the personal data could be lost before the need for public interest is realised. An example of how this can impact on society is the recent scandal of the British Broadcasting Corporation (BBC) where it was brought to light that employee, Sir Jimmy Savile, a beloved television personality for all ages, was allegedly involved in sex abuse of both children and adults over decades. Some of his offences were recorded in various formats and provide evidence of his wrongdoings

⁵⁵⁰ Image taken from company called Pingdom which offers anti-virus and back-up consultation services.

⁵⁵¹

which was widespread.⁵⁵² Erasure of that information in the past would have meant that the evidence to hold him accountable today would have been unavailable to investigators. Hence, the result of the ‘right to be forgotten’ could inevitably lead to a moral dilemma or legal fallout.

Another consideration is whether this proposal is at all feasible from a technical standpoint. As was discussed in a previous section, digital information is virtually impossible to totally erase even when properly managed due to data replication. A remnant of that information still remains in some form and, in many cases, in multiple locations. The European Network and Information Security Agency (ENISA) in its paper entitled, ‘The right to be forgotten – between expectations and practice’ states unequivocally that ‘the right to be forgotten [as] a purely technical and comprehensive solution to enforce in the open Internet is generally impossible.’⁵⁵³

Further, the group raised three very pertinent questions 1) what is the scope of personal data? 2) who has the right to deletion? and 3) what constitutes ‘forgetting a data item? From a records management perspective, it was already seen that the definition of ‘personal data’ is too vague even with the recent changes made by the EU. Hence, there is the need to clearly establish what data is truly personal data. This study has offered the solution of using the ‘life-story’ concept to identify the five elements which would make data/records be classified as truly personal and attributable. However, it becomes very challenging to deal with the second question in recordkeeping if a record, which may take a digital format such as a video, has more than one identifiable individual and one of them

⁵⁵² BBC, *Jimmy Savile Scandal: Report Reveals Decades of Abuse* found at www.bbc.co.uk/news/uk-20981611. Accessed on 3 April 2013.

⁵⁵³ ENISA, *The right to be forgotten – between expectations and practice* at www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten. Accessed on 24 April 2014.

request erasure. It may be easier to anonymise the individual who requested erasure by blocking out their face in the video rather than erasing the video in its entirety. This would protect the integrity of the record which may provide evidence and be useful for reasons of accountability, history or other inquiry over time. Lastly, in recordkeeping 'forgetting' information may not mean erasing that information totally. It may not even be possible due to data replication and duplication but may involve removing any means of enabling accessing to that data through erasure of access points to that data/record in indexes and other finding aids.

The 'right to be forgotten' is indeed a complex issue that requires much further research and consideration across many disciplines. All the answers cannot be provided by one interest group. Archivists as a group have been challenging the EU proposal and involved in discussion groups, writing position statements and online petitions to retard or prevent the adoption of this regulation for concern about the future of archival data retention.⁵⁵⁴

⁵⁵⁴ International Council on Archives, *Position Statement – Protection of Personal Data* found at www.ica.org/3881/position-statements/ica-position-statements.html. Accessed on 5 April 2013.



Image 15 Map of the West Indies and Central America (1910)
www.emersonkent.com/map_archive/central_america_1910.ht

6. CHAPTER 6

DATA PROTECTION IN THE WEST INDIES: RECOMMENDATIONS FOR EMERGING PRACTICE

One of the main objectives of this study is examine the provisions for data protection in selected jurisdictions from a records management perspective in order to inform emerging practice in the West Indies as a region. As mentioned in Chapter 2, the region referred to in this study include twelve islands namely, Jamaica, Antigua, Barbados, Trinidad and Tobago, Grenada, Montserrat, St. Lucia, St. Kitts & Nevis, Dominica, St. Vincent, Guyana, formerly British Guiana and Belize, formerly British Honduras.⁵⁵⁵ The second chapter also established that the administrative and legal systems that developed within these territories were inextricably linked to those of their coloniser.⁵⁵⁶ This historical reality has shaped the economic, social and political development of the region far beyond the colonial period and, as will be discussed in this chapter, has implications for the implementation of data protection in this complex and unique space.

This chapter investigates key research questions relating to the context and push factors for the implementation of data protection in the West Indies. It addresses: the main obstacles to data protection implementation in the West Indies; key drivers; the merits and demerits of an integrated approach and how the relationship between records management and data protection could be enhanced to stabilise its implementation.

⁵⁵⁵ Albert Fiadjoe, *Commonwealth Caribbean Public Law* 3rd Edition (New York, 2008), p.4.

⁵⁵⁶ Fiadjoe, p.4.

Thereafter, the study offers recommendations for the approach that could be taken in light of the lessons learnt in the comparative study of international jurisdictions undertaken in Chapter 3 with a view of the rapid technological developments taking place on a global scale.

6.1 The Challenge of Change: Main Obstacles to DP Implementation

Gordon K. Lewis in his study on *The Challenge of Independence in the British Caribbean* states that, 'independence is merely a redefinition of the legal status of the society [and] does not necessarily bring in its wake a profound social metamorphosis.'⁵⁵⁷ He outlined some of the challenges that would be faced by the region during its transition from colonial status to independent status. He essentially argues that colonialism left a legacy of weak administrative structures, over dependency on the metropole and generally a 'persistent poverty'. Lewis further surmised that independence would mean a readiness to look inwards, not outwards for solutions to problems. However, this study supports looking outward when it means assessing whether data protection implementation has been successful, in whole or in part, in other jurisdictions so as to provide lessons to the region. Looking inwards is also critical to determine whether the region 1) needs to implement data protection at all and 2) what aspects would need to be tailored to suit its own unique situation.

⁵⁵⁷ G.K. Lewis, 'The Challenge of Independence in the British Caribbean', edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996), p. 511.

This study argues that colonial experience of the West Indies and its legacy in the post-independence period resulted in the region lagging behind in the development of features that would provide a stable foundation for the implementation of information rights in any form. Three main obstacles to data protection implementation in the West Indies have been identified in this study. These obstacles are 1) the underdevelopment of its recordkeeping systems and lack of records management 2) the disparate and disjointed legal systems and 3) the lack of political will. These obstacles may be seen both at a regional and national levels.

Obstacle No.1 – Poor Recordkeeping Systems

The first and most pressing matter to tackle towards successful implementation of data protection is the problem of poor recordkeeping in both public and private organisations in the region. Why is this so important to data protection implementation? As discussed in Chapter 4, records in all their forms capture a high percentage of personal data in order to administer many functions within society. When these records are mismanaged, the risks of non-compliance with regulatory frameworks increase. Unfortunately, this is the current situation that presents itself in the majority of territories in the West Indies region mainly as a result of colonial dependency in the post-independence period. The systems that were set up by the British prior to their leaving at the end of the colonial period were not properly maintained.⁵⁵⁸

⁵⁵⁸Jeannette Bastian, *Owning Memory: How the Caribbean Community Lost its Archives and Found its History* (Westport, 2003).

What was seen in the post-independence region was the development of localised styles of maintaining records which are characterised by the failure to capture the right records in the right systems, lack of retention and disposition scheduling procedures, poor storage conditions, insufficient data security and dysfunctional archival preservation. This is also compounded by the fact that the region is situated in the tropics which means that even with the best efforts to keep records safe environmentally they are subject to dangers from natural and man-made disasters including hurricanes, tsunamis, pests, fires and mould outbreaks. The region's records and information are constantly under threat and require an extra effort by trained professionals to ensure that their integrity is maintained and preserved where necessary.⁵⁵⁹

There is also the issue of the lack of training in records and archives management. This has had a negative impact on the life-cycle management of records particularly in governmental agencies. Records are being created by daily activities, accumulated in an ad hoc manner, placed in unsafe and under-supervised storage areas both in the paper and electronic world and then indiscriminately dumped/destroyed when there are space constraints. In many of these situations, the creating offices have no existing expertise in the rudiments of records management and do not even realise that there is a problem with their recordkeeping until there is a crisis. This puts records containing personal data in a very vulnerable position. There are undocumented cases of

⁵⁵⁹ Based on observations as a trained records and archives practitioner and regional consultant.

unauthorised access to records by internal staff as well as external users with malicious intent.⁵⁶⁰

Although this paints a very grim picture of the state of the region's recordkeeping, the situation is not likely to end without sustained action from all levels of society. Caribbean governments need to place the issue of good recordkeeping much higher on their agendas and recognise that doing this is the only path to good governance. Private companies also need to recognise that their records reflect the activity of society and may be valuable not only to their business but have national significance. Records are the lifeblood of any organisation and only good recordkeeping will provide a stable foundation for all of society to function more effectively and efficiently. Additionally, many territories still do not have appropriate and/or up-to-date Archives Acts with the accompanying records management regulations. Many still have not instituted a career path for records management and archives that would provide an incentive for persons to train in these critical areas.⁵⁶¹

Since the establishment of the Caribbean Association of Archives in 1975, there has been some effort by a small group of trained archival Caribbean professionals to advocate and promote the role of records management and archival administration in society.⁵⁶² Among their stated objectives is to establish, maintain and strengthen

⁵⁶⁰ Experiences known from conducting regional RIM consultancies.

⁵⁶¹ The conclusions are drawn from the author's interaction with regional archivists and active participation in regional archival work as there is insufficient documented material to support these assertions.

⁵⁶² The author is part of this small group and serves as the Communications Chair for the Caribbean Archives Association.

relations between institutions and individuals concerned with the custody, organization and administration of archives in the Caribbean area; to encourage the description of archival material and to facilitate the exchange of information relating to archives and to act in ways which make material in Caribbean archives more widely known; to encourage in all countries in the Caribbean the establishment of archives; to promote in the Caribbean region the professional training of archivists and to promote the implementation of records management programs in whatever media in the various Caribbean countries.⁵⁶³

In addition to this effort, The University of the West Indies Archives and Records Management Programme has to be acknowledged as a significant contributor to the training of Caribbean archivists, records managers and other information management professionals and para-professional.⁵⁶⁴ The campuses at Mona and Cave Hill have been actively training the region's information management workers in both the public and private sectors since 1996 through its Certificate in Records Management programme and through the Masters in Heritage Studies programmes established by the University's Departments of History on three of its four campuses.⁵⁶⁵ Over three hundred records officers have been trained in the Cave Hill programme alone.⁵⁶⁶

⁵⁶³ Caribbean Branch of the ICA, *Constitution of CARBICA* found at www.carbica.org. Accessed on 11 April 2013.

⁵⁶⁴ See The University of the West Indies, Archives and Records Management Programme at www.uwi.edu/archives.

⁵⁶⁵ The author serves as a sessional lecturer in these programmes.

⁵⁶⁶ Sharon Alexander-Gooding, Paper presented at The University of the West Indies, Mona, Jamaica, February 2013.

This study asserts that sound data protection implementation/management and records management are irrefutably linked. The records management situation therefore has to be properly addressed in the territories before the implementation of data protection for it to stand a better chance for success. This requirement is further discussed when looking at recommendations.

Obstacle No.2 – The Disparate and Disjointed Legal Systems

Another obstacle towards successful implementation both at a national and regional level is the current state of law and legal systems. The tensions that were discussed in Chapter 3 between federal and state authorities as it relates to data protection implementation could arise in the West Indies between national authorities and the regional authority. The other issue in Chapter 3 of lack of harmonisation between laws could also affect the West Indies. A senior lecturer in the Faculty of Law at The University of the West Indies, Cave Hill Campus, states that ‘the region has seventeen distinct legal jurisdictions in a small geographical space’. Another legal expert in the West Indies revealed that, ‘there is a pervasive distrust among the territories and they favour the independence of their own system of justice’.⁵⁶⁷ In the jurisdictions studied, the issue of multiple layers of legal provisions at federal and state levels as well as sectoral codes was evident, even with an overarching piece of legislation. Disjointed legal systems can complicate the comprehensive implementation of data protection/privacy legislation as they can lead to contradictions and incompatibility reducing harmonisation. From a historical perspective, although Caribbean territories

⁵⁶⁷ Interview conducted with West Indian legal expert (Bridgetown, 2010).

have had a shared experience that resulted in most of them adopting British common law, localised legal systems developed in each small territory with each unique from the other.⁵⁶⁸ What essentially happens is that each island-jurisdiction undergoes the same repeated process in designing and adopting new legislation through the various offices of their Attorney Generals. This is tantamount to ‘reinventing the wheel’ every time the adoption of a law is desirable even where the intended law is for the same purpose.⁵⁶⁹ In this environment, data protection legislation would go through a similar process where each territory will design and adopt in isolation its own legislation. This would have an impact on the regional integration process as the move to harmonise the region under the umbrella of CARICOM will be hindered.

From a records management perspective, this study argues that the laws that exist do not always take into account the requirements for sound records or data protection management and at times seem to be created ‘in a vacuum’ as it relates to recordkeeping in practice and in principle. For example, national copyright legislation in many territories is not yet up to par with changes in the ICT technology being used in offices, libraries and archives. The legislation very often lags behind and does not deal with the real issues facing archives and libraries. Archives legislation, which is supposed to address national records management requirements, very often does not take into

⁵⁶⁸ Antoine, Rose-Marie Bell, *Commonwealth Caribbean: Law and Legal Systems* 2nd ed. (New York, 2008).

⁵⁶⁹ Based on interviews conducted with academics in the Faculty of Law at The University of the West Indies.

account other pieces of legislation that relate to recordkeeping and in many instances throughout the region has a low profile and is ineffectual.⁵⁷⁰

There is an issue of harmonisation of laws in the region. CARICOM has sought to address the issue by inviting international legal experts to the region as well as seeking consultation from other regions similar to the West Indies as part of a project called the 'HIPCAR project'. The HIPCAR Project was conceived by the ITU, the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication union (CTU) in response to requests from CARICOM States and other ICT stakeholders who saw the need for a more unified approach to the drafting legislation. It brings together the CARICOM governments, regulators, service providers, civil society, private sector, regional and international organizations to provide guidelines for harmonised policies and legislations.⁵⁷¹ The author was invited to attend a meeting of HIPCAR held in Barbados in 2013 and the project is still active, however, there has been little implementation activity resulting from the project to date. Another aspect to the lack of harmonisation is best seen with the manner in which data protection is being considered without a look at its compatibility with FoI legislation. In the jurisdictions reviewed by this study, it was noticed that these two pieces of legislation were dealt with in tandem or at least some consideration was given to how one would impact on the other. A case in point is the New Zealand model where both matters are dealt with

⁵⁷⁰ Based on discussions with directors of archival repositories across the region through the Caribbean Archives Association when attending meeting of the Executive and General Meetings.

⁵⁷¹ See HIPCAR Project under the auspices of CARICOM which is intended to harmonised ICT legislation across Member States at www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx. Accessed on 21 April 2014.

in one piece of legislation as was seen in Chapter 3. If this is not the approach adopted, as is currently happening in the region, there will undoubtedly be conflict, misunderstanding and misinterpretation of both types of laws by laymen i.e. general public.⁵⁷²

‘Adequacy’ with regard to international law is another aspect that must be considered to ensure successful implementation of data protection. The European Commission is the main proponent of this concept. The term ‘adequacy’ refers to assessing whether the privacy/data protection provisions in a particular jurisdiction are compatible with the EU Data Protection Directive.⁵⁷³ The region engages in business with multinational organisations and entities including *United Nations (UN)*, *Organisation of American States (OAS)*, *International Monetary Fund (IMF)* and the Department of International Development (DFID).⁵⁷⁴ Individual territories also approach international lending agencies, which may conform strictly to data protection provisions in Europe and other highly regulated jurisdictions, for grants and loans. In some instances, this would require the sharing of personal data or personal data transfer across borders and so it means that national legislation would have to meet standards and may be scrutinised by these bodies to assess their level of adequacy. In truth, the decision by these agencies to work with the region and/or individual nation-states could hinge on the strength of the legislation and whether it meets compliance requirements.

⁵⁷² An example of the adoption of Access to Information legislation without Data Protection legislation is in Jamaica.

⁵⁷³ European Commission – Justice, *Commission decisions on the adequacy of the protection of personal data in third countries* found at ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm. Accessed on 13 April 2013.

⁵⁷⁴ CARICOM Secretariat documents at www.caricom.org.

Obstacle No.3 – The Lack of Political Will

The holistic management of information particularly in governmental agencies has had very little appeal to the authorities in the West Indies. As seen with the selected jurisdictions reviewed in Chapter 3, the political will was evident in the reports from governmental agencies starting from the 1960s. This will help to propel the implementation of data protection. In the West Indian context, the progress of legislation and regulations has been slow to deal with issues such as records management, archives, freedom of information and informational privacy. To date, only one data protection law has been adopted in the region. Trinidad and Tobago adopted its Data Protection Act in 2011.⁵⁷⁵ However, as was shown in Chapter 2, this does not mean that the legislation is being fully enforced.⁵⁷⁶ Other islands including Jamaica, Barbados and Cayman Islands do have Data Protection bills. Some of these bills have been in existence for many years but there is no real push to adopt and/or enforce them.

Further to this, there is also the lack of will to allocate funding and ensure that persons are trained professionally to deal with the vast amounts of information being generated in all areas of society. There is little investment in some territories in information management infrastructure and the upgrade of systems to assure the highest levels of

⁵⁷⁵The Republic of Trinidad and Tobago, Data Protection Act, Act no.13 of 2011 found at www.ttparliament.org/legislations/a2011-13.pdf. Accessed on 13 April 2013.

⁵⁷⁶ Recent discussions with the National Archivist of Trinidad and Tobago have indicated that the legislation is not being considered by public bodies in their interactions with citizens and that education and awareness about the purpose of legislation is required.

security of information.⁵⁷⁷ The link between good records management and good governance is not understood. Leaders or managers are not held accountable for when information is lost, damaged or destroyed far less accessed without authorisation. This means that proponents of privacy/data protection would have to advocate at the highest levels for the right measures to be put in place. Undoubtedly, if this environment does not change, no real effort will be put into data protection management when dealing with the records and information of citizens.

