



Libraries and Learning Services

University of Auckland Research Repository, ResearchSpace

Copyright Statement

The digital copy of this thesis is protected by the Copyright Act 1994 (New Zealand).

This thesis may be consulted by you, provided you comply with the provisions of the Act and the following conditions of use:

- Any use you make of these documents or images must be for research or private study purposes only, and you may not make them available to any other person.
- Authors control the copyright of their thesis. You will recognize the author's right to be identified as the author of this thesis, and due acknowledgement will be made to the author where appropriate.
- You will obtain the author's permission before publishing any material from their thesis.

General copyright and disclaimer

In addition to the above conditions, authors give their consent for the digital copy of their work to be used subject to the conditions specified on the [Library Thesis Consent Form](#) and [Deposit Licence](#).

PRIVACY AUDITS: EXPECTATIONS AND IMPLEMENTATION

Alan Richard Toy

A thesis submitted in fulfilment of the requirements of the degree of
Doctor of Philosophy in Accounting, the University of Auckland, 2016.

ABSTRACT

This thesis tackles pressing issues for those tasked with undertaking a privacy audit. It is the first research to directly investigate the practice of privacy auditing through interviews with privacy auditors, analysis of privacy audit reports and legal analysis of information privacy laws and policy documents. The research questions focus on issues of both theoretical and practical significance to privacy auditors. This study addresses the research questions: *What auditing standards and/or methodologies are used for privacy audits, where are they derived from, and how much convergence and/or divergence is there among standards used by different auditors? Who benefits from privacy audits and are privacy audits an appropriate way to provide benefits to them?*

The thesis departs from the positivist philosophy prevalent in accounting research. It adopts a critical perspective which is useful for this area because the theoretical basis of both privacy auditing and the information privacy rights on which the practice is based are underdeveloped. Critical research allows the thesis to propose solutions to problems identified with previous privacy audits and to suggest goals that the practice of privacy auditing might aspire to. The legal theory supporting the thesis is also anti-positivist because this thesis proposes that privacy audits may be assisted by the application of a set of fundamental principles that may be ascertained from existing information privacy legislation in the five countries that are the subject of this thesis, with the addition of principles drawn from the latest proposals for policy and legislative reform regarding information privacy rights.

The existing privacy audit reports that are analysed demonstrate that there is a large degree of divergence between the criteria used by different privacy auditors. This divergence arguably should not be explained by differences in national information privacy legislation in the five countries. If privacy audits are to be seen as useful by stakeholders then such audits

may need to be of relevance to users in multiple countries, especially where a privacy audit examines the activities of an organization that operates across national borders. Privacy issues increasingly are of global impact.

This thesis contributes to the literature in both accounting and law with published papers in academic journals of both disciplines. It also presents the results of interviews with people who include regulators and private auditors. It identifies challenges that are currently faced by those undertaking privacy audits. It examines issues including the extent to which privacy auditors see harmonization of privacy auditing standards as possible and desirable, challenges relating to the definition of privacy auditing and the skills that privacy auditors may require and how they may gain these skills. It also identifies the stakeholders of privacy audits and investigates the efficacy of the benefits that privacy audits provide to them.

The thesis aims to provide opportunities for debate about the practice of privacy auditing culminating in the potential for insights that may illuminate areas in which the practice of privacy auditing may achieve greater relevance to its stakeholders. The potential exists for privacy audits to provide assurance to users of reports where the auditee organization operates across multiple countries.

In addition to providing a potential theoretical framework for harmonization of privacy auditing criteria, the thesis contributes to the theory of privacy auditing itself through its analysis of standards and methodologies that are used in the practice of privacy auditing. The contributions of the thesis to policy regarding privacy audit criteria and the regulation of privacy auditing are in a form that could provide the flexibility for the practice to improve as changes to technology pose greater and greater challenges to the information privacy rights of citizens.

DEDICATION

I wish to dedicate this thesis to the following people whom I treasure most in my life:

My parents

Michael and Gail Toy

My sister

Dr Virginia Toy

ACKNOWLEDGEMENTS

I am most grateful to everyone who has helped me through this project. In particular, I wish to extend my gratitude to the following people:

Professor David Hay and Associate Professor Gehan Gunasekara have been ideal supervisors for me and for this project. They have continuously supported me with their advice and have given generously of their time. Their guidance is very much appreciated.

The wider support network in my department has also been vital to this project. I especially wish to thank Professor Robert Knechel, Dr Julie Harrison, Dr Fred Ng and Dr Sharlene Biswas for their wise suggestions.

The interviewees, Marty Abrams, Tanya Allen, Malcolm Crompton, Souella Cumming, Jay Fedorak, Neil Sanson and Blair Stewart. These people contributed their time and their expertise to this research. This project would not have been possible without their assistance.

My inspiration for this project comes from my grandfathers. The late Professor Richard Toy, the first of my family to achieve the degree of Doctor of Philosophy and whose architectural design I can see from my desk at the business school when I look across to Holy Trinity Cathedral. Captain Ronald Puttick set the bar high as North American Route Supervisor and was Air New Zealand's last pilot to have flown every aircraft type operated by the company.

Co-Authorship Form

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work.** Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter six (6) of this thesis is extracted from: Alan Toy and David C. Hay (2015) Privacy Auditing Standards. AUDITING: A Journal of Practice & Theory: August 2015, Vol. 34, No. 3, pp. 181-199. doi: <http://dx.doi.org/10.2308/ajpt-50932>

Nature of contribution by PhD candidate	Underlying research, substance of paper, text
Extent of contribution by PhD candidate (%)	80


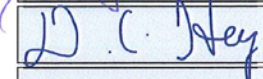
CO-AUTHORS

Name	Nature of Contribution
Alan Toy	Underlying research, substance of paper, text
David Hay	Guidance on research direction and presentation style

Certification by Co-Authors

The undersigned hereby certify that:

- ❖ the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- ❖ in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Alan Toy		Click here <i>9/9/2015</i>
David Hay		Click here <i>9/9/2015</i>
		Click here
		Click here
		Click here
		Click here

LIST OF PUBLISHERS' APPROVALS AND THIRD PARTY COPYRIGHT AGREEMENTS

The content of the following papers appears in this thesis:

Toy, A. 2013. Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy. *New Zealand Universities Law Review* 25 (5): 938-959.

Pages 82 to 112 of this thesis.

An email dated 14 June 2014 from Ursula Cheer, 2013 editor of the *New Zealand Universities Law Review*, advises that copyright remains with the author.

Toy, A. and D. Hay. 2015. Privacy Auditing Standards. *Auditing: A Journal of Practice & Theory* 34 (3): 181-199. DOI: <http://dx.doi.org/10.2308/ajpt-50932>

Pages 113 to 136 of this thesis.

A copyright transfer agreement exists which transfers copyright in this paper to the American Accounting Association. An email dated 30 September 2014 from Lisa Habblitz, Publications Coordinator for the American Accounting Association, grants permission to include this paper in this thesis.

CONTENTS

Abstract	2
Dedication.....	4
Acknowledgements	5
List of publishers' approvals and third party copyright agreements	7
Chapter 1: Introduction	11
1.1: Introduction	11
1.2: Motivation and contributions.....	12
1.3: Impetus for privacy audits	20
1.4: Research questions	24
1.5: Outline of chapters	25
1.6: Conclusion.....	27
Chapter 2: Literature Review	29
2.1: Introduction	29
2.2: Literature review	29
2.2.1 Studies of privacy disclosures and auditing	31
2.2.2 Studies of privacy that refer obliquely to privacy auditing.....	33
2.2.3 Studies of other types of non-financial auditing.....	36
2.3: Privacy audits across national borders.....	37
2.4: Privacy audits in Australia	39
2.5: Privacy audits in Canada.....	41
2.6: Privacy audits in Ireland	46
2.7: Privacy audits in New Zealand	47
2.8: Privacy audits in the United States.....	48
2.9: Conclusion.....	49
Chapter 3: Theoretical Basis	50
3.1: Introduction	50
3.2: Critical Theory.....	51
3.3: Jurisprudence	52
3.4: Conclusion.....	62
Chapter 4: Data and Approach to Analysis	64
4.1: Introduction	64
4.2: Multiple Research Methods	64
4.3: Research Design	66
4.4: Data Collection	68
4.5: Data Analysis.....	72
4.6: Ethics Approval.....	73