Additionally, there is the question of what are the expectations, if any, of the citizens themselves when it comes to the collection, use and storage of their personal information. One of the 'side effects' of colonialism is that regional citizens, for the most part made up by a former slave-class, have been accustomed to not making demands on their governments or holding them accountable for their actions as it relates to their private information. There is little agitation for the better management of personal data in the region accept on an individual basis. This is evidenced by the fact that there are no lobbyists, watchdog groups or other privacy advocates in the West Indies putting up any form of public resistance to the way that organisations both public and private are conducting their business. Although in the digital age, regional citizens have a sense that their information should be treated with respect, they have not put forward any sustained effort to ensure that the systems are working the way that they should and they willingly offer up their personal data without too much inquiry.

⁵⁷⁷ Based on attempts to meet with political leaders and/or policy makers to discuss issues affecting archives and records management through the Caribbean Association of Archivists and the Barbados Association of Records and Information Management in the capacity of President.

6.2 Why Data Protection?: Key Drivers for Data Protection in the West Indies

It is important for this study to establish why data protection should be desirable to the West Indies as a region. Some in the region may argue, as witnessed in an interview with one legal expert in the West Indies as well as an interview conducted with the former Director-General of the Organisation of Eastern Caribbean State, Len Ishmeal, that this provision is 'really not necessary' and that 'the region has been surviving without it for all this time.'⁵⁷⁸ It is true that the region does not have the same drivers as those in the selected international jurisdictions who were mainly motivated by fears of the use of technology to collect, use and store personal information and the possible abuse of that information. As was argued in the previous section, this was never the case in the region. The citizens do not press their governments to uphold to these standards in any significant way. The question then arises, why data protection for the West Indies? This study has identified three main reasons for the need to implement data protection in the region. These are 1) to meet compliance requirements for international agreements mainly for economic purposes 2) to facilitate good governance for reasons of competitiveness and 3) to uphold global standards for human rights to remain in good standing on the global scene.

Driver No.1 - Meeting Compliance Requirements for International Agreements

The region has been actively involved with signing new international treaties and agreements as a grouping. One such agreement was signed on 15 October 2008. This agreement, the Economic Partnership Agreement (EPA) ushered in a completely new

⁵⁷⁸ Based on an interview with a notable regional attorney-at-law.

trading relationship between the Region and Europe.⁵⁷⁹ Thirteen Member States of the Caribbean Forum of African Caribbean and Pacific (ACP) States (CARIFORUM) and the European Community signed the agreement. The EPA was negotiated over a period of four years and essentially allows for reciprocal trading arrangements between countries of the European Community and CARIFORUM including goods and services among other things. CARIFORUM then Secretary-General, His Excellency Edwin Carrington, speaking at the signing ceremony stated that, 'This approach to the implementation of the EPA may yet provide the stimulus and the foundation for the region's effective insertion into the global economy.'⁵⁸⁰ Sir Shridath Ramphal also agrees that it would be 'sensible' for the region to take a unified approach to dealing with data protection.⁵⁸¹

Interestingly, Chapter 6, Title 2 of the Economic Partnership Agreement directly addresses the need for the Protection of Personal Data.⁵⁸² In Article 197 – General Objectives, it clearly states:

- I. The parties and the Signatory CARIFORUM States, recognising:
 - (a) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular, their right to privacy, with respect to the processing of personal data,
 - (b) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data;
 - (c) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject,

⁵⁷⁹ European Commission, *Economic Partnership Agreement, Protection of Personal Data* p. 65 at <http://trade.ec.europa.eu>. Accessed on 25 February 2011.

⁵⁸⁰ CARICOM, *CARIFORUM and EC sign EPA* found at <http://www.caricom.org> . Accessed on 25 February 2011.

⁵⁸¹ Interview with Sir Shridath Ramphal (Bridgetown, 2013).

⁵⁸² European Commission, *Economic Partnership Agreement, Protection of Personal Data* p. 65 at trade.ec.europa.eu. Accessed on 25 February 2011.

agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals regard to the processing of personal data, in line with existing high international standards.⁵⁸³

As a result of this requirement in the EPA, the CARIFORUM States have had to pursue or seek to develop policies which would allow them to take up a more active role in the global information economy. Towards this end, proper frameworks for privacy and security would need to be established in order for the region to meet the obligations as described by the EPA.⁵⁸⁴ CARIFORUM States thus must co-ordinate their effort in this regard, recognising the importance of protecting the right to privacy with respect to the processing of personal data, including the collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, blocking, erasure or destructions, as well as transfers of personal data across national borders.⁵⁸⁵

As was seen in Chapter 3, Trinidad and Tobago remains the only West Indian territory to have adopted a Data Protection Act in 2011.⁵⁸⁶ The Bahamas adopted its law in 2007 and Cayman Islands sought to adopt their legislation by summer 2013. Other West Indian territories namely, Antigua & Barbuda, Barbados and Jamaica still have data protection in bill form. Jamaica has recently revisited and re-opened discussions about the adoption of its Act. There is therefore still much work to be done to promote and

⁵⁸³ European Commission, *Economic Partnership Agreement, Protection of Personal Data* p. 65 at <http://trade.ec.europa.eu>. Accessed on 25 February 2011.

⁵⁸⁴ See Appendix 3.

⁵⁸⁵ CARIFORUM, *Project Proposal* to assist CARIFORUM with meeting its obligations under the Personal Data Protection chapter of the EPA (April, 2010).

⁵⁸⁶ See Appendix 4.

raise awareness about the need for data protection regionally to meet the challenges in the increasingly globalised and digital world.

Driver No.2 - Facilitating Good Governance

In discussing the *Repositioning the Caribbean within Globalisation (2008)*, Anthony Payne and Paul Sutton state that ‘good governance’ is important for economic and social development.⁵⁸⁷ They elaborate on the higher values that imply good governance by the World Bank in their report in 2005.⁵⁸⁸ This paper views data protection and other information rights legislation such as freedom of information as important pieces to the ‘puzzle’ of what would make regional governments operate at optimal levels of transparency and democracy. Data protection could fit into some of the following categories set out by World Bank that would reflect good governance.

The categories as provided in the report are:

- *Voice and Accountability* – measuring the political, civil and human rights. Payne and Sutton state that all the Commonwealth Caribbean countries have higher than global average rating. This would bode well for data protection implementation.
- *Political Instability and Violence* – measuring the likelihood of violent threats to, or changes in government. Three Commonwealth Caribbean territories fall below global average ratings namely, Guyana, Jamaica and Trinidad and Tobago.

⁵⁸⁷ Anthony Payne and Paul Sutton, *Repositioning the Caribbean for Globalisation* in *The Caribbean Community in Transition* ed. by Kenneth Hall and Myrtle Chuck-A-Sang (Kingston, 2008), p. 99.

⁵⁸⁸ World Bank, *Governance Report* found at www.worldbank.org/wbi/governance/govdata. Accessed on 25 February 2011.

- *Government Effectiveness* – measuring the competence of the bureaucracy and the quality of the public service. The only Commonwealth Caribbean country to fall below global average ratings in this regard was Guyana. However, this does not mean that there are not many challenges to be addressed in other territories.
- *Regulatory Burden* – measuring the incidence of market unfriendly policies. Guyana was the only Commonwealth Caribbean country to fall below global average ratings.
- *Rule of Law* – measuring the quality of contract enforcement, the police and the courts , as well as the likelihood for crime and violence. Two countries fall below the global average ratings, Guyana and Jamaica.
- *Control of Corruption* – measuring the exercise of public power for private gain. Two countries fall below global average ratings, Guyana and Jamaica.⁵⁸⁹

Out of these values/goals, the four most valuable to the study of data protection are 1) voice and accountability 2) government effectiveness 3) rule of law and 4) control of corruption. Improving the ratings in all four values would depend in part on how personal data is collected, used and stored by organisations. Personal data is required to ensure accountability, to improve services, to provide evidence in legal matters resulting in accountability and transparency and when personal data is properly managed, it can reduce levels of corruption. These values would need to be taken into consideration when seeking to implement a successful model for data protection in the West Indies.

⁵⁸⁹ Anthony Payne and Paul Sutton, *Repositioning...*p. 99.

Driver No.3 - Meeting Global Standards for Human Rights

In the post-World War II period, ideas of enlightenment spread across the globe and have led to the recognition of human rights as universal values.⁵⁹⁰ The United Nations has been instrumental in the dissemination and promotion of international human rights. This coupled with globalisation has put increased pressure on governments and their various entities to meet the expectations of their citizenry on matters related to the protection of fundamental rights. The modern West Indies is challenged with dealing with this global reality. Fundamental rights that need to be addressed include property rights and civil rights of equality, life, liberty and the security of the individual to freedoms of thought, religion, expression, association and so on.⁵⁹¹ A great deal of effort is being put in these areas throughout the individual territories, however, the rights of persons as they relate to aspects of privacy and data protection have not yet been pointedly addressed as fundamental human rights in the region.⁵⁹²

Additionally, demands on administration both in the public and private sector are ever increasing in the new global environment. The citizenry expects fairness at every level in administrative procedures, rational exercise of discretion and satisfactory remedies against the abuse of power. These expectations have begun to spread to regional citizens who are generally well travelled peoples. The more exposure to these ideals will heighten their sensitivity to the actions of their governments. Further to this, the region is witnessing the expansion of the role of government into areas that did not exist in the

⁵⁹⁰ Fiadjoe, (New York, 2008), p. 129.

⁵⁹¹ Fiadjoe, (New York, 2008), p. 150.

⁵⁹² Information based on interviews conducted with West Indian legal minds.

past. Greater roles bring greater responsibilities. It has been argued that membership of governments in regional governmental bodies such as the Commonwealth Caribbean (CARICOM), the sub-regional Organisation of Eastern Caribbean States (OECS) and the newly formed Association of Caribbean States is placing increasing pressure on West Indian governments to tackle a myriad of deep-seated social, economic and political regional issues.⁵⁹³

The various Constitutions of the West Indies usually include a section on the fundamental rights and freedoms of the citizenry called The Bill of Rights. Interestingly, these Bills of Rights are directly influenced by international sources of law.⁵⁹⁴ The Bills of Rights embody the provisions of international standards for fundamental human rights including the European Convention for Human Rights, the United Nations Universal Declaration of Human Rights and the American Convention on Human Rights.

In modern times, international law has been greatly influential on legal systems on a global scale.⁵⁹⁵ It may be seen in the West Indies as an important source of law. International law has had a significant impact on the constitutional law and human rights law. National legal systems have adopted the rules of international law by way of agreement in conventions and treaties or by way of practice. However, there are times when international law conflicts with domestic interests and particularly in the area of human rights and West Indian customs and norms may dictate a divergence from

⁵⁹³ A new draft Treaty of Basseterre reveals the plans for OECS to become a Commission in June 2010 found at www.oecs.org.

⁵⁹⁴ Sir Fred Phillips, *Commonwealth Caribbean: Constitutional Law* (London, 2002), p. 37.

⁵⁹⁵ Antoine, p. 205 – 209.

international jurisprudence.⁵⁹⁶ Caribbean courts in today's globalised environment have found that in order to be acknowledged and given the respect of the international community, they have to bring themselves more in line with international accepted standards and international law. This becomes even more important in the face of regional efforts in securing international funding and joining international bodies. It is this reality that could lay the groundwork for the development and incorporation of an international standard for data protection and a collective response to the protection of personal data across borders regardless of location regionally.

6.3 Data Protection in the West Indies: An Integrated Approach?

A question in this study is whether an integrated approach is the most suitable to solving the main challenges to the West Indies in designing a framework for data protection implementation. Several attempts had been made to federate the region politically and economically throughout the course of its history without lasting effects. In the post-1930s period, federalism was seen by the region's politicians as a means towards political independence. Beyond this, as argued by noted Caribbean integrationist economist Norman Girvan, other perceived benefits include the scope for enabling economic gains as there would be a pool of resources that could be shared among the territories;⁵⁹⁷ Integration would also result in greater legal and administrative efficiency because a federal approach would result in harmonisation in the legal systems and administrative frameworks for good governance. Some regional

⁵⁹⁶ Based on interview with a regional legal expert in 2009.

⁵⁹⁷ Norman Girvan, *The quest for regional integration in the Caribbean – successes and challenges*, Paper presented at The University of the West Indies, Mona, Jamaica, 2011.

political scientists such as Cynthia Barrow-Giles also agree that integration would enable enhanced security from a military and surveillance standpoint as the territories would be in a position to defend each other collectively.⁵⁹⁸ The geographic proximity and historical and cultural commonality should have been unifying factors but unfortunately, to date, these features have not been enough to foster true regional integration among the West Indian territories.

6.4 Developing a West Indian Framework for Data Protection: Lessons Learnt

The comparative research conducted in this study has resulted in a major conclusion. There is no model that would totally serve the needs of the West Indies as a region. This study then proposes that what can be gleaned from the international jurisdictions and the other sources of investigation of this topic would assist with the development of a framework for the West Indies region. This chapter will provide that framework from a records management perspective. It acknowledges that the framework should be further expanded on by other key stakeholders that would need to be involved in developing a West Indian approach for data protection implementation. The study also acknowledges that there are other perspectives that would need to be taken into consideration to produce a complete and workable model for the West Indies. Additionally, any framework or eventual model provided must seek to address the obstacles outlined at the beginning of this chapter.

⁵⁹⁸ Barrow-Giles, Cynthia, *Introduction to Caribbean Politics* (Kingston, 2002), p. 265

Key Lessons to the West Indies from DP Models

Lesson #1: Establish an Independent Authority for Privacy/Data Protection

One of the first lessons learnt from the selected jurisdictions is that it is prudent to establish an independent authority for the regulation and enforcement of privacy/data protection. This means that the data protection authority must be impartial, that is, free from any political affiliations or other influences based on the needs of select interest groups within society. This would be critical to ensuring that both public and private agencies are subject to the same requirements and are held to the same standards. The Information Commissioner should not have his or her authority challenged or undermined in any way by any political actor or activist and should be in a position to bring the full force of the law to any agency or individual without fear of victimisation especially with a view to imposing sanctions and penalties.

Lesson # 2: Institute a 'One-Stop' Shop for Data Protection Regulation

In harmony with lesson #1, having a single point of contact for national data protection regulation to supervise processing operations could have a positive effect on the strength of the regulatory framework as is currently being looked at in the EU. As seen in the US situation where there is no central authority to go to for direction and guidance, the risks of breaches could potentially increase. This type of environment can be very unstable for privacy protection in general except in particular sectors where special attention is usually paid to the management of information such as in health. There must be clarity and not a patchwork of legislation and supervisory authorities which can make it too complex for both organisations and individuals to figure out

where to go for access to the right information and guidance. It would also help to reduce inconsistencies in the regulation of privacy/data protection.

Lesson #3: Develop Strong Data Protection Principles

This study posits that principles are even more important and lasting than law. Whereas laws constantly are updated and changing to meet the shifting environment, the principles will remain static and serve as a 'compass' where laws are unclear. In all of the selected jurisdictions, there are guiding data protection or privacy principles. The principles first set out by the Organisation for Economic Co-operation and Development (OECD) continue to be very relevant even though they were first articulated in 1980. All the jurisdictions under review in this study, with the exception of the US, developed comprehensive privacy/data protection principles that underpin their privacy/data protection regime.

Lesson #4: Ensure Consistency in the Legislation (Harmonisation)

Data protection legislation should not be overly prescriptive but a balance must be struck to ensure that it is compatible with other national, regional and international laws. Harmonisation is critical in the pursuit of improved economic relations and functional cooperation particularly at a regional and international level. The world is globalised as a result of emerging technologies and no country should exist 'in a vacuum'. Harmonisation would help to reduce the tensions between differing data protection regimes such the EU and the US and ease the conduct of international business. At a national level, data protection legislation should be synchronised with

Freedom of Information legislation and/or any other type of information management legislation such as Computer Misuse Acts. Any exemptions and exceptions to data protection law would also need to be carefully considered.

Lesson #5: Introduce Effective Judicial Remedies and Adequate Sanctions

An important lesson learnt is that appropriate judicial remedies and adequate sanctions should be established to ensure that data protection regulation and enforcement is effective. In instances where the sanctions are too weak, it was seen that breaches were higher as agencies did not invest the necessary effort and resources to properly manage data protection. As a result, some jurisdictions are reviewing this aspect of their legislation. The punishment must fit the crime and only meaningful sanctions will achieve the desired effect.

Lesson #6: Strengthen Administrative Structures/Systems

The region must seek to strengthen its administrative structures and systems. This would involve reducing bureaucratic burdens and streamlining operations with effective systems that manage the risks involved in dealing with organisational information. Centralisation wherever possible will enhance consistency in management. It is also critical to develop all the right policies and procedures as well as choosing the right hardware, software and equipment to ensure the highest levels of security. Privacy risk assessments and audits should be conducted at all levels and in all functional areas of the organisation. In addition, traditional paper-based systems should be maintained at the same standards as electronic systems and vice versa.

Lesson #7: Improve Organisational Infrastructure for DP Management

The breaches recorded in Chapter 3 have shown that effective data protection management is required at the level of the organisation. This could only be achieved when the key stakeholders engage in effective cooperation and collaboration. Teams for data protection management should be established to work collaboratively in the design of appropriate policies and procedures. As was discussed in Chapter 4, records and information management professionals should be included in any data protection management planning and activities.

Lesson #8: Develop Appropriate Data Protection Guidelines and Codes of Practice

Codes of Practice and Data Protection Guidelines can be very useful when formulated and made available to organisations operating in specific sectors. These industry codes, however, should always be reviewed within reasonable timeframes to ensure that they are in keeping with constantly changing legislation and the technological environment. In some cases, these codes and guidelines are the only way for data processors and controllers to properly interpret the law as it relates to their specific business needs.

Lesson #9: Define Clear Requirements for Data Transfer across Borders

It is also important that requirements for data transfer across borders are clearly defined. Personal data is required for electronic commerce, travel and immigration, criminal investigations and national security. The issue of 'adequacy' is still being reviewed and debated between the EU and the US in spite of their 'Safe Harbor' Agreement. Arrangements such as these are necessary as a result of the changing legal

and digital environment in order to maintain coherent practices across borders. Countries need to ensure that they are comfortable with the level of adequacy in other jurisdictions that they conduct business with and where necessary a legally binding agreement should be put in place. Harmonisation of laws is the best approach to combat the problem of adequacy.

Lesson #10: Empower Citizens with Choices about their Personal Data

Ultimately, data protection seeks to empower citizens with the ability to control the collection and use of their personal data held by public and private organisations. In cases where citizens are not afforded what is now considered the 'right' to data protection, they are left vulnerable to the misuse of their data for illegal or ill-willed purposes. As was previously mentioned in the study, the protection of this type of privacy could be a matter of life or death. Jurisdictions that employ the measures stated in Chapter 3 to protect the citizen's right to choice of how they want their data to be treated, will be viewed in the globalised world as the more advanced societies and will gain the trust of consumers and clients. This would inevitably lead to increased productivity and competitiveness and could only bode well for the society at large.

6.5 Recommendations to the West Indies

Recommendation #1: Choose the Most Feasible Approach

An examination of the international regimes in Chapter 3 revealed that many tensions exist among 'actors' particularly those with federal systems, that may also manifest themselves in an attempt to implement data protection in the West Indies. The

approach chosen will be important to reducing those tensions. It must be noted that the region sits strategically between the US and Europe. Although there are historical ties to the UK, in its contemporary history, the region has been aligning itself to the US. This may result in the region being influenced by the two vastly different approaches. What the region's policy-makers have to take into account is which alignment serves best as it relates to its development.

After close examination of the existing approaches for privacy/data protection, this thesis concludes that there is no 'model' approach for the West Indies rather the West Indies can seek to develop a 'framework' based on the lessons learnt from other jurisdictions. The jurisdictions reviewed have revealed that there is no 'one size fits all' approach to implementation of data protection. This is mainly because of the combination of historical, political, social and economic factors that influence how privacy/data protection is defined, perceived and responded to in these individual societies/regions. The word 'model' which connotes something to be emulated in its entirety is therefore not applicable in this study. The term 'framework' is more suitable as the main elements of these approaches most adaptable to West Indian society could be extrapolated and brought together towards formulating sound recommendations for the West Indies.

The EU approach has proven to be the most comprehensive and scalable one and with some adaptations may be more suitable to the West Indies. It has very useful elements in its provisions for regulating and the infrastructure established for monitoring and

enforcement that may be applicable in the West Indian context. It is therefore recommended that an overarching, independent Data Protection Supervisor, similar to that in the EU, be placed on top of the pyramid of regulation and enforcement. Offices for Information Commissioner and Assistant Information Commissioners based on geographic location would also be a good model for the WI to adopt. These Commissioners should report directly to the Data Protection Supervisor. It would also be prudent to employ a Data Protection Officer on a mandatory basis for companies of a medium to large size to ensure that the responsibility for data protection compliance is clearly designated to a high-level officer. This would also improve the aspect of accountability. The following diagram is a recommended organisational chart for DP regulation in region.

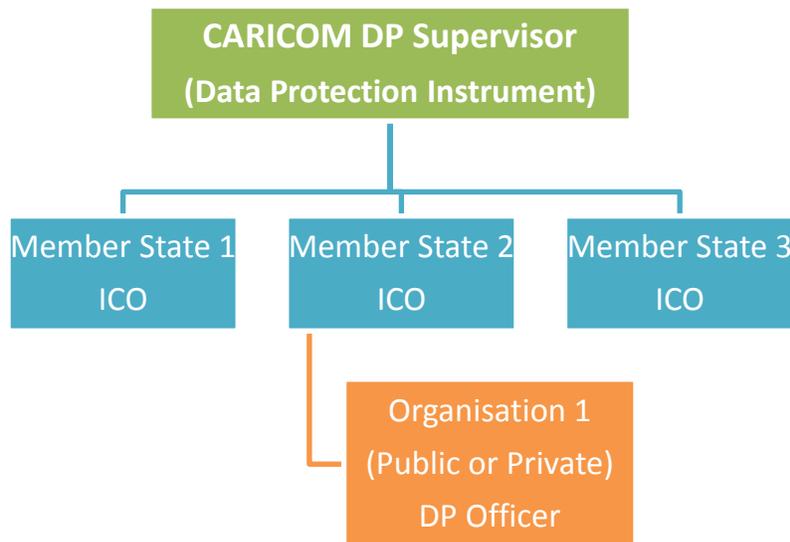


Figure 8 Proposed Framework for Regional DP Regulation
produced by the author

It is further proposed that in the current organisational structure of CARICOM, the CARICOM Secretariat which serves an administrative, policy-advisory and coordinating role could be the branch that has oversight of data protection. The Data Protection Supervisor could be placed under the most appropriate Division suitable to deal with information rights in Member States.

Additionally, the region could revisit the first attempt to address the globalisation of data protection made by the Organisation for Economic Co-operation and Development (OECD). The OECD developed its data protection guidelines in 1980 entitled, 'OECD Guidelines on the Protection of Privacy and Transborder Flows on Personal Data'. The OECD guidelines were meant to serve as the common denominator between Europe and the United States approaches to data protection as OECD Member countries.⁵⁹⁹ It was felt that the disparities in national privacy/data protection could hamper the free flow of personal data across frontiers. These flows increased and grew further with the widespread introduction of computers and communications technology. The OECD therefore sought to prevent serious disruptions in important sectors of the economy, such as banking and insurance.⁶⁰⁰ In view of the success of the approach taken by the OECD, this study posits that the similar guidelines be developed by CARICOM to provide sound guidance that would enable the region to overcome some of its challenges with harmonisation and the free flow of information.

⁵⁹⁹ András Joris, *Data Protection in Europe* at <http://www.dataprotection.eu>. Accessed on 17 February 2009. p.1.

⁶⁰⁰ OECD, *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data* at www.oecd.org. Accessed on 28 January 2009.

Recommendation #2: Strengthen the Regional Legal System toward DP Implementation

A move to strengthen the regional legal system was made when the Caribbean Court of Justice (CCJ) was established on 14 February 2001 by the 'Agreement Establishing the Caribbean Court of Justice.' The agreement was signed on that date by the Caribbean Community (CARICOM) states of Antigua & Barbuda; Barbados; Belize; Grenada; Guyana; Jamaica; St. Kitts & Nevis; St. Lucia; Suriname and Trinidad & Tobago. Two further states, Dominica and St. Vincent & The Grenadines, signed the agreement on 15 February 2003, bringing the total number of signatories to 12. The CCJ was inaugurated on 16 April 2005 in Port of Spain, Trinidad & Tobago.⁶⁰¹

The CCJ was intended to be the final court of appeal replacing the UK Privy Council.⁶⁰²

The stated mission of the CCJ is to perform to the highest standards as the supreme judicial organ in the Caribbean Community. In its original jurisdiction, it ensures uniform interpretation and application of the Revised Treaty of Chaguaramas, thereby underpinning and advancing the CARICOM Single Market and Economy. As the final court of appeal for member states of the Caribbean Community it is intended to foster the development of an indigenous Caribbean jurisprudence.⁶⁰³ However, to date only Barbados and Guyana has subscribed fully to the jurisdiction of the CCJ. There are what appear to be insurmountable constitutional challenges in some territories with the abolition of the Privy Council as the final Court of Appeal. However, there are positive

⁶⁰¹ CARICOM, *Caribbean Court of Justice* found at www.caribbeancourtofjustice.org. Accessed on 21 July 2009.

⁶⁰² Albert Fiadjoe, *Commonwealth Caribbean Public Law* 3rd Edition (New York, 2008), p. 209.

⁶⁰³ CARICOM, *Caribbean Court of Justice* found at www.caribbeancourtofjustice.org. Accessed on 21 July 2009.

factors that are in favour of the CCJ as a regional Court of Appeal. These include among many:

- The unique institutional strengths of the CCJ;
- The current expertise of the CCJ which cuts across the civil, law, common law and international law;
- The regional character of the court as a plug for its independence ensuring that no one attempts to interfere with the court's operations;
- The innovative nature of the court with its accessible, simple court-driven rules intended to guarantee speedy disposition of cases;
- Visible signs of the beginning of a West Indian jurisprudence;
- The CCJ's instruments are not an imposition by regional governments but rather the result of constructive civil society representations.⁶⁰⁴

It is therefore recommended that the CCJ could play a role in the judicial oversight of data protection/privacy at a regional level. The groundwork has been laid for the modernisation of the justice system in the region that would provide a solid foundation for the introduction of modern, international legislation as well as allowing for its successful implementation. The advantage of the CCJ being politically independent is an added strength as well as its ability to adapt to the cultural nuances of the West Indies. At present, there is no direct link between HIPCAR project and the CCJ other than they are both administered under CARICOM. However, the HIPCAR project is the first step towards harmonising data protection legislation regionally and that should lead to a

⁶⁰⁴ Fiadjoe, p, 208.

unified approach to data protection implementation and enforcement of data protection law in the West Indies with the CCJ interpreting and upholding the law. The infrastructure for data protection implementation on a regional level is there, it is the political will to take it forward that is lacking.

As it relates to the legislation itself, in an ideal situation CARICOM Member States would be subject to a single piece data protection legal instrument similar to the EU model that could allow for national legislation to be developed in keeping with a singular legal instrument. However, this legislation may have to be introduced at a later stage as the region is not yet prepared to adopt regionally centred legislation. In the initial stages, a Protocol could be introduced and signed between Member States to adopt regional standards for data protection. The disadvantage here is that a Protocol would not have the judicial weight of domestic legislation and therefore adequate sanctions and judicial remedies cannot be applied down to the level of an individual Member State. Since Trinidad and Tobago has adopted its DPA and some of the territories namely Antigua, Barbados and Jamaica have gone ahead and drafted their own legislation, it may be best to use the CARICOM protocol or agreement as the baseline standard to which these national laws are held, giving the territory leeway to tailor the law to best suit their situation.



Image 16 Inauguration of the Caribbean Court of Justice (2001)
www.caribbeancourtjustice.org

Recommendation #3: Strengthen the Role of Records Management in W.I. Data Protection Management

One of the major obstacles foreseen to regional implementation of data protection at the beginning of the chapter is the state of its recordkeeping, this thesis contends that understanding the state of recordkeeping and archives administration in the region and addressing it is essential to successful data protection management. Further to this, the region has not fully explored a unified and coordinated approach to administrative structuring and related activities such as recordkeeping. Each individual government has tried to grapple with its challenges on its own or has looked outwardly as they traditionally have for assistance. External sources of assistance have not produced the best results as the region tends to have its own unique approach to dealing with matters

and so recommendations that may work in other jurisdictions do not always fit naturally into West Indian life and culture.

The last official survey of the state of recordkeeping in the region took place in 2001⁶⁰⁵ and showed that ten territories were beginning to institute formal records management programmes and there were ongoing recordkeeping initiatives even though it has been a slow process. Over ten years later, the situation has not changed significantly. The territories are still struggling to establish or maintain a high standard of records management. The Caribbean Branch of the International Council on Archives (CARBICA) continues seeking to update archivists about all matters related to records management and electronic recordkeeping including data security and privacy. The Association of Commonwealth Archivists and Records Managers has also provided seminars and meetings resulting in resolutions being passed to strengthen the response of professionals. Associations who advocate for records management and privacy such as ARMA International, the US-based association for records management, have formed chapters in Jamaica, Trinidad and Barbados and they seek to conduct various educational and outreach programmes that attract a range of professionals to raise awareness about these pressing issues.⁶⁰⁶

However, Caribbean governments must play their role in the stabilisation of the recordkeeping environment in the region that would result in the benefits discussed in

⁶⁰⁵ The survey was conducted by the Caribbean Association of Archivists now referred to as CARBICA. The survey was never published.

⁶⁰⁶ Sharon Alexander-Gooding and Sonia Black, A National Response to ISO 15489: A Case Study of the Jamaica Experience, *The Information Management Journal* March/April 2005, Vol. 39, No. 2, p.62.

Chapter 4 of this study. Caribbean archivists and records managers struggle to capture the attention of Ministers and senior officials. When records and archives management is established by regional governments in the fullest sense, only then would the right data protection mechanisms previously discussed be put in place to ensure that data protection requirements are being met. In short, the absence of records and archives management in public and private organisations means that the successful implementation of data protection would be severely impaired. It is hoped that the linkages between the two pursuits have been made clear throughout this paper.

The point was also made in Chapter 3 that effective risk management for data protection must also take place at organisational level. It is recommended that the right stakeholders be brought together to ensure compliance with data protection law in regional agencies. This would include the Data Protection Officer (DPO), a representative from IT as well as Legal Counsel, wherever applicable. As a result of the high level of privacy protection required with personnel records, a representative from the Human Resource section within organisations would be desirable. This should not overshadow one of the most important arguments in this paper that collaboration of records and information professionals in data protection management is critical. The research has shown that this has not been recognised in some major jurisdictions. Archivists and records management are many times in the fore-front of management systems that contain vast amounts of personal data and they should be involved in decision-making and allowed to sit with other key stakeholders to design data

protection principles and policies. The following diagram is a recommended organisational chart for data protection management at organisational level.

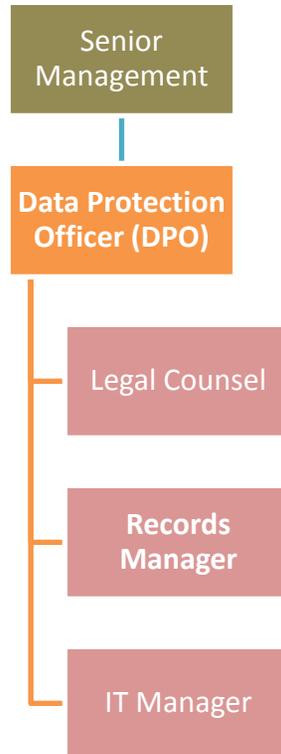


Figure 9 Proposed Framework for Organisational Data Protection Management
Produced by author

Recommendation #4: Develop Sound Regional DP Principles

The development of regional policy statements would be a significant achievement moving forward. As was seen with all jurisdictions, with the exception of the US, principles form the basis of data protection legislation even in the face of rapid changes. The region could again re-visit the OECD's principles which would have adopted in some form by various regimes across the globe.⁶⁰⁷ The following is a description of the core principles that need to cover the following areas:-

⁶⁰⁷ OECD, *OECD Privacy Principles* at oecdprivacy.org. Accessed on 25 April 2014.

1. Collection Limitation – establishes limits to the collection of personal data. Collection should be fair and lawful.
2. Principle for Data Quality – ensures that personal data when collected is kept accurate, up-to-date and complete.
3. Principle for Purpose Specification – ensures that the purpose is specified as well as the time frame in which data needs to be kept to fulfil the purpose.
4. Principle for Use Limitation – ensures that personal data when collected is not disclosed with the consent of the data subject or the authority of the law.
5. Principle for Security Safeguards – ensures that personal data is protected with reasonable security measures and from risks of unwarranted disclosure.
6. Principle for Openness – ensures that the means used and main purposes behind the collection and use of personal data are openly stated and readily available to data subject by the data controllers
7. Principle for Individual Participation – ensures that the data subject has the right to obtain requested information or communication from the data controller, including challenging data related to him or her or requesting erasure and/or amendments within a reasonable manner and timeframe
8. Principle for Accountability – ensures that the data controllers is held accountable for compliance with data protection legislation

These principles should serve to guide the data controller, processor and subject even where there is no data protection legislation. West Indies organisations should seek to act in the ‘spirit of the law’ in the absence of legislation to meet international standards of practice.

Recommendation #5: Raise Public Awareness and Education about Privacy/Data Protection

One of the areas that need to be urgently addressed in the region is the education of citizens as to their rights including their right to privacy. As was discussed in the section on the main obstacles, the citizenry have traditionally been accustomed to government

and other large organisations 'controlling' how their information is handled without much participation. Citizens have not been particularly demanding of how their information is used but that is mainly because they are not aware of the risks. The main information on privacy is only being filtered through in the international media where almost daily there are news stories about the invasion of privacy in some form.

It is therefore recommended that regional governments take a more pro-active stance to openness, transparency and accountability and one way of doing this is to educate and raise the awareness of their citizens about the perils of privacy and the need for data protection. This would be even more crucial as the technologies are advancing and outpacing practice and legislation. Citizens must know what risks they are up against and how organisations both public and private are coping with the risks. Being secretive and closed can only lead to the eventual downfall of a company when data protection legislation takes effect on a regional scale.

On a private level, West Indians must also be made aware of the dangers of conducting business on the Internet and the pitfalls of social media. Information is no longer confined to small, intimate spaces but has gone global in an unprecedented way.

6.6 Conclusion

The ushering in of data protection as a public policy in the West Indies is still in the embryonic stages with only one of the territories fully adopting its own Data Protection Act to date. There has generally been a slow pace of enactment of comprehensive

legislation and this has mainly been as a result of the lack of awareness of West Indians as to how their privacy is being affected in modernised organisations that increasingly use technologies to conduct their day-to-day operations.

The research in the form of interviews has shown that some regional law makers do not see the pressing need for this type of legislation and believe that it is already adequately covered by other legal instruments. With the rapid advances in technology, including intrusive devices, portable devices, social media networks and 'cloud' computing, the 'door is wide open' and opportunities exist for attacks on people's identity and other cyber related criminal activity to take place. A dedicated law will not totally prevent breaches as was seen in Chapter 3 but it would reduce the risks when properly executed and at least justice would be served to those who deliberately undermine personal privacy for selfish or malicious purposes.