4.7: Documentary Analysis	74
4.8: Legal Research	77
4.9: Legal Research in this Thesis	79
4.10: Conclusion	81
Chapter 5: Different Planets or Parallel Universes:.....	82
Old and New Paradigms for Information Privacy	82
Abstract.....	82
5.1: Introduction	82
5.2: Rights in the form of principles.....	84
5.3: Challenges to information privacy law	86
5.4: International influences	87
5.5: Principles or rules?.....	88
5.6: Thesis of this Chapter: seven fundamental principles.....	94
5.7: Importance of international interoperability.....	98
5.8: European Court of Human Rights and European Court of Justice	101
5.9: European Commission.....	104
5.10: United States Consumer Privacy Bill of Rights.....	107
5.11: Federal Trade Commission	109
5.12: Conclusion	111
Chapter 6: Privacy Auditing Standards	113
Abstract.....	113
6.1: Introduction	113
6.1.1 Standards used in privacy audits	115
6.2: Genesis of Privacy Audits.....	116
6.2.1 Types of privacy audits.....	117
6.3: Principles.....	120
6.3.1 Fundamental principles for privacy audits.....	121
6.3.2 Privacy audits distinguished from Information Security Audits.....	125
6.3.3 International requirements for assurance engagements.....	125
6.4: Analysis	126
6.4.1 Results	128
6.4.2 Practice in privacy audits that are conducted by regulators	128
6.4.3 Practice in privacy audits that are conducted by auditors.....	132
6.4.4 Degree of consistency between different types of privacy audits	132
6.5: Conclusion.....	133
Chapter 7: Standards and Methodologies of Privacy Auditing and Drivers of the Practice	137
7.1: Introduction	137

7.2: Literature Review	139
7.3: Data Analysis.....	140
7.4: Theme One: Harmonization of Standards.....	144
7.4.1 Summary of Theme One.....	151
7.5: Theme Two: Definition of Privacy Audits	152
7.5.1 Summary of Theme Two.....	155
7.6: Theme Three: Privacy Audit Standards and Methodologies.....	156
7.6.1 Summary of Theme Three.....	163
7.7: Theme Four: Beyond a Pure Compliance Approach.....	165
7.7.1 Summary of Theme Four	168
7.8: Theme Five: Skills of privacy auditors	170
7.8.1 Summary of Theme Five	176
7.9: Theme Six: Privacy maturity assessment framework	178
7.9.1 Summary of Theme Six.....	180
7.10: Theme Seven: Interaction with stakeholders.....	181
7.10.1 Summary of Theme Seven.....	186
7.11: Theme Eight: Risk management and internal audit.....	188
7.11.1 Summary of Theme Eight	190
7.12: Theme Nine: Impetus for privacy audits	191
7.12.1 Summary of Theme Nine.....	193
7.13: Theme Ten: Privacy impact assessments.....	193
7.13.1 Summary of Theme Ten	195
7.14: Conclusion	195
Chapter 8: Conclusion.....	199
8.1: Introduction	199
8.2: Addressing the Research Questions.....	200
8.3: Legal theories	201
8.4: Jurisprudential perspective.....	202
8.5: Evolution of information privacy rights	204
8.6: Development of Privacy Auditing	207
8.7: Contributions.....	208
8.8: Conclusion.....	211
Reference List.....	228

CHAPTER 1: INTRODUCTION

Alan Toy

1.1: INTRODUCTION

Auditing research has not generally touched on privacy audits. This research is important because at present there are no international standards for privacy audits, even though some organisations subject to them operate on a worldwide basis. With little direct research on privacy audits society may struggle to improve the practice and any damage to the privacy rights of the population base will be exacerbated. It is worth investigating whether privacy audits could be enhanced by the adoption of a set of fundamental principles that include principles of transparency and accountability.

While the idea of privacy audits is not new, few have been done until recently. It may even be supposed that, compared to financial auditing, privacy auditing is just a drop in the ocean. Furthermore, the effects on the individual citizen are minimal even if an organization flagrantly breaches their privacy rights with its every move. And yet the harm to society as a whole is very great. Privacy audits may be mechanisms for addressing this deficit but this will only be achieved if such audits are implemented effectively. Privacy audits are now firmly on the agenda of professional services firms and some well publicized privacy audits have targeted high-profile organisations (Hill 2011). Individual citizens are concerned, and this concern is amplified by the sweeping nature of privacy violations¹ which can affect large groups of citizens at once.

¹ The Target data breach affected 70 million customers (Prah 2014) while in New Zealand the ACC privacy breach in 2012 involved the unauthorised disclosure of the personal information of 6,748 individuals (KPMG and IIS 2012).

Variation of standards impedes the development of privacy audits as an assurance service. Without a clear goal for a privacy audit, some existing audits have reverted to a simple application of the information privacy laws within a particular jurisdiction. On the other hand, some privacy audits have transcended the jurisdiction-specific nature of national legislation, incorporating wider developments in international best practice in information privacy. The latter approach produces privacy audits that are capable of providing assurance to organisations that operate internationally, and to other stakeholders such as consumers who might reside in a different country from the one in which the audit report is produced.