As it relates to the implementation of data protection in the West Indies, it is clear that the region is lagging too far behind these developments. No longer can the West Indies wait to change its compliance landscape to be on par with the rest of the world. We now reside in a global community drawn closer together by technology. What affects one jurisdiction impacts on another. Although the drivers for the region are not the same as its international counterparts, the risks are the same. The region does not only need to strive to be competitive and attract support from global benefactors but to protect its citizens from unwarranted attacks on their rights and privileges. Data

protection is now recognised as a basic human right and a progressive region must put measures in place to ensure that it could cope with the realities of the digital world.

The West Indies must then acknowledge that the world of records and information management is rapidly changing and be prepared to cope with these changes. The best means to achieve this objective is to build up and fortify the foundation on which all sound information rights regimes are built, that is, to institute proper, fully functioning, accountable and transparent records and information management systems.

7. CHAPTER 7

CONCLUSION

7.1 Data Protection and Records Management: Where Are We Now?

The relationship between records management and data protection is significant and should be exploited to ensure successful implementation of data protection. The relationship has always existed but was not highlighted by those inside or outside of the profession in a meaningful way. In an interview at The National Archives of UK, in speaking about the relationship between records management and data protection, it was stated, 'long before data protection law applied, archivists and records managers were applying that sensitivity in the interest of people'. It was further explained that, 'data protection law codified a great deal of what was already done [by records managers and archivists] but required a greater deal of accountability on the part of the records manager and archivist.'⁶⁰⁸

This study shows that the relationship could be enhanced using the key findings, mechanisms and conclusions of the previous Chapters. Further to this, the thesis suggests that some of the key issues of data protection/privacy could be addressed in a direct way by including a records management approach to the implementation and management of data protection/privacy. It would therefore be prudent for jurisdictions to enact and update both data protection and archival legislation (covering records management provisions) simultaneously. This would ensure that the two pieces of

⁶⁰⁸ Interview at The National Archives UK (Surrey, 2010).

legislation are always compatible. The lessons provided in the jurisdictions point to a clear need for collaboration with records managers and the other major players in managing privacy at the organisational level. The other critical professionals include those from disciplines such as law, sociology, public policy, human resource management, finance and IT. Forming alliances in research between these professionals could make a significant difference in dealing with this increasingly global challenge in a digital world. Ultimately, the region of the West Indies should examine its current position with records management and ensure that this area is not excluded in the quest to implement and uphold data protection legislation.

From the onset of this study, the research suggested that the dramatic changes that took place in society in the 1960s were as a result of revolutionary advancements in technology and this was the main driver leading to data protection arising as a public issue in that period. Fifty years later, this study agrees that technology is the tool that facilitates the widespread collection, distribution and manipulation of personal data and that advances in technology underpin the need for data protection. The study goes further by suggesting that today's technology is more intrusive and pervasive than at any point of mankind's history and so the need for data protection is even more vital in today's digital world than ever before. Privacy, therefore, is under its most severe threat in our current era due to the capabilities of technology. This is evidenced by the number and types of breaches as well as the rise of privacy advocates that seek to 'whistle-blow' and counteract breaches in information-driven societies.

However, the study concludes that real cause for the need for data protection is the human factor which is inescapable in understanding how personal data is handled. The 'tool' of technology when placed in the wrong hands can have very disastrous or damaging effects on the lives of individuals. People working with records and information in public and private entities as well as those who interact with these entities, are empowered with the means, knowledge and skills to breach controls that seek to deal with access and use of personal information in unimaginable ways that affect the lives of 'data subjects'. As witnessed in the jurisdictions discussed in Chapter 3, breaches may also occur unintentionally due to human error because technology, even when well designed, allows the storage of information in the most accessible ways through networked databases, cloud storage and the World Wide Web. Therefore, data protection regulation, enforcement and management is a noble attempt at protecting personal information but this attempt is fraught with what appears to be insurmountable challenges because of how people are using the new devices and the Internet to carry out acts of terrorism, hacking, identity theft and spying. The social media revolution and unlimited remote storage of information through 'cloud computing' adds new dimensions to these risks. The harsh reality is that as long as people are empowered with intrusive tools, devices and opportunity, there will always be the need to find new, innovative solutions to protect personal data. Therefore, the study posits that the need for data protection and the discipline of records and information management is greater now than fifty years ago when the two pursuits emerged.

7.2 Reflections on the Thesis

With this in view, this thesis has provided a perspective on the subject of data protection that has never been presented in any writings to date. It has used a multi-disciplinary approach but has principally been written and argued from the viewpoint of an archivist/record manager. The thesis has considered sociological theories such as 'Post-industrialism' and the 'Information Society' from the 1960s and has considered new developing theory on the 'Social Media Revolution'. This study has examined the background to human behaviour and societal changes that impact on that behaviour because they were seen as critical to putting the need for data protection in context.

Chapter 1 of the thesis has laid the groundwork for understanding the context of the subject of the thesis. It has reviewed the existing literature and has discussed definitions and interpretations of privacy and data protection across the selected jurisdictions with a view to showing how the concept of informational privacy and data protection as well as the terminology evolved through time and space. This chapter has shown how there is lack of harmonisation with data protection legislation due to historical, cultural and other factors. It has looked at attempts to develop international standards and come to international consensus on how to deal with data protection across borders. This chapter has also provided a background to records management as a discipline showing how this pursuit emerged in the same period as the public problem of data protection and has highlighted other synergies between the two pursuits. Finally, the chapter described the historical background of the West Indies towards understanding the obstacles and challenges this region would face in implementing data protection.

Chapter 2

This chapter has dealt with the historical background and development of the West Indies, showing its uniqueness as a region and providing evidence of its current status with data protection. It has examined the legal and recordkeeping traditions inherited by the regions and discussed how these traditions impact on the slow progression of data protection and archival legislation. It has laid the foundation for the later conclusions and recommendations to the West Indies on how to successfully embark on data protection implementation.

Chapter 3

This Chapter has been a pivotal chapter in the study. It has outlined the four data protection models across the selected jurisdictions, comparing and contrasting these models in order to unearth which of these models would best suit developing a framework for the West Indies. After examination of the models, it was concluded that a framework rather than a model could be developed for the West Indies. Chapter 3 of the thesis has assessed the successes and failures of the models by examining cases of breaches which appear to be typical evidenced by listings of breaches captured in the annual reports of Information/Privacy Commissioners. The breaches provided critical evidence the provisions for data protection have not reached that organisational level and that there is need for a sound records management environment at that level for the successful implementation of data protection. Therefore the thesis has concluded that data protection must be dealt with in a comprehensive way at all levels of society. This means that management of data protection should be instilled right down to the

level of the individual. Staff within a public or private organisation must be taught proper data protection practices through persistent efforts at training and a good communication strategy. At the level of the 'data subjects', citizens should be made aware through an education programme of how their personal information held by organisations is managed and should be advised to employ sensible practices when creating personal records using social media and other technologies.

Chapter 4

Chapter 4 has provided a detailed focus on the role that records management can play in all aspects of data protection management. A new approach for the identification of personal records in recordkeeping systems has been introduced along with a hierarchy for privacy protection. This chapter has also provided guidance for records practitioners in the form of surveys and questionnaires and outlined key mechanisms to employ in records management programmes. It has also provided recommendations on the role of responsibilities in organisations as they relate to the management of data protection from the creation to the final disposition of records. The chapter briefly highlights some of the key issues when dealing with records containing personal information in archival collections.

Chapter 5 of the thesis has examined how new technological trends and devices has impacted on data protection and records management. It has discussed some of the new proposals of the very influential European Union data protection regime. It has shown how some of the principles such as 'the right to be forgotten' will have

implications for data retention and data erasure that could lead to gaps in records for future generations. The chapter has explored how practices such as 'life-logging' and 'cloud-computing' impact on how people are remembered through records captured and stored remotely in cyber-space.

Chapter 6 has been the most prescriptive chapter as it has provided recommendations to the region of the West Indies on the implementation of data protection. This has been based on the comparative data from the selected jurisdictions discussed in Chapter 3. Firstly, the chapter has set out what are the perceived obstacles for successful implementation of data protection. Secondly, it has stated the key drivers for data protection implementation. Thirdly, it has outlined the lessons learnt and finally it has provided a framework or strategy to implement data protection on a regional level. The information in this chapter would not only be useful in the context of the West Indies but in other regions that are similar in background and development.

Chapter 7

Chapter 7 has provided the overarching conclusions of the study and positioned records management as having a significant relationship and role in the quest to successfully implement data protection. It has acknowledged that records management alone cannot provide all the answers in this complex issue and recognises the need to collaborate with other key professionals towards this end. It also raises new and interesting questions that require further investigation beyond what has been done in this study.

Chapter 8

Chapter 8 will show future prospects for the topic on the relationship between data protection and records management. It introduces new developments in the influential EU data protection regime as well as new trends and new devices that will impact data protection in records management. It also suggests activities that should be taking place by professional bodies for records managers and archivists within organisations to cope with the new changes.

7.3 Data Protection and Records Management: Where Are We Going?

As it relates to the future of data protection and records management, the thesis concludes that privacy and data protection legislation will never keep abreast of technological advances. The provisions will always fall short of the capabilities of the technology. Therefore, the study posits that ensuring proper management of records and information will continue to be absolutely critical in this quest to prevent the unwarranted disclosure of personal information given these circumstances. Technological solutions and legislation alone will not be enough to combat the behaviours of people in the future. Although the study is not suggesting that records and information management will solve the problems in their entirety, it proposes that a good records and information management foundation would create a more stable environment for data protection management through reliable policies, procedures and practices.

Beyond this study, in-depth research into the impact of technologies on societies and the behaviours of people is required. Questions such as how does the social media revolution influence the definition of privacy must be explored. In addition, what effect will devices such as flying drone cameras or discreet wearable computer devices have on personal data capture and distribution? Will governments increase surveillance on citizens in their anti-terrorism and other crime prevention campaigns and if so, what will be the response of citizens? Further to this, how will 'whistle-blowers' such as Edward Snowden be judged by society? Finding the answers to these questions must be tackled in a multi-disciplinary way for optimum results.

8. CHAPTER 8

FUTURE WORK

The year 2015 will mark significant additions and developments in the world of data protection. One such development is that the EU Data Protection Regulation first proposed in 2012, has been delayed until 2015.⁶⁰⁹ The other developments to come will mainly be as a result of three factors 1) the use of new technologies in networking, computing devices and the on-line environment 2) proposed reforms to the very influential EU data protection regime and 3) the new global standard for privacy in ICTs. Privacy and data protection as a public policy is on the minds of individuals even more now than ever before in the history of mankind. The views and opinions of the masses of citizens across all the jurisdictions reviewed are very accessible as social media becomes the most widespread tool of communication. In these online discussions, the re-occurring theme is that privacy in today's environment is dying and in peril. There is also a concern about how records and information is being collected, stored and used by governments in particular as seen in the US context. This echoes the initial concern that drove societies in the 1960s to adopt data protection legislation. The dynamics are constantly changing and one could ask what will be the next big issues to grapple with in informational privacy and data protection in the next five years?

⁶⁰⁹ European Commission, *Article 29 Working Party - Work Programme 2014-2015* at ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_en.pdf Accessed on 13 September 2015.

The next section 8.1, forecasts the main topics that should be subject to further research and debate in the immediate future of data protection. The section includes: an introduction to some of the emerging and/or growing new technologies and practices; an overview of the proposals and new concepts being discussed in the EU data protection regime; a look at the new global standard for data protection; possible ways to educate the masses on data protection; a proposal for the International Council on Archives to assist archivists/records managers with coping with the changes on a global scale and finally a call to formulate toolkits specifically designed for archivists and records managers to conduct data protection management in their archives and records management programmes.

8.1 Addressing DP in New Technologies and Concepts

a) Emerging Organisational Practice – Bring Your Own Device (BYOD)

There is currently an emerging trend in today's organisations to Bring Your Own Device (BYOD) to work. This essentially means that employees could bring their own computing devices for use at work to conduct business. These devices are typically laptops, smartphones and tablets. This practice raises a number of data protection concerns particularly as it relates to the data security and would need to be more fully explored by advocates of privacy as well as records practitioners. In the UK, the Information Commissioner's Office has rightly prepared guidelines to safeguard personal data from loss, theft and/or destruction.⁶¹⁰

⁶¹⁰ Information Commissioner's Office, *Bring Your Own Device (BYOD)* found at http://ico.org.uk/for_organisations/data_protection/topic_guides/online/~media/documents/library/Da

Notably, in today's organisations, there is an increasing demand by senior officers in particular to be able to operate and conduct the business of the organisation from any location. For archivists/records managers, new skill sets will be required to cope with this practice. This practice marks a further divergence from centralised recordkeeping systems and could result in increasing lack of control of the organisation's information assets. How do archivists/records managers ensure that business data containing personal data is kept separated or segregated? What additional mechanisms would be required to reduce breaches to data protection when employing BYOD? What new policies will need to be written to manage the risks involve with BYOD? These are but some of key research questions that arise and need to be addressed in the near future.

b) Emerging Organisational System – Personal Data Store (PDS)

An emerging trend in business is the Personal Data Store (PDS). This is defined as a system that enables individuals to gather and manage their own data held by organisations.⁶¹¹ It is beginning to be employed by large corporations, governmental agencies and mobile operators. The PDS systems allow customers/clients to communicate beyond phone calls, letters and emails with organisations. The individual's identity is part of the verification which allows him or her to connect to the system. Once they are in they are allowed to collect, manage, analyse, use and share the information in ways they can control. These systems are already in use by Facebook,

ta_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx. Accessed on 18 May 2013.

⁶¹¹ Privacy Law & Business, *Data Protection & Privacy Information Worldwide - United Kingdom Report*, 'Will 2013 be the year of the personal data store?' Issue 65, January 2013, pp.1-3.

LinkedIn and Google. The PDS systems may extend in the near future to enabling individuals to manage their own health records held in medical facilities.

Although there are some perceived benefits with emerging PDS systems, this could also have serious data protection and records management repercussions. Undoubtedly, the issue is once again data security as well as the unauthorised movement of data to another location. As communication between organisations and individuals becomes more interpersonal, customisable and direct, several researchable topics will arise. Questions such as, how secure and how private are the PDS channels between the organisation and the customer/client? What impact would PDS systems have on records creation, maintenance and use? How would records in PDS systems be classified as records if they are subject to uninhibited changes? How would the continuum of care of records be affected within this environment? Research into these matters would require a period of time to pass for the full impact to be understood.

c) Emerging Concept (EU) – Data Portability

The new proposals by the EU to strengthen its data protection regime include ‘the right to data portability’. This is intended to give individuals the right to obtain a copy of their personal data being processed and move it to another platform.⁶¹² There is no doubt that archivists and records management would need to pay close attention to this concept which has been elevated to the level of a ‘right’. In this scenario, similar to the

⁶¹² European Commission, *Proposal for a General Data Protection Regulation* COM (2012) 11 at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 21 April 2014.

PDS systems individuals have been empowered to have full control of their personal data in a way that could totally impact on data quality, accountability, records integrity and the long term preservation of archival records containing personal data.

Some of the key research questions arising out of this going forward are, what impact data portability would have on the archival principles of *provenance* and *original order*? Would the ability to move data in portions not leave unexplained gaps in the records? How would this affect the quality of archives in the future? Data portability will not augur well for the future archives and records management and if the work is not done to understand its true effect on recordkeeping, society could lose its most valuable information. The actions and ideas of people are what gives a society its meaning and if those are not properly captured and safeguarded the context, content and structure of these records will be forever lost.

d) New Computing Devices – Wearable Computers

One of the latest and trendiest computing devices that has hit the global market is Google Glass. This is new in a range of emerging wearable computers. Google Glass is a hands-free computing device with a built-in camera, microphone, display and touchpad built to the size of regular spectacle frames.⁶¹³ This device enables its users to take photographs, create film and video conference. It can also be tethered to a smartphone, share GPS data and record messages and has a voice-to-text functionality. This device is

⁶¹³ Techradar.Av, *Google Glass: What You Need to Know* found at <http://www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114>. Accessed on 18 May 2013.

only limited by where its wearer can physically go as far as the eye can see. The ability for an individual to 'life-log' is now instantaneous. This also means that the ability for one individual to log the actions of another is also instantaneous and therefore presents issues related to privacy and data protection.

New types of records are being created by individuals everyday in unimaginable quantities. How will tomorrow's archivists and records managers cope with the control of personal data in increasingly digital records? What impact would records created on devices such as Google Glass have on privacy, records retention and disposition, archival appraisal and selection? Will there be a new role for archivists and records managers in the digital world? Is there a need for new theories and concepts? The answers to these pertinent questions merit full investigation by new age records practitioners.



Image 17 Google Glass⁶¹⁴

www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114

⁶¹⁴ Image taken from TechRadar a company that conducts technology reviews.

8.2 Enhancing Outreach and Educational Campaigns on DP

A concerted effort is needed to educate global citizens on data protection. In Chapter 2, it was seen that the errors and breaches in some cases was caused by human ignorance or error. In some jurisdictions, the Information/Privacy Commissioner's Offices carry out the function of educating citizens about privacy/data protection through their websites, publications and various presentations. However, other tools could be designed towards further sensitisation programmes. Advocates of privacy could use the same technologies to reach the minds of the masses and teach them how to safeguard their own privacy. One may ask who could be involved in this campaign.

Undoubtedly, the media could play a vital role in taking this message to the masses. Television, radio, magazines and newspapers remain very popular as means of communication. Companies who sell technological devices and software should seek to develop as part of their suite of products, privacy tutorials as part of the induction of new customers. Additionally, organisations should include privacy awareness as part of their communication strategy. New and old staff could be oriented in dealing with privacy in whatever function they carry out. Customers could be reached through company websites and publications. Much more could be done in this area of outreach and education.

8.3 Empowering Archivists and Records Managers to deal with Data Protection: The Role of International Council of Archives (ICA)

The International Council on Archives (ICA) is the premier international body for archivists dedicated to the effective management of records and the preservation and care of the world's archival heritage. As such, issues related to privacy/data protection and their impact on recordkeeping are important to the ICA and its members. This is evidenced by its reaction to the new proposals for reform of its data protection regime by the EU. The ICA responded by producing a position statement clearly setting out its concerns regarding new rights being discussed by the EU and its perceived impact on archives and records.⁶¹⁵

As the professional body for archivists and records managers, the ICA is in a unique position to provide sound guidance to its members and potential members in the form of guidelines on managing privacy/data protection in archives and records management programmes. Archivists and records managers have a unique perspective on the issues relating to privacy/data protection because of their in-depth involvement in the life-cycle or continuum of care in organisational records and information. This study pointed out that the role of the archivist and records manager has been understated in the management of privacy/data protection at the organisational level and the ICA as a body is best placed to ensure that these professionals are not left out of building the global privacy programme.

⁶¹⁵ International Council on Archives, Position Statement, *Protection of Personal Data* found at <http://www.ica.org/14222/position-statements/protection-of-personal-data.html>. Accessed on 20 May 2013.

It would also be prudent for the ICA or some other professional body for records practitioners such as ARMA International to formulate toolkits in privacy/data protection management for archivists/records managers. These types of aids could be made available in paper and electronic form so that they could have a global reach to all practitioners regardless of where in the world they may be. As data protection legislation spread and becomes part of the legal compliance landscape globally, organisations would need more and more support to cope with the rapid advancements in ICT technology.

The European Data Protection Supervisor, Peter Hustinx announced at the IAPP Data Protection Intensive 2013 in London attended by the author that substantial changes were scheduled to take place in the EU data protection regime by summer of 2013. However, the regulation will not take effect until 2016.⁶¹⁶ There have been over three thousand reforms proposed (Article 29 Working Party) that would change the current provisions made in the Data Protection Directive (95/46/EC). Two of the most significant changes are that 1) data protection has now in itself been given the status of a right i.e. it no longer merely sits under the 'right to privacy' and 2) the EU Commission plans to elevate the Directive to a Regulation. There would be a further centralisation of regulation and enforcement with stronger judicial remedies at the level of the EU. This is in an attempt to ensure there is consistency in practice particularly in digital environments where privacy is becoming increasingly challenging to manage.

⁶¹⁶ EU Data Protection Act, EU Data Protection Regulation at www.eudataprotectionact.com/eu-data-protection. Accessed on 25 April 2014.

The search for compliance solutions to privacy/data protection will never end and it is critical that all stakeholders including records managers and archivists be proactive in finding the right means and mechanisms to deal with this ever-increasing public problem. However, it must be noted that the West Indies is not the only region that lags behind in addressing the key elements and further research is required to identify and address other regions in the world where privacy/data protection regulation and enforcement are still in the embryonic stages. Doing this would bring these regions closer to developing a meaningful, effective and harmonious global response to the problem of data protection particularly in light of the unforeseen capabilities of advancing technology.

Bibliography

Books

- Ackroyd, Carol and Karen Margolis, *The Technology of Political Control* (London, 1980).
- Altman, Irwin, *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding* (California, 1975).
- Antoine, Rose-Marie Bell, *Commonwealth Caribbean: Law and Legal Systems* 2nd ed. (New York, 2008).
- Australian Society of Archivists Inc., *Keeping Archives* (Canberra, 2008).
- Roy Augier, *Before and After 1865: Education, Politics and Regionalism in the Caribbean* (Kingston, 1998).
- Avgerou, Chrisanthi, *Information Systems and Global Diversity* (Oxford, 2002).
- Bainbridge, David, *Data Protection Law: The Act and all SIs in One* (Essex, 2000).
- Barr, Jean, Beth Chiaiese and Lee R Nemchek, *Records Management in the Legal Environment* (Kansas, 2003).
- Barrow-Giles, Cynthia, *Introduction to Caribbean Politics* (Kingston, 2002).
- Bastian, Jeannette, *Owning Memory: How the Caribbean Community Lost its Archives and Found its History* (Westport, 2003).
- Beckford, George L., *Persistent Poverty: Underdevelopment in the Plantation Economies of the Third World* (Kingston, 2000).
- Bell, Daniel, *The Coming of Post-Industrial Society* (New York, 1973).
- Beniger, James R., *The Control Revolution: Technological and Economic Origins of the Information Society* 2nd ed. (Boston, 1986).
- Bennett, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (New York, 1992).
- Bennett, Colin and Charles Raab, *The Governance of Privacy: Policy Instruments in a Global Perspective* 1st ed. (Surrey, 2003).

Bennett, Colin, *The Privacy Advocates: Resisting the Spread of Surveillance* (Massachusetts, 2008).

Behrnd-Klodt, Menzi, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005).

Brenckenridge, Adam Carlyle, *The Right to Privacy* (Nebraska, 1970).

Bulmer, Martin, *Censuses, Surveys and Privacy* (New York, 1979).

Burt, Eleanor and John Taylor, *The Freedom of Information (Scotland) Act 2002: New Modes of Information Management in Scottish Public Bodies?*, sponsored by the Scottish Information Commissioner (St. Andrews, 2007).

Carey, Peter, *Data Protection: A Practical Guide to UK and EU Law* (Oxford, 2004).

Cate, Fred H, *Privacy in the Information Age* (Massachusetts, 1997).

Chosky, Carol, *Domesticating Information: Managing Documents Inside the Organisation* (Maryland, 2006).

Cohen, Ruth N., *Whose files is it anyway?* sponsored by the National Council for Civil Liberties (Ahmedabad, 1982).

Cordata, James W., *Making the Information Society: Experiences, Consequences and Possibilities* (New Jersey, 2002).

Dabydeen, David and John Gilmore, *No Island is an Island: Selected Speeches of Sir Shridath Ramphal* (London, 2000).

DeCew, Judith, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (New York, 1997).

Doyle, Carolyn and Mirko Bagaric, *Privacy Law in Australia* (Sidney, 2005).

Diamond, Susan Z., *Records Management: A Practical Guide, Policies, Practices, Resources and Technologies* (New York, 1995).

Dunn, Richard, *Sugar and Slaves: The Rise of the Planter Class in the English West Indies 1624-1713* (Williamsburg, 1972).

Fiadjoe, Albert, *Commonwealth Caribbean Public Law* 3rd Edition (New York, 2008).

Flaherty, David, *Protecting Privacy in Surveillance Societies: The Republic of Germany, Sweden, France, Canada and the United States* (North Carolina, 1992).

Franks, Patricia, *Records and Information Management* (London, 2013).

Frankel, Boris, *The Post-Industrial Utopians* (Oxford, 1987).

Frye, Curtis, *Privacy-Enhanced Business* (Connecticut, 2001).

Garrett, Brandon, *The Right to Privacy* (New York, 2001).

Goveia, Elsa, *A Study of the Historiography of the British West Indies to the end of the Nineteenth Century* (Washington, 1956).

Green, W.A., *British Slave Emancipation: The Sugar Colonies and the Great Experiment 1830-1865* (Oxford, 1976).

Hall Kenneth and Myrtle Chuck-A-Sang, *The Caribbean Community in Transition* (Kingston, 2008).

Heinke, Rex, *Litigation, Libel and Invasion of Privacy Cases: Programme Material* (California, 1984).

Heinke, Rex S., *Media Law* (Washington, 1994).

Hondius, Frits W., *Emerging Data Protection in Europe* (Amsterdam, 1975).

Hunton & Williams, *Client Alert* (New York, 2009).

Innes, Julie C., *Privacy, Intimacy and Isolation* (New York, 1992).

Jacob, Francis G., *European Law and the Individual* (U.S., 1976).

Jay, R. and Hamilton, A. *Data Protection: Law and Practice* (London, 1999).

Jenkinson, Hilary, *A Manual of Archives Administration* (London, 1965).

Klang, Matias and Andrew Murray, *Human Rights in the Digital Age*, (London, 2005).

Kenyon, Andrew and Megan Richardson eds., *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge, 2006).

Korff, Doune, *Data Protection Laws in the European Union* (Brussels, 2005).

- Law Society of Scotland, *Data Protection and FoI* (Edinburgh, 2003).
- Leigh, David, *The Frontiers of Secrecy: Closed Government in Britain* (Unknown, 1980).
- Lemieux, Victoria, *Managing Risks for Records and Information* (Kansas, 2004).
- Lewis, Gordon K., *The Growth of the Modern West Indies* (Kingston, 2004).
- Livelton, Trevor, *Archival Theory, Records, and the Public* (Chicago, 1996).
- Lloyd, Ian, *Information Technology Law* (Oxford, 2008).
- Manson-Smith, Derek, *What's on my record: Practical Guide to Your Rights Of Access to Personal Information*, published by the Scottish Consumer Council (Scotland, 2007).
- Menzi L. Behrnd-Klodt et al, *Privacy & Confidentiality Perspectives: Archivists & Archival Records* (Chicago, 2005).
- Miller, Laura, *Archives Principles and Practices* (London, 2010).
- Moore, Barrington, *Privacy: Studies in Social and Cultural History* (New York, 1984).
- Mullock, James and Peirs Leigh-Pollitt, *The Data Protection Act Explained*, The Stationery Office (London, 2001).
- Penn, Ira et al, *Records Management Handbook*, 2nd ed. (Vermont, 1994).
- Parry, J.H. et al, *A Short History of the West Indies* 4th ed. (Oxford, 1987).
- Phillips, Fred, *Caribbean Life and Culture: A Citizen's Reflects* (Kingston, 1991).
- Phillips, Fred, *Commonwealth Caribbean Constitutional Law* (London, 2002).
- Anthony Payne, *The Political History of CARICOM* (Kingston, 2008).
- Ricks, Swafford & Gow, *Information and Image Management: A Records Systems Approach* (Ohio, 1992).
- Room, Stewart, *Data Protection & Compliance in Context* (Swindon, 2007).
- Robek, Mary F. et al, *Information and Records Management: Document-Based Information Systems* 4th Edition (California, 1995).
- Routledge.Cavendish Lawcards, *European Union Law* Fifth Edition (Oxon, 2006).

- Ricks, Betty R. et al, *Information and Image Management* (Ohio, 1992).
- Rule, James, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford, 2007).
- Rule, James, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (Missouri, 1981).
- Schellenberg, Theodore, *Modern Archives: Principles and Techniques* (Chicago, 1956).
- Shepherd, Elizabeth and Geoffrey Yeo, *Managing Records: A Handbook of Principles and Practice* (London, 2003).
- Sieghart, Paul, *Privacy and Computers* (London, 1976).
- Solove, Daniel J., *The Digital Person: Technology and Privacy in the Information Age* (New York, 2004).
- Stephens, David O., *Electronic Records Retention: New Strategies for Data Life Cycle Management* (Kansas, 2003).
- Toffler, Alvin, *Creating a New Civilization: The Politics of the Third Wave* (Nashville, 1995).
- Touraine, Alain, *The Self-Production of Society* (Chicago, 1997).
- The Sedona Conference Working Group Series, International Overview of Discovery, Data Privacy & Disclosure Requirements, *Germany*, Public Comment Version (Spain, 2009).
- The University of the West Indies, *Report of the Caribbean Archives Conference held at The University of the West Indies*, Mona (Kingston, 1965).
- Ticher, Paul, *Data Protection for Library and Information Services* (London, 2001).
- Waldo, James, *Engaging Privacy and Information Technology in a Digital Age* (Washington, 2007).
- Webster, Frank, *Theories on the Information Society* 4th ed. (London, 2014).
- Westby, Jody R., *International Guide on Privacy* (Chicago, 2004).
- Westin, Alan F., *Privacy and Freedom* (London, 1970).
- Wheare, Kenneth Clinton, *Federal Government*, 4th ed. (New York, 1964).

Williams, Eric, *Capitalism and Slavery* (London, 1964).

Williams, Eric, *From Columbus to Castro: The History of the Caribbean 1492-1969* (New York, 1970).

Chapters in Books

Augier, Roy, 'Before and After 1965' edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996).

Axline, W. Andrew, 'From CARIFTA to CARICOM: Deepening Caribbean Integration', edited by Hilary Beckles and Verene Shepherd, *Caribbean Freedom: Economy and Society from Emancipation to the Present* (Princeton, 1996).

Bolland, O. Nigel, 'Systems of Domination after Slavery: The Control of Land and Labour in the British Caribbean', in *Caribbean Freedom: Economy and Society from Emancipation* edited by Hilary Beckles and Verene Shepherd (Princeton, 1996).

Alan Bell, 'Participation vs. principle: does technological change marginalize recordkeeping theory?', in *Archives and Recordkeeping: Theory into Practice* edited by Caroline Brown (London, 2014).

Jeremy, J. Enid Woodley and Lyall Kupke, 'Access and Reference Services', 3rd ed. *Keeping Archives* (Canberra, 2008)

Lewis, Gordon, 'The Challenge of Independence in the British Caribbean', in *Caribbean Freedom: Economy and Society from Emancipation* edited by Hilary Beckles and Verene Shepherd (Princeton, 1996).

Wallace, Elizabeth, 'The Break-up of the West Indies Federation', in *Caribbean Freedom: Economy and Society from Emancipation* edited by Hilary Beckles and Verene Shepherd (Princeton, 1996).

Journals

Alexander-Gooding, Sharon and Sonia Black, 'A National Response to ISO 15489: A Case Study of the Jamaica Experience', *The Information Management Journal* March/April 2005, Vol. 39, No. 2.

ARMA International, *Information Management Journal* (Kansas, 2000-2006).

Atherton, Jay, *From Life Cycle to Continuum: Some Thought on Records Management – Archives Relationship* Achivaria 21 at journals.sfu.ca/archivar. Accessed on

Bearman, David, *Diplomatics, Weberian Bureaucracy and the Management of Electronic Records in Europe and America* Archives & Social Studies: A Journal of Interdisciplinary Research at archivo.cartagena.es/publicas/catalogos/social_studies/_vYni1KYCfL-ZPeZr1dQhYw. Accessed on

Bigami, Francesca, 'Protecting Privacy Against the Police in the European Union: The Data Retention Directive', *Duke Law School Faculty Scholarship Series*, Paper 76 (North Carolina, 2007).

Booms, Hans, Hermina Joldersma and Richard Klumpenhauer, 'Society and the Formation of a Documentary Heritage: Issues in the Appraisal of Archival Sources', *Achivaria* 24 (Summer, 1987).

Booz, Charles, 'Electronic Records and the Right to Privacy', *Information Management Journal*, July 2001.

Cook, Terry and Schwartz, Joan, 'Archives, Records and Power: The Making of Modern Memory', *Archival Science* Vol. 2, Issue 1-2.

Cook, Terry, 'What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm', *Achivaria* 43 (Spring, 1997).

Duranti, Luciana, 'Diplomatics: New Uses for an Old Science', *Achivara* 28 at journals.sfu.ca/archivar.

EU Data Protection Act, *EU Data Protection Regulation* at www.eudataprotectionact.com/eu-data-protection. Accessed on 25 April 2014.

Harris, Verne, 'The Archival Sliver: Power, Memory, and Archives in South Africa', *Archival Science* 2: 63–86, (2002).

International Council on Archives, 'Archives and Recordkeeping in Australasia and Oceania' *Comma* 2011-1, (2012).

Ketelaar, Eric, 'Archival Temples, Archival Prisons: Modes of Power and Protection', *Archival Science* 2: 221–238, (2002).

Jimerson, Randall, 'Archives Power: Memory, Accountability, and Social Justice', *Archival Science Commons* (Chicago, 2009).

McKemmish, Sue, *Yesterday, Today and Tomorrow: A Continuum of Responsibility*

Prosser, William, *Handbook of the Law of Torts* 4th ed. (Minnesota, 1971).

Reidenberg, Joel R., 'E-Commerce and Transatlantic Privacy', *Houston Law Review* Volume 38 (2001).

Shepherd, Elizabeth, Stevenson, Alice and Andrew Flinn, 'The Impact of Freedom of Information and Records Use in Local Government: A Literature Review', *Journal of the Society of Archivists* Vol. 30 Issue 2 (2009).

Stanford Law Review, *The Right to be Forgotten* at www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten. Accessed on 21 April 2014.

Stone, M.G. and Malcolm Warner, 'Politics, Privacy and Computers', *The Political Quarterly* 40 (1969).

Upward, Frank, 'Structuring the Records Continuum Part 1 & 2', *Archives and Manuscripts* 24 & 25 (Monash, 1996-1997).

Warren, Samuel D. and Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

Westin, Alan, 'Social and Political Dimensions', *Journal of Social Issues*, Vol. 59, No. 2, 2003.

Yeo, Geoffrey, 'Concepts of Records (1): Evidence, Information and Persistent Representations,' *American Archivist*, Vol. 70 (Fall/Winter 2007).

Yeo, Geoffrey, 'Concepts of Record (2): Prototypes and Boundary Objects,' *The American Archivist*, Vol. 71 (Spring/Summer 2008).

Legislation

Data Protection Act No. 13 of 2011 (Trinidad and Tobago) at www.ttparliament.org/legislations/a2011-13.pdf. Accessed on 21 April 2014.

Data Protection Act 1998 (UK) Chapter 29 at www.legislation.gov.uk/ukpga/1998/29/contents. Accessed on 21 April 2014.

Federal Data Protection Act 1994 (Germany - Bundesdatenschutzgesetz BDSG) (BGBl. I S. 2325) at www.iuscomp.org/gla/statutes/BDSG.htm. Accessed on 21 April 2014.

Official Information Act 1982 no. 156 at <http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html>. Accessed on 21 April 2014. Accessed on 21 April 2014.