As privacy audits develop, new types of expertise and institutions might arise to conduct them. This may include private auditors such as audit firms developing specialised privacy audit teams, or it may go further than that. This research project identifies areas of consistent standards and methodologies between different privacy audit reports. It also uses semi-structured interviews to examine the practices of people and organisations involved with privacy audits with a view to ascertaining the standards and methodologies used in the practice of privacy auditing. Challenges to the construction of standards and methodologies for privacy auditing are also investigated.

1.2: MOTIVATION AND CONTRIBUTIONS

More and more information is being collected about people in society and it has been stated that “[t]he scope of surveillance and social control in contemporary society is at an unprecedented high” (Bygrave 2002, 100). The focus must now turn from preventing collection of personal information to overseeing its uses. The power of those who control this data is increasing and this must be matched by a corresponding increase in their responsibility. Accountability of data controllers can be facilitated by the rise of privacy

auditing. It has not been necessary until recently for privacy auditing to assume a greater role, but changes in technology now make this imperative.

The earliest privacy audits appear to have taken place in West Germany in the early 1980s (Flaherty 1989, 58). Early examples also took place in other countries in Europe and in Canada (Bennett and Raab 2003, 110). Privacy audits are related to other mechanisms of privacy governance such as Privacy Impact Assessments (Wright and De Hert 2012, 172) which can assess the effect on privacy rights of the possible implementation of a new product or service. If a Privacy Impact Assessment (PIA) is done at an early stage of development of a new product or service then a privacy audit may be done after implementation of the new product or service to assess whether or not the PIA was accurate. Privacy Enhancing Technologies (PETs) are technological mechanisms for privacy governance and they may also assist to enhance the privacy protection of citizens (Bygrave 2002, 101).

Regulatory and self-regulatory policy instruments are also relevant to privacy governance, and these may assist to protect the privacy of citizens in addition to privacy audits. Examples include United Nations guidelines in 1990 (Bygrave 2014, 51) and a Council of Europe Convention which was adopted in 1980 (Bennett and Raab 2003, 72). The International Organization for Standardization (ISO) sought to develop standards for information privacy and it has produced a set of standards in 2011² but these have not yet gained widespread acceptance. Privacy seal organizations such as TRUSTe are another example of self-regulatory attempts to protect information privacy (Bennett and Raab 2003, 129), but these are not synonymous with privacy audits and therefore they will not be discussed in detail in this thesis.

² ISO/IEC 29100:2011. Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123 (site accessed 15 February 2016).

The advent of Big Data³ has important implications for privacy and will result in increasing opportunities for breaches of privacy. The benefits of Big Data are myriad, but the danger is that people could be subject to profiling and decisions could be made without the subject individuals knowing the reasons for such decisions. Privacy audits may be a method of addressing these concerns. To guard against the possibility of loss of autonomy and individual liberty, “big data will require monitoring and transparency, which in turn will require new types of expertise and institutions” (Mayer-Schonberger and Cukier 2013, 179). For example, some tertiary institutions in the United States that have enough resources to do so, are using the social media history of individual applicants as a screening process to assist in a determination of whether to admit a student to a college or not. The potential students are sometimes not informed that their information has been used in this way (Singer 2014). Privacy concerns of consumers appear to be significant (Shelton 2010, 23), and in research by the Federal Trade Commission (FTC) in the US, “a nationwide survey indicated that 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons” (FTC 2013, 3).

Important revelations regarding the collection of personal data under the auspices of the Government of the United States have resulted in public anxiety and action, including legal action.⁴ There have also been official reports within the United States that recommend changes to official policies on data collection, due to the fact that “there have been serious and persistent instances of noncompliance in the Intelligence Community’s implementation of its authorities. Even if unintentional, these instances of noncompliance raise serious concerns about the Intelligence Community’s capacity to manage its authorities in an

³ The term “Big Data” has no formal definition, but it is generally understood that “big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more.” (Mayer-Schonberger and Cukier 2013, 6).

⁴ For example: *Klayman v Obama* [2013] 957 F. Supp. 2d 1, United States District Court for the District of Columbia, which was brought following the revelations by Edward Snowden.

effective and lawful manner” (The President’s Review Group on Intelligence and Communication Technologies 2013, 76). There is also a recommendation that “the US Government should follow the model of the Department of Homeland Security and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons” (The President’s Review Group on Intelligence and Communication Technologies 2013, 19). This indicates both an impetus for change, and a confirmation that information privacy is an issue that affects people across national boundaries. Privacy audits could assist to provide accountability in respect of personal information that has been gathered under these programs.