Privacy Act 1988 (Australia) No .119 at www.comlaw.gov.au/Series/C2004A03712. Accessed on 21 April 2014.

Privacy Act (Canada) 1985 c. P-21 at http://www.priv.gc.ca/leg_c/r_o_a_e.asp. Accessed on 21 April 2014.

Privacy Act 1993 (New Zealand) No. 28 at www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html. Accessed on 21 April 2014.

US Privacy Act of 1974 (5 U.S.C § 552a) at www.usa.gov. Accessed on 21 April 2014.

United States Courts, *The Fourth Amendment* at www.uscourts.gov. Accessed on 21 April 2014.

Newsletters

DataGuidance, *Data Protection Law & Policy*, Volume 10, Issue No. 03 (March 2013).

Privacy Law & Business, *Data Protection & Privacy Information Worldwide - United Kingdom Report* Issue No. 65 (January 2013).

Privacy Law & Business, *Data Protection & Privacy Information Worldwide - International Report* Issue 122 (April 2013).

Sidley Austin LLP, *Privacy, Data Security & Information Law Update*, 'Business Concern over Amendments to Proposed EU Data Protection Regulation' (January 15, 2013).

Statewatch News Online, *Impossible to Legality of EU Communications Data Retention Directive Says German Parliament* found at www.statewatch.org/news/2011/jun/eu-mand-ret-wp-on-dp-prel.pdf. Accessed on 28 August 2012.

Newspapers

Davidson, C.P.D., 'Continuing Dangers of Uncontrolled Storage Data', *The Times*, July 17, 1980.

Davidson, C.P.D., 'How lack of computer privacy may affect overseas trade', *The Times*, March 3, 1980.

Davidson, C.P.D., 'UK Lagging Behind in Data Protection', *The Times*, March 28, 1980.

Evans, Peter, 'Plan to ensure that computers have a regard for privacy', *The Times*, December 7, 1975.

Foster, John, 'Safeguarding the right to privacy', *The Times*, May 5, 1981.

Geddes, Diana, 'Everyone should have the right to challenge information in data files, civil liberties council says', *The Times*, February 8, 1977.

Gibb, Frances, 'British Dilemma over Data Privacy Convention', *The Times*, October 22, 1980.

Gibb, Frances, 'Data protection challenge to UK', *The Times*, February 2, 1981.

Gibb, Frances, 'Lawyers call for legal control of personal data', *The Times*, July 19, 1980.

Gibb, Frances, 'MPs criticize Home Office for failing to act on privacy and data protection', *The Times*, 11 December 1980.

Gibb, Frances, 'Mr. Whitelaw's delay on data protection likely to anger MPs', *The Times*, December 22, 1980.

Gibb, Frances, 'Privacy Law to Protect Citizens Outlined', *The Times*, August 13, 1980.

Hennessy, Peter, 'MP to press for action on data protection', *The Times*, July 31, 1980.

Johnstone, Bill, 'Slow start for data register', *The Times*, December 28, 1985.

Johnston, Rory, 'Do computers really threaten our privacy?', *The Times*, March 26, 1980.

Kenny, J.J., 'Britain lags behind in the privacy issue', *The Times*, September 26, 1974.

Owen, Kenneth, 'Data body criticizes White Paper on privacy', *The Times*, November 30, 1976.

Owen, Kenneth, 'Licensing powers needed for data bank privacy body', *The Times*, December 19, 1975.

Owen, Kenneth, 'Licensing scheme urged for personal data files', *The Times*, September 30, 1977.

Owen, Kenneth, 'PO favours compromise authority on privacy', *The Times*, December 14, 1976.

Owen, Kenneth, 'Seven principles for the protection of privacy', *The Times*, November 1976.

Starboek News found at landofsixpeoples.com. Accessed in 2009.

The Australian, *Medicare Privacy breaches shakes e-health legislation* at www.theaustralian.com.au/technology/medicare-privacy-breaches-shake-healthcare-identifier-legislation/story-e6frgakx-225835812144?nk=480f6c969b3412bedeed88fc7bec2db3. Accessed on 24 April 2014.

The Guardian, *The NSA Files* at www.theguardian.com/world/the-nsa-files. Accessed on 20 April 2014.

The Most Important News, *WikiLeaks Scandal Explodes* at themostimportantnews.com/archives/the-wikileaks-scandal-explodes. Accessed on

The Times Editorials:

'Data Protection body challenged', December 6, 1976.

'The computer's challenge to privacy', March 22, 1977.

'UK will sign European pact on data protection', March 20, 1981.

'Data Protection Register', February 18, 1982.

'Improved law on privacy urged', June 23, 1982.

'Data Protection Bill – Keeping tabs on how much 'they' know', November 23, 1982.

'Data Protection – 'Data users' in the Firing Line?', November 26, 1985.

World News, *Conscription in the United States Vietnam War - History of the Military Draft* at wn.com/conscription_in_the_united_states_vietnam_war.

Official Papers

Australian Government, Australian Law Reform Commission, *Privacy Law and Practice* at www.alrc.gov.au/inquiries/privacy. Accessed on 25 April 2014.

CARICOM Secretariat, CSME – Chapter Three: Free Movement in the CARICOM Single Market and Economy (CSME) at www.caricom.org. Accessed on 7 August 2009.

CARICOM Secretariat, *The Treaty of Chaguaramus* at www.caricom.org/jsp/community/revised_treaty-text.pdf.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 at conventions.coe.int/Treaty/en/Treaties/Html/005.htm. Accessed on 28 January 2009.

Council of Europe, *The Convention [108] for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 1981).

Great Britain, *Acts of Parliament*, London, HMSO at www.hmso.gov.uk.

Great Britain, *Freedom of Information Act 2000*, HMSO (London, 2000).

Great Britain, *Report of the Committee on Data Protection*, [Chair Sir Norman Lindop] Cmnd 7341 HMSO (London, 1978). Accessed on 7 August 2009.

Great Britain, Parliament, *Report of the Committee on Privacy*, [Chair Rt. Hon. Kenneth Younger] Cmnd. 5012 HMSO (London, 1972).

Great Britain, Home Office, *White paper: Computers and Privacy*, Cmnd 6353 HMSO (London, 1975).

ENISA, *The right to be forgotten – between expectations and practice* at www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten. Accessed on 24 April 2014.

European Commission, *Article 17, Preamble (53)* found at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 3 April 2013.

European Commission, *Article 29 Working Party - Work Programme 2014-2015* at ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_en.pdf Accessed on 13 September 2015.

European Commission, *Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors of third countries under Directive 95/46/EC* at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF. Accessed on 13 January 2014.

European Commission, *Data Protection Day 2014: Full Speed on EU Data Protection Reform* at europa.eu/rapid/press-release_MEMO-14-60_en.htm. Accessed on 1 February 2014.

European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing*

of personal data and on the free movement of such data (Brussels, 1995) at europa.eu. Accessed on 11 May 2014.

European Commission, *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* at euwiki.org/2002/58/EC. Accessed on 11 May 2014.

European Commission, *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950 at europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm Accessed on 21 April 2014.

European Commission, Press Release Database, Progress on EU data protection reform now irreversible following European Parliament vote at europa.eu/rapid/press-release_MEMO-14-186_en.htm. Accessed on 11 May 2014.

European Commission, *Proposal for a General Data Protection Regulation* COM (2012) 11 at ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed on 21 April 2014.

European Commission, *Report from the Commission: First Report on the Implementation of Data Protection 95/46/EC (2003)* at europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm Accessed on 28 January 2009.

Information Commissioner's Office, *Annual Report 2007/08* HMSO (London, 2008).

Information Commissioner's Office, *Data protection and journalism: a guide for the media* (draft) at ico.org.uk/news/latest_news/2014/~media/documents/library/Data_Protection/Research_and_reports/data-protection-and-journalism-a-guide-for-the-media-draft.pdf. Accessed on 13 September 2014.

Information Privacy Principles, at www.oaic.gov.au/privacy/privacy-act/information-privacy-principles. Accessed on 21 April 2014.

International Standards Organisation, *ISO/IEC 29100: 2011 Information Technology – Security Techniques – Privacy Framework* at www.iso.org.

Korff, Douwe, European Union, Directorate-Justice, Freedom and Security, *Comparative Study on Different Approaches to New Privacy Challenges, In Particular in Light of Technological Developments, Country Studies – UK* (June 2010) at ssrn.com/abstract=1638938. Accessed on 10 September 2012.

Ministry of Justice and The National Archives, *Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000* HMSO (London, 2009).

PricewaterhouseCoopers, *UK Information Security Breaches Survey – Technical Report* at www.pwc.co.uk. Accessed on 13 September 2012.

Robinson, Neil et al, *Review of the European Data Protection Directive* RAND Corporation sponsored by the Information Commissioner's Office (UK) 2009 at www.rand.org/randeurope.

The National Archives, *An inquiry into the culture, practices and ethics of the press: report [Leveson]* at webarchive.nationalarchives.gov.uk/20140122145147/http://www.levesoninquiry.org.uk. Accessed on 13 September 2014.

The National Archives, Society of Archivists, Records Management Society and National Association of Information Managers, *Code of Practice for Archivists and Records Managers Under Section 51(6) of the Data Protection Act 1998* at www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf. Accessed on 28 January 2009.

United Nations, *Universal Declaration of Human Rights of 1948* at www.un.org/Overview/rights.html. Accessed on 28 January 2009.

United Kingdom Report, Privacy Laws & Business, Data Protection & Privacy Information Worldwide, *Will 2013 be the year of the personal data store?* Issue 65, January 2013.

US Department of Commerce, National Institute of Standards, *Assessment of Access Control Systems and Technology* at csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf. Accessed on 13 September 2014.

US Department of Commerce, National Institute of Standards and Technology, *Audit Trails* at csrc.nist.gov/publications/nistbul/itl97-03.txt. Accessed on 13 September 2014.

U.S. Department of Health, Education and Welfare, *Records, Computer, and the Rights of Citizens* (1973) at epic.org/privacy/hew1973report. Accessed on 28 January 2009.

U.S. Department of Justice, *Overview of the Privacy Act of 1974* (2002) at www.usdoj.gov. Accessed on 6 February 2009.

Web Publications

ABC News, *Obama: Looking Into Celeb 'Secret File' Hack* found on www.abcnews.go.com/US/michelle-obama-joe-biden-celebrities-personal-information-allegedly/story?id=18707707. Accessed on 18 March 2013.

American Institute of Certified Public Accountants, *Privacy Risk Assessment Questionnaire* from at www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/PrivacyServices/Pages/Privacy%20Risk%20Assessment%20Questionnaire.aspx?action=print. Accessed on 13 September 2014.

ARMA International at www.arma.org. Accessed on 26 February 2009.

BBC News, *Edward Snowden: Leaks that exposed US spy programme* at www.bbc.co.uk/news/world-us-canada-23123964.

BBC News, *PR Officer loses job over racist Twitter comment* at www.bbc.co.uk/news/world-us-canada-25484537.

BBC News Technology, *Frozen Android Phones Gives Up Data Secrets* found at www.bbc.co.uk/news/technology-21697704. Accessed on 21 March 2013.

BBC, *Jimmy Saville Scandal: Report Reveals Decades of Abuse* found at www.bbc.co.uk/news/uk-20981611. Accessed on 3 April 2013.

BBC News, *Q&A: News of the World Phone Hacking Scandal* at www.bbc.com/news/uk-11195407. Accessed on 13 September 2014.

Basinar, David, *Data Protection Laws around the World* (April 2003) www.privacy.org/survet/dpmap.jpg. Accessed on 7 February 2009.

Bennett, Colin, *Private Sector Privacy Reform in Canada: Lessons for Australia* (1997) at www.austlii.edu.au.

Berlin Commissioner for Data Protection and Freedom of Information, *Parliament* at www.datenschutz-berlin.de/content/berlin/parlament. Accessed on 11 March 2012.

Big Brother Watch, *NHS Breaches of Data Protection Law: How patient confidentiality was compromised five times every week* found at www.bigbrotherwatch.org.uk/home/2011/10/nhs-data-protection.html. Accessed on 9 September 2012.

Caslon Analytics Privacy Guide, *New Zealand* at www.caslon.com.au. Accessed on 26 January 2009.

CARICOM, *Caribbean Court of Justice* found at www.caribbeancourtjustice.org. Accessed on 21 July 2009.

CARICOM Community Secretariat, *Caribbean Single Market and Economy* at www.caricom.org/jsp/single_market/single_market_index.jsp?menu=csme.

Centre for Democracy and Technology at www.cdt.org/privacy/eudirective/EU_Directive_.html. Accessed on 17 February 2009.

CNNMoney, *Apple probably isn't cracking down on native app cookie tracking – yet* found at money.cnn.com/news/newsfeeds/gigaom/articles/2013_02_26_apple_probably_isnt_cracking_down_on_native_app_cookie_tracking_yet.html. Accessed on 11 March 2013.

Council of Europe, ETS no. 108 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* at conventions.coe.int. Accessed on 28 January 2009.

Cricket World Cup 2007, *Cricket World Cup Schedule* at www.travour.com/icc-cricket-world-cup-2007-west-indies/schedule-for-cricket-world-cup.html.

E-Hacking News, *Breaking News* found at www.ehackingnews.com. Accessed on 18 March 2013.

E-Health Europe, *German National, E-Health Programme: Contested but Driven Forward* at www.ehealthurope.net/Features/items. Accessed on 12th March 2012.

Electronic Privacy Information Centre, *USA Patriot Act (H.R. 3162)* at epic.org/privacy/terrorism/hr3162.html. Accessed on 19 September 2012.
Europa, *Basic Information* found at <http://europa.eu>. Accessed on 9 February 2012.

European Union, *Data Retention Directive (2004/24/EC)* at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML. Accessed on 28 August 2012.

European Network and Information Security Agency, *The Right to be Forgotten between Expectation and Practice* found at www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten. Accessed on 25 February 2013.

Farivar, Cyrus, *EU Data Protection Authority Condemns Data Retention Directive* published in 2011 at www.dw.de/dw/article/0,15120172,00.html. Accessed on 29 August 2012.

Forbes, *iCloud Data Breach: Hacking and Celebrity Photos* at www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos. Accessed on 13 September 2014.

Fox News, *Spying on Congress – NSA Scandals gets even worst in 2014* at www.foxnews.com/opinion/2014/01/09/spying-on-congress-nsa-scandal-gets-even-worse-in-2014. Accessed on 21 April 2014.

Geek Interview on *Aggregate Data* at www.learn.geekinterview.com/data-warehouse/data-types/aggregate-data.html. Accessed on 13 September 2014.

Gellmen, Robert, *Fair Information Practices: A Basic History* at bobgellman.com/rg-docs/rg-FIPshistory.pdf . Accessed on 31 December 2008.

Health Information Technology for Economic and Clinical Health (HITECH), *Annual Report to Congress on Breaches of Unsecured Protected Health Information 2009 and 2010* found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf. Accessed on 21 September 2012.

HIPAA Privacy Standard at www.all-things-medical-billing.com/hipaa-privacy-standard.html. Accessed on 21 September 2012.

Hogan Lovells, *Latest Entries in the Hogan Lovells Chronicle of Data Protection – Privacy & Information Security News & Trends* found at www.hldataprotection.com. Accessed on 29 August 2012.

Holmes, Nancy, *The Right to Privacy and Parliament, In Brief*, Parliamentary Information and Research Service, Parliament of Canada 2006 found at www.parl.gc.ca/Content/LOP/researchpublications/prb0744-e.htm. Accessed on 28 November 2008.

Huff Post Entertainment, *Michele Obama on Oscars Criticism: ‘Absolutely Not Surprising’* found at www.huffingtonpost.com/2013/03/01/michelle-obama-oscars-criticism_n_2788512.html. Accessed on 11 March 2013.

IHS Healthcare and Privacy Blog, *Germany’s E-Health Card: Revolutionary Step or Another Doomed Initiative?* at healthcare.blogs.ihs.com/2012/11/12/germanys-e-health-card-revolutionary-step-or-another-doomed-initiative. Accessed on 24 April 2014.

Inozemtsev, Vladislav L., *The Inevitability of a Post-Industrial World: Concerning the Polarity of Today's World Order* at www.postindustrial.net.

Institute of Education, *Student Fair Processing Notice* at www.ioe.ac.uk/about/documents/About_Policies/Data_Protection_for_Students.pdf. Accessed on 13 September 2014.

International Association of Privacy Professionals at www.iapp.org.

International Association of Privacy Professionals, *The PATRIOT Act of 2001* at www.iapp.org.

Information Commissioner's Office, *Bring Your Own Device (BYOD)* at ico.org.uk/for_organisations/data_protection/topic_guides/online/~media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx.

Information Shield, *US Privacy Laws* found at www.informationshield.com/usprivacylaws.html. Accessed on 25 January 2014.

Institute of Education, *Student Fair Processing Notice* at www.ioe.ac.uk/about/documents/About_Policies/Data_Protection_for_Students.pdf. Accessed on 13 September 2014.

International Council on Archives, Position Statement, *Protection of Personal Data* at www.ica.org/14222/position-statements/protection-of-personal-data.html. Accessed on 20 May 2013.

International Standards Organisation, ISO 15489-1: 2001 *Records Management Standard* at www.iso.org.

INTERPOL, *Caribbean officials visit INTERPOL to Plan for Cricket World Cup* at www.interpol.int.

Jóri, András, *Data Protection in Europe* at www.dataprotection.eu. Accessed on 17 February 2009.

Lawyers.com, *Lawsuit targets Facebook privacy issues* at communications-media.lawyers.com/privacy-law/lawsuit-target-facebook-privacy-issues.html. Accessed on 21 April 2014.

Mirror, *Kate Middleton Topless Pictures: Place says invasion of privacy is "grotesque and totally unjustifiable" and evokes memories of Princess Diana* at www.mirror.co.uk/news/uk-news/kate-middleton-topless-pictures-palace-1323761. Accessed on 25 April 2014.