The President of the United States has clearly given a high priority to privacy concerns in a recent speech delivered at the Federal Trade Commission (Freeman 2015). A new Consumer Privacy Bill of Rights has now been proposed (The White House 2015). If passed, this bill would allow enforcement by the FTC of privacy rights for consumers. This is a very significant document because it supports the approach taken in this thesis. It would implement many of the fundamental principles that are discussed in more detail in chapters 3 and 4, supplemented by industry codes of conduct. However, it does not embrace the principles of Proportionality, Legitimacy and Privacy by Design to the full extent that has been recommended by the latest European proposals, and proposals by the FTC itself. Nevertheless, it would be an important step forward for the US to enact a privacy bill of rights to cover the general privacy rights of consumers. Even in its draft form, this bill can provide useful guidance to privacy auditors regarding the privacy principles that are currently seen as important, and these principles are more up to date than those enacted as “principles” in countries such as Australia and New Zealand.

Despite the risks of disclosure of personal information, a “*privacy paradox*” was noted: despite reported high privacy concerns, consumers still readily submit their personal

information in a number of circumstances” (Smith et al 2011, 993). Given that privacy is valued as a right, it may still be assigned an economic value. This has given rise to the idea of privacy as a commodity. In essence, this means that consumers trade their privacy for certain benefits (Pavlou 2011, 981). An example of such a benefit may be free access to online social networking services. However, this argument faces one major obstacle. In the case of some online social networking services, privacy controls exist and therefore consumers do not necessarily expect to give up their entire right to privacy simply by using these services (although, even if consumers expect to trade some of their privacy rights for use of these services, they do not necessarily surrender all of their privacy rights). Facebook allows consumers to restrict access to their data, and a consumer using such restrictions may not be pleased if their personal information is divulged to unauthorised persons. A recent report of the US Government claims that there exists flawed speculation that privacy cannot exist anymore because it is inconsistent with “modern communications technologies” (The President’s Review Group on Intelligence and Communication Technologies 2013, 45). According to this report, there is no basis in fact for the decline of privacy, and there is justification for a strengthening of responses by officials to adjust to new threats to privacy.

The use of new technologies is also changing the balance between privacy and other interests in the legal sphere. New judgments are striking a different balance regarding privacy and interests such as law enforcement. For example, in *Riley v California*⁵ the majority in the Supreme Court of the United States held that an appropriate balance must be struck with regard to searches of digital data on cell-phones that is different to that struck with regard to searches of other objects.⁶ In a concurring judgment, Justice Alito said that this issue required a “new balancing of law enforcement and privacy interests”⁷ This judgement prevents police

⁵ *Riley v California* 134 S. Ct. 2473 (2014).

⁶ *Ibid*, 2484.

⁷ *Ibid*, 2496-2497.

officers from performing a warrantless search of a cell-phone data even if the cell-phone is in the possession of a person who has been arrested. The basis of this ruling is that the sheer quantity of data held on a cell-phone requires different treatment from other items in a person's possession, confirming that changes in technology can result in increases in privacy legal protections. These increasing legal protections may result in different requirements for standards applied in privacy audits, depending on the extent to which privacy audit standards are aligned to the legal standards. As will be seen in this thesis however, this is not a settled issue.

Privacy audits are one way of increasing privacy protections in the age of big data and social networking. These audits investigate the flows of personal information within an organization and determine whether the organization implements appropriate privacy principles in its management of these data flows. The scope of a privacy audit relates to personal information, which may or may not be within an IT system. A privacy audit is not, therefore, an IT audit (which does not focus on implementation of appropriate privacy principles but instead focuses on a different aspect: the security of information. Even if an organization implements the best security controls available, it may still fail to implement appropriate privacy principles). It has been suggested that from a management perspective, it may be useful to have a privacy audit (Hui, Teo, and Lee 2007, 28). In Europe, "the number and frequency of [privacy] audits is increasing" (Kuner 2007, 51). However the number of privacy audits still varies widely "with hundreds performed annually in some Member States, and just a few in others" (Kuner 2007, 52). Interestingly, there has been some use of consistent privacy audit standards simultaneously in multiple states of the European Union. For example, in 2006 the Article 29 Working Party began investigation of data processing

practices in the Private Health Insurance sector. This was a “co-ordinated EU-wide investigation”⁸ that used the same methodology across the different countries.

There have been a small but increasing number of privacy audits required under orders by the FTC. These have generally targeted large, dominant players in the online environment such as Google.⁹ Another example is that Snapchat has recently been issued with a consent order that requires it to have biennial assessments that “certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.”¹⁰

There have been calls for greater harmonization of information privacy laws, and one recent survey regarding personal information finds that “73% of respondents indicated that there should be a call for a global consumer bill of rights and furthermore saw the United Nations as fostering that” (Cloud Security Alliance 2014, 6). Furthermore, the FTC has been active in recommending new initiatives to address the challenges to privacy that are presented by the rise of Data Broker organizations. These are organizations that collect personal information of consumers and then use or transfer that information with or to others. There exist privacy risks with this business model. The FTC has stated that “[t]he specific legislative recommendations made by the Commission reflect high-level principles drawn from the findings of this study, the Commission’s previous work in this area, and the ongoing public debate about data brokers” (FTC 2014, vii). These principles reflect best practices for privacy protection, such as “privacy by design, which includes considering privacy issues at

⁸ Article 29 Working Party Press Release 13 March 2006. Available from: http://ec.europa.eu/justice/policies/privacy/news/docs/etf_press_release_final_13_11_06_en.pdf (site accessed 17 December 2014).

⁹ Agreement Containing Consent Order with a service date of October 28, 2011, between Google Inc and the Federal Trade Commission (US).

¹⁰ Agreement Containing Consent Order with a service date of December 14, 2014, between Snapchat Inc and the Federal Trade Commission (US), 4. Available from: <http://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf> (site accessed 6 January 2015).

every stage of product development” (FTC 2014, 54). These policy recommendations may have significant influence on the practice of privacy auditing because the high-level principles that the FTC is recommending reflect some aspects of best practice that are not currently part of information privacy laws in any of the five countries from which data was gathered for this thesis (Australia, Canada, Ireland, New Zealand, and the United States). The FTC has an influence on privacy audits, and it “will continue to work with industry, consumer groups, and lawmakers to further the goals of increased transparency and consumer control”¹¹ (FTC 2014, 57). This indicates that the direction of the United States may be one of increased leadership in information privacy best practice. The goal of transparency is also echoed in other reports of the US Government (The President’s Review Group on Intelligence and Communication Technologies 2013, 28).

There is currently a lack of research on privacy audits in general, including the degree of harmonisation between standards and methodologies used by different privacy auditors. The development of a rigorous privacy audit discipline depends on a robust set of standards that are capable of application across different countries. This research examines the standards used in privacy audits. It appears that there is currently a wide divergence between the standards used for such audits in different jurisdictions. The research also raises the potential for convergence of standards that the practices of different organisations are assessed against, by examining international developments in information privacy best practice. The research provides opportunities for comparison and debate about best practice in information privacy.

¹¹ The National Telecommunications and Information Agency (NTIA) within the US Department of Commerce has begun to convene meetings to craft codes of practice for privacy best practices in specific industries. The “multistakeholder process to develop a code of conduct on mobile application transparency” (FTC 2013, iii) began in July 2012 and there have been a number of subsequent meetings. If the process results in the development of strong codes, the FTC may refrain from exercising its law enforcement powers against an organization that adheres to such a code (FTC 2013, 12).

1.3: IMPETUS FOR PRIVACY AUDITS

The concept of privacy audits has existed at least since Gelinas' PhD research (1978). It was not until the 1990's that publicly available privacy audits were conducted (the earliest examples are from Australia, as detailed in chapter 2 of this thesis). Many privacy audits arise from complaints to regulators such as Privacy Commissioners. An example is the audit of the Canadian Firearms Program, where it is stated that the Privacy Commissioner of Canada "has received a number of inquiries and complaints about the Program.... In part to assist our Office in responding to these complaints and inquiries, we decided in September 1999 that it was an opportune time to review the Program." (Office of the Privacy Commissioner of Canada 2001, 4). Complaints were also made regarding Staples Business Depot. Between 2004 and 2008, Staples had sold devices to consumers without properly wiping the electronic memory. Some of these devices contained personal information about Canadians, and the Canadian Privacy Commissioner commenced a privacy audit (Office of the Privacy Commissioner of Canada 2011a, 6). The most well known complaint-driven privacy audit is the audit of Facebook Ireland Ltd in 2011 (Office of the Data Protection Commissioner of Ireland 2011). This audit was done by the Office of the Data Protection Commissioner of Ireland, following receipt of a complaint by Max Schrems, an Austrian law student (Duncan 2011).