NARA, *The Privacy Act* (April 2006) found at www.nara.org.

Oracle, *Database Advanced Security Guide - Redaction* at docs.oracle.com/database/121/ASOAG/redaction.htm#ASOAG594. Accessed on 13 September 2014.

Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (Paris: 1981) at www.oecd.org. Accessed on 28 January 2009.

PC Magazine, *What You Need to Know About Cloud Computing* found at www.pcmag.com/article2/0,2817,2372163,00.asp. Accessed on 19 March 2013.

PistolStar Authentication Blog, *Problems in the "Safe" Harbor* at blog.pistolstar.us/blog/problems-in-the-safe-harbor. Accessed on 25 January 2014.

Privacy and Human Rights 2003: Overview found at www.privacyinternational.org/survey/phr2003/overview.htm. Privacy International at www.privacyinternational.org. Accessed 9 February 2009.

Privacy Law and Policy Reporter, *Remedies under New Zealand Privacy Law* at www.austlii.edu.au. Accessed on 9 February 2009.

Privacy News From Around the World, *Treasurer's daughter, Marshall University settle FERPA breach lawsuit* found at www.pogowasright.org/?p=16273. Accessed on 24 September 2012.

Privaterra at www.privaterra.org. Accessed on 7 August 2009.

Privicilla.org at www.privacilla.org/index.html.

Pros and Cons of Data Retention found at www.vorratsdatenspeicherung.de/content/view/83/87/lang,en. Accessed on 11 March 2012.

Reuters, *Three quarters of Americans distrust the government* at rt.com/usa/government-trust-americans-poll-172.

SearchDataBackup, *Data Protection Management* at searchdatabackup.techtarget.com/definition/data-protection-management-DPM. Accessed on 21 January 2014.

Sidley Austin LLP, Privacy, Data Security & Information Law Update, *Business Concern over Amendments to Proposed EU Data Protection Regulation*, January 15, 2013.

Solove, Daniel, *Student Privacy in Peril: Massive Data Gathering with Inadequate Privacy and Security* found at www.huffingtonpost.com/daniel-j-solove/student-privacy-in-peril_b_1156907.html. Accessed on 24 September 2012.

Sopata, David, *How FERPA Compares to HIPAA* found at www.infosecisland.com/blogview/17467-How-FERPA-Compares-to-HIPAA.html?amp. Accessed on 24 September 2012.

Student Paper, *The Influence of the European Commission Data Protection Directive on Third Countries* (2007) at www.allacademic.com. Accessed on 17 February 2009.

Symantec, *Introduction to Encryption* at www.symantec.com/connect/articles/introduction-encryption. Accessed on 13 September 2014.

The Australian, *Medicare Privacy breaches shakes e-health legislation* at www.theaustralian.com.au/technology/medicare-privacy-breaches-shake-healthcare-identifier-legislation/story-e6frgax-1225835812144. Accessed on 24 April 2014.
TechnoBuffalo, *Death Threats and Privacy: A Judge Orders Apple to Reveal More Info in Tracking Lawsuit* found at www.technobuffalo.com/2013/03/08/apple-tracking-privacy-lawsuit. Accessed on 11 March 2013.

The Information Commissioner at www.informationcommissioner.gov.uk. Accessed on 7 August 2009.

The National Archives of Australia, *Records management and the cloud – Checklist* found at www.naa.gov.au/Images/Cloud_checklist_with_logo_and_cc_licence_tcm2-41355.pdf. Accessed on 19 March 2013.

The Privacy Place Research Center at www.theprivacyplace.org. Accessed on 7 August 2009.

The Washington Post, *IP Addresses are Personal Data, EU Regulator Says* found at www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html. Accessed on 19 March 2013.

United Nations International Convention on Civil and Political Rights (1997) at <http://www.hrweb.org/legal/cpr.html>. Accessed on 10 February 2009.

US Department of Commerce, National Institute of Standards, *Assessment of Access Control Systems and Technology* at csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf. Accessed on 13 September 2014.

US Department of Commerce, National Institute of Standards and Technology, *Audit Trails* at csrc.nist.gov/publications/nistbul/itl97-03.txt. Accessed on 13 September 2014.

Techradar.Av, *Google Glass: What You Need to Know* at www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114. Accessed on 18 May 2013.

Upward, Frank, *Structuring the Records Continuum – Part 1 Postcustodial Principles and Properties* at www.infotech.monash.edu.au/research/groups/rcrg/publications/recordscontinuum-fupp1.html. Accessed on 17 October 2012.

US Department of Education, *Family Educational Rights and Privacy Act (FERPA)* at www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Accessed on 24 September 2012.

World Privacy Forum at www.worldprivacyforum.org. Accessed on 7 August 2009.

WWI and WWII Propaganda Posters at www.propagandaposters.us. Accessed on 9 February 2012.

Yahoo! News, *Apple denies iCloud breach let hackers take iPhone hostages* at news.yahoo.com/apple-denies-icloud-breach-let-hackers-iphones-hostage-123055818.html. Accessed on 13 September 2014.

Presentations, Proceedings & Speeches

CARICOM Community Secretariat, *Statement by H.E. Edwin Carrington on the Occasion of the Inauguration of the CARICOM Single Domestic Space* (1 February 2007), found at www.caricom.org/jsp/pressreleases/pres26_07.jsp.

Evans, David et al, 'To be or not to be personal data', Notes from Presentation by Group Manager - Business and Industry, UK Information Commissioner's Office at *IAPP Data Protection Intensive 2013*, April 2013.

New Zealand Privacy Commissioner, *The Official Information Act and Privacy: New Zealand's Story*, Speech at the FOI Live 2005 Conference London, 2005.

Girvan, Norman, 'The Quest for Regional Integration in the Caribbean – Successes and Challenges', Speaking Notes at The University of the West Indies, Mona, Jamaica, September, 2011.

Hustinx, Peter, 'Recent developments in EU data protection: stepping up to more comprehensive and more effective protection', Speech by European Data Protection Supervisor given at the *RISE Conference on Ethics and Governance of Biometrics and*

Identification Technologies, (Brussels, 2010) at globalseci.com/?page_id=1462. Accessed on 18 May 2013.

Hustinx, Peter et al, 'Update on the Data Protection Regulation: The Role of the DPAs', Notes from Presentation by European Data Protection Supervisor at *IAPP Data Protection Intensive 2013*, April 2013.

McKemmish, Sue, 'Yesterday, Today and Tomorrow: A Continuum of Responsibility', *Proceedings of the Records Management Association of Australia 14th Convention*, 15-17 September, RMAA (Perth, 1997) at www.monash.edu.au. Accessed on 12 February 2009.

Weiss, Stefan et al, 'Don't Start from Scratch! Leverage Your Compliance Programme to Deliver Privacy Compliance', Notes from Presentation by Global Data Protection Officer, Swiss Reinsurance Company Inc. at *IAPP Data Protection Intensive 2013*, April 2013.

Yeo, Geoffrey, *Records and Representations*, Paper presented at the Conference on the Philosophy of Archive, Edinburgh, Scotland, 10 April 2008.

Audio-visual Materials

Childs, Mary, *Privacy Law and Records Management for Anti-Violence Workers in BC* 4 April 2013 at <http://www.youtube.com/watch?v=Qh3WO56JBdc>. Accessed on 18 May 2013.

EUTube, *ProtectingYour Rights – Data Protection* 5 December 2011 at <http://www.youtube.com/watch?v=qRDcuQPfX6k>. Accessed on 18 May 2013.

Information Commissioner's Office, *Data Protection Training Videos* 7 June 2012 at <http://www.youtube.com/watch?v=wAe4358amJc&list=PLBEEA03BA780B128E>. Accessed on 18 May 2013.

Interview (Video) of Sir Fred Phillips conducted as part of an Oral History Project of the West Indies Federal Centre entitled, 'Remembering the West Indies Federation' in (Bridgetown, 2006).

Interview (Video) of Sir Shridath Ramphal conducted as part of an Oral History Project of the West Indies Federal Centre entitled, 'Remembering the West Indies Federation' in (Bridgetown, 2006).

William and Mary Law School, *What is Privacy Interest in Public Records?* 6th Conference on Public and Private Access to Court Records, 29 June 2010 at http://www.youtube.com/watch?v=IPvYmd_CyYQ. Accessed on 18 May 2013.

Images

Advanced Card Systems, *Eh880* at www.eh880.com/eh880.php. Accessed 18 May 2013.

Aujas US at aujasus.wordpress.com/category/data-leak-prevention. Accessed 18 May 2013.

Diagram of Email Path from a POP Server at www.vimm.com/wp-content/uploads/2012/05/POP_diagram-email.jpg. Accessed 18 May 2013.

Dreamstime, *Stock Images: Data Protection* at www.dreamstime.com/stock-images-data-protection-image19541884. Accessed 18 May 2013.

Ehow at www.ehow.com. Accessed 18 May 2013.

Google Glass at www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114. Accessed 18 May 2013.

ICC Cricket World Cup 2007 Logo at www.cricketstar.net/cca/images/ICC%20quarterly_12%202005.pdf. Accessed on 17 February 2009.

Inauguration of the Caribbean Court of Justice (2001) at www.caribbeancourtofjustice.org. Accessed on 17 February 2009.

Indiana University, *Privacy of Medical Records* at protect.iu.edu/privacy/cartoons. Accessed on 18 May 2013.

Interactive Maps of Breach Notification Status at info@databreachmaps.com.
Internet Privacy at browertech.wordpress.com/category/internet-privacy. Accessed on 13 September 2012.

Map of the West Indies and Central America (1910) at www.emersonkent.com/map_archive/central_america_1910.htm. Accessed on 17 February 2009.

Photograph (black & white still), *London Delegation in 1953* digitised from the Federal Information Service Photographic Collection at W.I. Federal Archives Centre, The University of the West Indies, Cave Hill Campus, Barbados.

Privacy Cartoons, www.behance.net/gallery/Privacy-Cartoons/3754298. Accessed on 18 May 2013.

Typophile Temp, *1984 Big Brother Is Watching Poster* at typophile.com/node/82726. Accessed on 18 May 2013.

Yahoo Finance, *Number of active users at Facebook over the years* found at finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html. Accessed on 3 April 2013.

Interviews

Formal

Aylmer, Lynsey, Interview by Cherri-Ann Beckles with Senior FoI Assessor at the National Archives UK (TNA) (Surrey, 2009).

Bell, Alan, Interview by Cherri-Ann Beckles with Records Manager/Compliance Officer at the University of Dundee, Centre for Archive and Information Studies (Dundee, 2013).

Bramwell, Jane, Interview by Cherri-Ann Beckles with Head of Tate Britain Library, Archives and Collection Access (London, 2009).

Carnegie, Ralph, Interview by Cherri-Ann Beckles with Emeritus Professor of Law, The University of the West Indies (Bridgetown, 2010).

Crooks, Colin, Interview by Cherri-Ann Beckles with Senior Information Access Manager – Information Rights Team at the Department of Schools, Children and Families (London, 2009).

Cumberbatch, Jeff, Interview by Cherri-Ann Beckles with Senior Lecturer, Faculty of Law, The University of the West Indies, Cave Hill Campus (Bridgetown, 2009).

Dawson, Gerry, Interview by Cherri-Ann Beckles with Information Services Development Manager at Tate Britain (London, 2009).

Falconer, Maureen, Interview by Cherri-Ann Beckles with Senior Guidance and Promotions Officer – Scottish Information Commissioner's Office (Edinburgh, 2008).

Graham, Susan, Interview by Cherri-Ann Beckles with University Records Manager at the University of Edinburgh (Edinburgh, 2012).

Healy, Susan, Interview by Cherri-Ann Beckles with Head – FoI at The National Archives (TNA) (Surrey, 2010).

Kennedy, Jane, Interview by Cherri-Ann Beckles with Gallery Records Manager at Tate Britain (London, 2009).

MacDonald, Ken, Interview by Cherri-Ann Beckles with Scottish Information Commissioner – Assistant UK Information Commissioner (Edinburgh, 2008).

Newton, Velma, Interview by Cherri-Ann Beckles with Senator of Government of Barbados Senate and Dean of the Faculty of Law, The University of the West Indies, Cave Hill, Campus (Bridgetown, 2010).

Potter, Helen, Interview by Cherri-Ann Beckles with FOI Assessor at The National Archives UK (TNA) (Surrey, 2009).

Ramphal, Shridath, Interview by Cherri-Ann Beckles with Emeritus Chancellor of The University of the West Indies, West Indian Federalist, Founding Member of CARICOM, Commonwealth Secretary-General and International Statesman (Bridgetown, 2013).

Russell, Roslyn, Interview (Email) by Cherri-Ann Beckles with Deputy Chair UNESCO Memory of the World, Australia Committee (Canberra, 2010).

Sigworth, Claire, Interview by Cherri-Ann Beckles with Head of Investigations – Scottish Information Commissioner's Office (Edinburgh, 2008).

Sweeney, Shelly, Interview by Cherri-Ann Beckles with Head of Archives & Special Collections at the University of Manitoba (Manitoba, 2010).

Varin, Marie-Eve, Interview by Cherri-Ann Beckles with Archiviste, Responsable des Restriction – Direction du Centre de Montreal et des Archives Privees, Judiciaires et Civiles, Bibliotheque et Archives Nationales du Quebec, Canada (Montreal, 2009).

Wheater, Fiona, Interview (Telephone) by Cherri-Ann Beckles with Officer of Planning, Policy and Governance at the University of Stirling (Stirling, 2012).

Youseff, Mona, Interview by Cherri-Ann Beckles with Human Resource Manager at Tate Britain (London, 2009).

Informal

Aarons, John, Interview by Cherri-Ann Beckles with University Archivist at The University of the West Indies, Vice Chancellory (Mona, 2010).

Alexander-Gooding, Sharon, Interview by Cherri-Ann Beckles with Campus Records Manager/Head Archivist at The University of the West Indies, Cave Hill Campus (Bridgetown, 2010).

Belfon, Avril, Interview by Cherri-Ann Beckles with the National Archivist of Trinidad and Tobago (Port-of Spain, 2014).

Bertin, Cletis, Interview by Cherri-Ann Beckles with Legal Counsel of the Organisation of Eastern Caribbean States (OECS) Secretariat (Castries, 2010).

Haraksingh, Kusha, Interview by Cherri-Ann Beckles with Lead Negotiator of CARICOM, Barrister and Senior Lecturer, Faculty of Law, The University of the West Indies, St. Augustine Campus (Port-of-Spain, 2010).

Ishmael, Len, Interview by Cherri-Ann Beckles with Director-General of the Organisation of Eastern Caribbean States (OECS) (Castries, 2010).

Marshall, Woodville K. Interview by Cherri-Ann Beckles with Professor Emeritus of History (Bridgetown, 2013).

Ramphal, Shridath, Interview by Cherri-Ann Beckles with Emeritus Chancellor of The University of the West Indies, West Indian Federalist, Founding Member of CARICOM, Commonwealth Secretary-General and International Statesman (Bridgetown, 2013). [Interviewed again by telephone]

Thomas, Richard, Interview by Cherri-Ann Beckles with Former UK Information Commissioner and Global Strategy Advisor at the Centre for Information Policy Leadership, Hutton & Williams LLP (London, 2013).

Online Survey

Online survey designed by Cherri-Ann Beckles for Scottish Higher Education Information Practitioners Group (SHEIP) in 2012 using University of Bristol Online Survey software at University of Bristol, *Bristol On-line Surveys* at www.survey.bris.ac.uk. Accessed on 10 September 2014.

Appendices



The University of Dundee
Centre for Archive and Information Studies (CAIS)
PhD Archive and Information Studies
 SEMI-STRUCTURED INTERVIEW

Key Objective – To conduct an international comparison of data protection regimes from a records management perspective in order to inform emerging practice in the West Indies

1. How does data protection/privacy legislation impact on recordkeeping in the public and private sectors?
2. Which agency/agencies are responsible for administering data protection?
3. What are the key mechanisms for enforcing the legislation in XXXX?
4. How does Data Protection interface with FoI?
5. Are there any challenges with enforcing data protection/privacy in XXXX?
6. Are there any perceived idiosyncrasies in the provisions of the Data Protection/Privacy Act as it relates to recordkeeping?
7. What are the perceived weaknesses or strengths of the legislation for records and archives management?
8. Do Records Managers and/or Archivists face any challenges when seeking to comply with the data protection/privacy legislation?
9. Is there a Code of Practice for Records Managers and Archivists to deal with data protection/privacy in XXXX?
10. If so, is the Code implementable and relevant to the work of the Records Manager and/or Archivist?
11. In your view, does the legislation require further revision?
12. What aspects of the legislation would you recommend require review and/or revision?

Key Objective – To assess the current status of data protection in the West Indies in order to inform emerging practice

1. What are your main areas of expertise?
2. Is the West Indies as a region unique in its development of legal framework?
3. What social, political and economic themes are shared by the West Indies region that impact on its legal tradition(s)?
4. To what extent have these common elements been integrated into West Indian legal frameworks?
5. Has the development of the legal system been different across the territories?
6. What is the perceived role of the Caribbean Court of Justice (CCJ) and in your view, has it been effective in fulfilling its mandate?
7. Is there a West Indian strategy for the management and sharing of information?
8. Has there been a coordinated effort to introduce any form of information rights legislation in the West Indies?
9. What information rights legislation is there in the region?
10. Does the West Indies require a more extensive regime for information rights legislation?
11. In your view, are the current practices (governance) in the West Indian public and private agencies suitable for properly regulating data protection and/or FOI?
12. What are the common challenges for the region in administering information rights legislation?
13. What are the main issues for the West Indian legal community regarding the establishment of data protection?
14. What recommendations would you give to any territory looking to establish data protection legislation?
15. Do you think that we should develop a regional model for administering data protection and FOI?
- 16.



INFORMED CONSENT FOR INTERVIEWS

[Name of Project]

I, _____, agree to be interviewed for the project entitled _____ which is being produced by [*your name*] of [*your institution*].

I certify that I have been told of the confidentiality of information collected for this project and the anonymity of my participation; that I have been given satisfactory answers to my inquiries concerning project procedures and other matters; and that I have been advised that I am free to withdraw my consent and to discontinue participation in the project or activity at any time without prejudice.

I agree to participate in one or more electronically recorded interviews for this project. I understand that such interviews and related materials will be kept completely anonymous, and that the results of this study may be published in an academic journal or book.

I agree that any information obtained from this research may be used in any way thought best for this study.

_____ Date _____
Signature of Interviewee

If you cannot obtain satisfactory answers to your questions or have comments or complaints about your treatment in this study, contact:

[your or your institution's contact information here]

Cc: signed copy to interview.

Timeline for Major Developments in Data Protection in the Selected Jurisdictions (1960 – 2012)

<u>Year</u>	<u>Development</u>
1960 – 1970	Major developments begin to take place with the emergence of microcomputers and the growing use of information and communication technologies (ICTs) in public and private agencies
1965	The U.S. House of Representatives Special Subcommittee on the Invasion of Privacy holds hearings on the effect of computers on personal privacy
1972	The Younger Committee headed by Sir Kenneth Younger produces a report on privacy establishing ten principles on the handling of personal data (UK)
1973	Sweden passes the first Data Protection Act
1974	The U.S. Government passes its first Privacy Act (Federal)
	The Canadian Government enacts the first federal public sector privacy protection in Part IV of the Canadian Human Rights Act
	White Paper entitled, <i>Computers and Privacy</i> outlines how personal information held within computerised systems should be safeguarded (UK)
1977	West Germany passes its Data Protection Act
1978	Data Protection Committee headed by Sir Norman Lindop is established in the UK to prepare the way for the setting up of permanent machinery

The Lindop Report proposes a scheme for UK data protection legislation

- 1980 Organisation for Economic Cooperation and Development (OECD) formulates its data protection guidelines (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)
- 1981 The Council of Europe adopts the 1981 Convention for Data Protection (Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data)
- 1982 Canadian Government passes Canada's first Privacy Act
- 1984 The United Kingdom passes its first Data Protection Act
- 1988 Australia passes its first Commonwealth Privacy Act
- Germany passes the German Federal Data Protection Act covering Data Protection in 16 German states
- 1993 New Zealand passes its first Data Protection Act
- 1994 Quebec passes the Respecting the Protection of Personal Information in the Private Sector Act
- 1995 European Union adopts Directive 95/46/EC based on Article 100a of the Treaty establishing the European Community
- 2001 After lengthy negotiations, the U.S. Government and the EU Commission come to an agreement in which American businesses that comply with the EU Directive are to be recognised as

providing 'adequate' levels of protection for data transfer (Safe-Harbor Agreement)

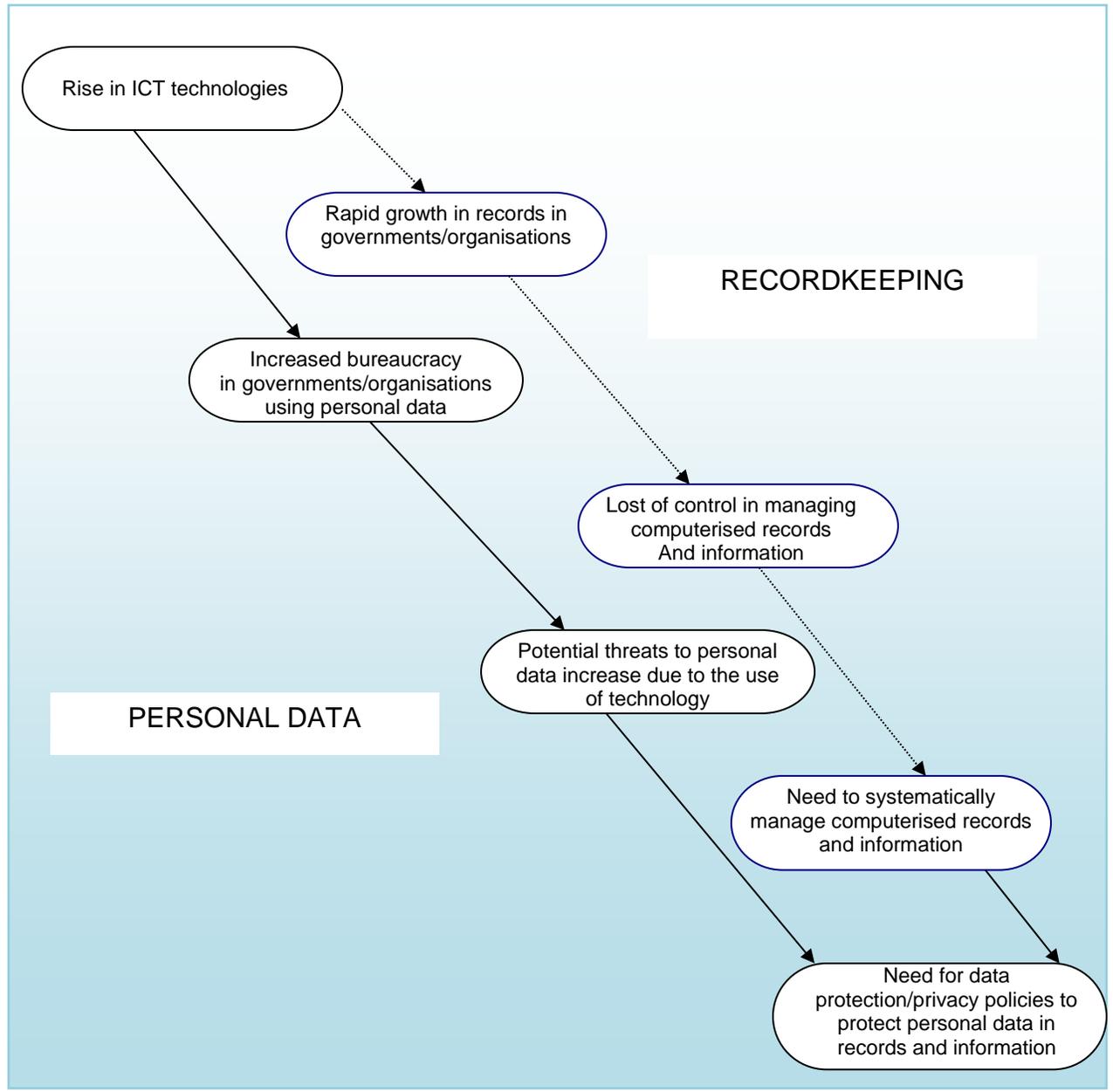
Canadian Federal Personal Information Protection & Electronic Documents Act (PIPEDA) came into effect

2002

Public consultation on the EU Data Protection Directive

2012

EU publishes proposal to reform to data protection rules



Trajectory showing Impact of ICTs on Recordkeeping and Personal Data 1960-1980

**BRITISH WEST INDIAN TERRITORIES
VS.
CARICOM MEMBER STATES**

BRITISH WEST INDIAN TERRITORIES* (Former territories of The West Indies Federation 1958-1962)	CARICOM MEMBER STATES
<ol style="list-style-type: none"> 1. Antigua and Barbuda 2. Barbados 3. Belize (associated territory) 4. Dominica 5. Grenada 6. Guyana (associated territory) 7. Jamaica 8. Montserrat 9. St. Kitts-Nevis(-Anguilla) 10. St. Lucia 11. St. Vincent and the Grenadines 12. Trinidad and Tobago 	<ol style="list-style-type: none"> 1. Antigua and Barbuda 2. Barbados 3. Belize 4. Dominica 5. Grenada 6. Guyana 7. Haiti 8. Jamaica 9. Montserrat 10. St. Kitts and Nevis 11. St. Lucia 12. St. Vincent and the Grenadines 13. Suriname 14. The Bahamas 15. Trinidad and Tobago

***The area referred to in the thesis as the West Indies is composed of the ten former British territories and two associated territories that made up The West Indies Federation 1958-1962.**

BRITISH WEST INDIES TIMELINE FROM EMANCIPATION TO PRESENT

1833

- **28 August:** The passing of the Abolition of Slavery Act. However, ex-slaves were indentured to their former owners under the Apprenticeship system.

1838

- **1 August:** The end of the Apprenticeship system in the British West Indies. Full emancipation granted to former slaves.

1871

- The British Leeward Islands Federation was established and consisted of Antigua, Barbuda, the British Virgin Islands, Montserrat, Saint Kitts, Nevis, Anguilla and Dominica.

1876

- British proposal for a confederation of Barbados and the Windward Islands triggers bloody riots in Barbados.

1930-1939

- Riots occurred across the islands of the British West Indies due to persistent poor conditions of labourer (ex-slaves).

1938

- **5 August:** A Royal Commission under the chairmanship of Lord Moyne investigated the conditions affecting workers in the British West Indies and made recommendations aimed to alleviate the conditions. A report was released in 1945.

1947

- The Montego Bay Conference (Jamaica): Meetings of the Standing Closer Association Committee.
 - The start of almost a decade of discussions and conferences in London and the West Indies on the implications of Federation.

1956

- British Leeward Islands Federation ends.
- **23 February:** Lancaster House: Signing of the agreement to federation by representatives of the ten (10) member territories.

- **29 May:** Standing Federation Committee formed to set up preliminary establishment needed for the formation of the West Indies Federation.
 - Four meetings held in Barbados, Jamaica and Trinidad

West Indies Federal Period

1958

- **3 January:** Arrival of the Governor-General, Lord Hailes and the official start of the West Indies Federation.
- **25 March:** West Indies Elections held in all ten member territories.
 - 45 representatives were elected to the Federal House of Representatives.
- **12 April:** Announcement of Federal Senators appointed by the Governor-General following consultation with member territorial Governors.
- **22 April:** Inauguration of the Federal Parliament, by HRH Princess Margaret.

1960

- **January:** New constitutions for the Windward and Leeward Islands came into effect. A Chief Minister (Premier) was appointed in each territory. The Federal Cabinet replaced the Council of State.

1961

- **September:** A Jamaica referendum went in favour of secession from the Federation and in early in 1962, the Jamaica Labour Party (JLP) headed by Alexander Bustamante won the election and led Jamaica to independence severing ties with the Federation.

1962

- **14 January:** The People's National Movement (PNM) in Trinidad, led by Dr. Eric Williams, passed a resolution rejecting any further participation in a Federation.
- **29 May:** The West Indies Federation was dissolved by the West Indies (Dissolution and Interim Commissioner) Order-in-Council (S.I. No. 1084, 1962).

Post-Federal Period

1965

- **15 December:** The Caribbean Free Trade Association (CARIFTA) was founded.

1973

- **1 August:** CARIFTA became the Caribbean Community & Common Market (CARICOM) after the signing of *the Treaty of Chaguaramas* on 4 July 1973.

1981

- **18 June:** Organisation of Eastern Caribbean States (OECS) was established by the signing of the Treaty of Basseterre.

2001

- **5 July:** Caribbean Single Market & Economy (CSME) was established by the revised Treaty of Chaguaramas.

2005

- The Caribbean Court of Justice (CCJ) was established.

2013

- CARICOM celebrated its 40th anniversary.

ECONOMIC PARTNERSHIP AGREEMENT

CHAPTER 6

TITLE II

PROTECTION OF PERSONAL DATA

Page 65 of 1953 of the
Economic Partnership Agreement

Article 197

General objective

1. The Parties and the Signatory CARIFORUM States, recognising:

(a) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data,

(b) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data;

(c) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject, agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards⁶¹⁷

2. The Signatory CARIFORUM States shall endeavour to implement the provisions of paragraph 1 as soon as possible and no later than seven years after the entry into force of this Agreement.

Article 198

Definitions

For the purposes of this Chapter:

(a) 'personal data' means any information relating to an identified or identifiable individual (data subject);

(b) 'processing of personal data' means any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, blocking, erasure or destruction, as well as transfers of personal data across national borders;

(c) 'Data Controller' means the natural or legal person, authority or any other body which determines the purposes and means of the processing of personal data.

⁶¹⁷ Such standards are those included in the following international instruments:

(i) Guidelines for the regulation of computerised personal data files, modified by the General Assembly of the United Nations on 20 November 1990; (ii) Recommendation of the Organisation for Economic Cooperation and Development Council concerning guidelines governing the protection of privacy and trans-border flows of personal data of 23 September 1980.

*Article 199***Principles and general rules**

The Parties agree that the legal and regulatory regimes and administrative capacity to be established shall, at a minimum, include the following content principles and enforcement mechanisms:

(a) Content principles

(i) the purpose limitation principle — data should be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those provided by legislation and necessary in a democratic society for important public interests;

(ii) the data quality and proportionality principle — data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed;

(iii) the transparency principle — individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information in so far as this is necessary to ensure fairness. The only exemptions permitted should be those provided by legislation and necessary in a democratic society for important public interests;

(iv) the security principle — technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller;

(v) the rights of access, rectification and opposition — the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be those provided by legislation and necessary in a democratic society for important public interests;

(vi) restrictions on onward transfers — as a matter of principle, further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection;

(vii) sensitive data — where special categories of data are involved, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures, data may not be processed unless domestic law provides additional safeguards.

(b) Enforcement mechanisms

Appropriate mechanisms shall be in place to ensure that the following objectives are achieved:

(i) to ensure a good level of compliance with the rules, including a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them; the existence of effective and dissuasive sanctions; and systems of direct verification by authorities, auditors, or independent data protection officials;

(ii) to provide support and help to individual data subjects in the exercise of their rights, who must be able to enforce their rights rapidly and effectively, and without prohibitive cost, including through appropriate institutional mechanisms allowing independent investigation of complaints;

(iii) to provide appropriate redress to the injured party where rules are not complied with allowing compensation to be paid and sanctions imposed where appropriate in accordance with applicable domestic rules.

General Privacy Principles from the Data
Protection Act (2011) of Trinidad and
Tobago

The following principles are the General Privacy Principles which are applicable to all persons who handle, store or process personal information belonging to another person:

(a) an organization shall be responsible for the personal information under its control;

(b) the purpose for which personal information is collected shall be identified by the organization before or at the time of collection;

(c) knowledge and consent of the individual are required for the collection, use or disclosure of personal information;

(d) collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization;

(e) personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;

(f) personal information shall be accurate, complete and up-to-date as is necessary for the purpose of collection;

(g) personal information is to be protected by such appropriate safeguards having regard to the sensitivity of the information;

(h) sensitive personal information is protected from processing except where otherwise provided for by written law;

(i) organizations are to make available to individuals documents regarding their policies and practices related to the management of personal information except where otherwise provided by written law;

(j) organizations shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information;

(k) the individual has the ability to challenge the organization's compliance with the above principles and receive timely and appropriate engagement from the organization; and

(l) personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

**Comments on Data Protection Policy/Bill from
the Government Archivist of Trinidad and Tobago – Avril Belfon**

Having reviewed the **National Policy on Data Protection (NPDP)** and the **Explanatory Memorandum on Data Protection Policy and Bill (hereafter “the Memo”)**, the following comments are submitted for your consideration.

1. We at the National Archives were pleased to hear that this policy is proceeding towards legislation. However, we are deeply concerned that the proposed legislation to govern the operations of the National Archives had not reached a similar stage. The principles and related policies outlined in the NPDP are intimately connected to the policies necessary for the effective management of archives and records. It is heartening to note that both NPDP and the Memo acknowledge the need for special provisions to balance issues of privacy with archival and research needs (historical, statistical and genealogical). However, without a legislative framework for the National Archives there can be no balance.

A typical example is Clause 3.5 which is based on Principle 5. Clauses 3.5.2 and 3.5.3 define conditions for retention and disposition of personal information and 3.5.2 ends with the line:

An organisation may be subject to legislative requirements with respect to retention periods.

Unfortunately, those legislative requirements for Archives and Records Management are not yet in place. There is no Archives Act to direct Ministries and Government Agencies to prepare Records Retention and Disposition Schedules as part of their Records Management Programme. There is no penalty for breaching a directive from the National Archives to safeguard or transfer records of long-term value. Thus the additional safety net necessary for Data Protection Legislation to be balanced does not exist. We ask therefore that if the Data Protection Bill must go forward then the Archives Bill must be submitted as a matter of urgency.

2. Currently, and in the proposed Archives Legislation, the Government/National Archivist must grant approval for the destruction of any public record. Part III.14 seems to be in conflict with this function.

III.14 Disposal of personal information

A public authority shall dispose of the personal information in its control or custody in accordance with regulations established by order of the Minister.

Extract from CARICOM Special Visa

CARICOM SPECIAL VISA

COUNTRIES THAT DO NOT REQUIRE A VISA

All CARICOM Nationals Except Haiti

Japan

Canada

Spain

France

South Africa

Germany

The Netherlands

Ireland

United Kingdom

Italy

United States of America

Instruction Sheet For Application Form

The CARICOM Special Visa application form can be filled out online (**recommended**), printed, signed and submitted with the relevant documents. (<http://www.caricomimpacs.org/visaform/ApplicationForm.pdf>)

If you cannot download an application form, please contact the nearest visa [issuing site](#), or any of the overseas Missions of the following CARICOM countries and request that the form be forwarded to you.

Antigua and Barbuda

Jamaica

Barbados

St. Kitts and Nevis

Dominica

Saint Lucia

Grenada

St. Vincent & The Grenadines

Guyana

Trinidad and Tobago

The CARICOM Special Visa application form is also available from any of the [United Kingdom's Missions](#) abroad.

The form is designed to be printed on plain letter size paper. Please ensure that the entire form is printed. The form should be completed online before downloading or otherwise clearly completed in block letters in blue or black ink. Applications for visas may not be submitted online since other documents need to be forwarded with your completed application.