Public concern may provide the impetus for an audit in a more general way than the complaints route, and may trigger a privacy authority to conduct an audit. This is the case with the privacy audit of the Canadian Border Services Agency, which came about after findings in a 2004 study that "the Canadian public is concerned about the trans-border flow of their personal information to the United States" (Office of the Privacy Commissioner of Canada 2006, 6). The Office of the Revenue Commissioners of Ireland has "acknowledged that it shares public concern regarding a number of breaches of data security in the public

sector in recent years...” (Office of the Data Protection Commissioner of Ireland 2009, 4).

These concerns led to a privacy audit of the Office of the Revenue Commissioners by the Office of the Data Protection Commissioner of Ireland.

Highly publicised privacy breaches have also necessitated privacy audits. The Department of Social and Family Affairs of Ireland “was scheduled for priority audit in direct response to further media reports in October 2007 alleging a series of unlawful disclosures of personal data by an employee of the Department who then used the information for criminal purposes” (Office of the Data Protection Commissioner of Ireland 2008, 5). This was in the context of broader public concern over how this department was handling personal data. In Canada in 1998, information collected by the federal government and held by National Archives Canada was transferred to a contractor for disposal. The contractor instead arranged to sell the intact paper files to the highest bidder (the files contained information about thousands of Canadians such as tax information and parole records). This led to an audit by the Canadian Privacy Commissioner (Office of the Privacy Commissioner of Canada 2010a, 4). In 2008, hundreds of credit reports regarding Canadians were downloaded from 14 mortgage brokers by an unauthorised person for his own use. A privacy audit followed this breach (Office of the Privacy Commissioner of Canada 2010b, 3). The federal police force in Canada was found to be disclosing “details of convictions, discharges or pardons to employers without the informed consent of the prospective employee” (Office of the Privacy Commissioner of Canada 2011b, 3) and this also provided justification for a privacy audit. Into this category also falls the Google privacy audit (PwC 2012) which was done pursuant to an agreement struck with the FTC.¹² In New Zealand, the Accident Compensation

¹² Agreement Containing Consent Order with a service date of October 28, 2011, between Google Inc and the Federal Trade Commission (US).

Corporation was audited following a privacy breach (KPMG and IIS 2012), as was the Ministry of Social Development which also breached privacy (Deloitte 2012).

Government action may provide reasons for privacy audits. This is demonstrated with the 2007 privacy audit of nine institutions of the Canadian government, to determine their compliance with the Privacy Impact Assessment Policy that had been introduced by the Government of Canada in 2002 (Office of the Privacy Commissioner of Canada 2007, 3). A change to legislation requiring organizations to submit Federal Annual Privacy Reports also provided a reason for the Canadian Privacy Commissioner to assess compliance with this change (Office of the Privacy Commissioner of Canada 2009a, 1). The Canadian Privacy Commissioner also conducted a privacy audit in 2009 of the Passenger Protect Program, an anti-terrorist initiative set up in 2007 (Office of the Privacy Commissioner of Canada 2009b, 2).

Further impetus for privacy audits can occur due to changes at public institutions. An example is the sudden growth and change of Canadian Passport Operations. This produced a situation where an unprecedented increase in staff numbers resulted in a potentially lower level of compliance with privacy procedures because new staff had not yet completed their privacy training before starting work (Office of the Privacy Commissioner of Canada 2008a, 7). Technology upgrades such as the provision of smartphones to thousands of public servants have raised concerns regarding the protection of data and have given rise to a privacy audit of wireless environments in federal institutions (Office of the Privacy Commissioner of Canada 2010c, 1). The introduction of “naked scanners” (Schmidt 2010) by the Canadian Air Transport Security Authority also justified a privacy audit (Office of the Privacy Commissioner of Canada 2011c, 3).

Previous privacy audits or even mere investigations may also raise issues that ought to be followed up in subsequent audits. This was the case with the re-audit of Facebook Ireland

(Office of the Data Protection Commissioner of Ireland 2012, 3). It is also demonstrated in a joint audit done by the Canadian Office of the Auditor General and the Office of the Privacy Commissioner (Office of the Privacy Commissioner of Canada 2009c, 1). This is the first evidence of collaboration in Canada between these two offices in a privacy audit. An investigation of Veterans Affairs Canada also led to a subsequent audit (Office of the Privacy Commissioner of Canada 2012, 7).

The obligation to obtain a privacy audit may exist in respect of certain organisations that are subject to exceptional legal requirements. Organisations that wish to transfer data across national boundaries may encounter restrictions, such as the requirements of the EU that prevent data being transferred out of the EU to other countries that do not have acceptable levels of protection for that data.¹³ One way of ensuring an acceptable level of protection is to have Binding Corporate Rules (BCRs) that would allow data subjects to enforce rights against all entities that are part of a (possibly multi-national) organisation. It may be necessary for BCRs to provide for an audit (Bender and Ponemon 2006, 158). The EU BCR system operates in respect of organizations that are subject to the legal requirements of the EU but there is also an APEC system of Cross-border Privacy Rules (CBPRs) for the Asia Pacific region. This system is an effort to provide general requirements that could be adhered to voluntarily by an organization that wishes to operate across different APEC member states. This is based on the APEC Privacy Framework (APEC 2005) which is touched on in chapters 5 and 7, and this thesis determines it to be not sufficiently up to date. There is currently no mutual recognition between the EU and the APEC systems. Nevertheless, an informal referential guide to similarities and differences between the two approaches has been developed (APEC 2014). According to this document, the EU BCR

¹³ 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, articles 25 and 26.

system does require audits, but that the APEC system does not. Organizations in specific sectors such as the healthcare sector may also have requirements to seek privacy audits. Audits of healthcare providers relating to the Health Insurance Portability and Accountability Act (US) may be necessary (Ross and Friedman 2006, 133).

Privacy Enhancing Technologies (PETs) exist to enable citizens to implement their information privacy rights. These should be distinguished from technologies that exist to protect security (Bennett and Raab 2003, 141). It is possible that a privacy audit may consider the use of PETs by an organization.

Finally, organisations wishing to project a public image of respect for privacy may voluntarily submit to the requirements of privacy seals. Certain organisations, such as TRUSTe, provide privacy seals after they verify that an organisation has met certain minimum privacy protection requirements. In order to ensure compliance, the privacy seal organisation may require “Certified Public Accountant (CPA) audits of privacy policies...” (LaRose and Rifon 2006, 1014; Jamal et al. 2005, 94). Privacy audits have been done by members of the American Institute of Certified Public Accountants (AICPA) for WebTrust, a privacy seal organization (Hui, Teo, and Lee 2007, 28). These audits are private documents and they are not available for the research in this thesis.

1.4: RESEARCH QUESTIONS

The focus of this thesis is on ascertaining the similarities and differences between the practices of different privacy auditors with the ultimate goal of suggesting improvements that may make privacy audits more relevant to the people who benefit from them. This requires a study of the standards and methodologies used by privacy auditors as well as an investigation of who the beneficiaries are and if the current practice of privacy auditing is serving the interests of these beneficiaries.

The research questions are:

1. What auditing standards and/or methodologies are used for privacy audits, where are they derived from, and how much convergence and/or divergence is there among standards used by different auditors?
2. Who benefits from privacy audits and are privacy audits an appropriate way to provide benefits to them?

1.5: OUTLINE OF CHAPTERS

The research ascertains the degree of convergence (or divergence) between standards and methodologies used in different privacy audits. Comparisons are made across jurisdictions, as well as among different types of auditors within each jurisdiction. The research includes an assessment of international best practice in information privacy, and a comparison of this to the practice of privacy auditing in different jurisdictions. The goal is to suggest an improvement in harmonization leading to greater quality of privacy audits in terms of their relevance to stakeholders across a range of different jurisdictions, including jurisdictions that are different from the jurisdiction in which the audit originated. It is therefore important to investigate research questions that cover the standards and methodologies of privacy audits in addition to identification of stakeholders.

Chapter 1 defines the research topic and gives background on why privacy audits have arisen. This chapter serves to introduce the research questions and the motivations and contributions of the study. From the advent of Big Data to the political imperatives underlying the practice of privacy auditing, this chapter indicates why the research questions are important.

Chapter 2 examines the research that has already been conducted on the practice of privacy auditing. It details the academic literature, of which there is very little directly touching on privacy auditing, and it also examines documents from the practice of privacy auditing in the five countries that are the subject of the research in this thesis. The documents show a divergence between the practices of privacy auditors and this demonstrates the relevance of the research questions.

Chapter 3 situates the theoretical basis of the research method. The use of critical theory is enhanced by a non-positivist view of jurisprudence which gives this thesis a justification for challenging the current basis of the practice of privacy auditing. The jurisprudential arguments made in this chapter are essential to the fundamental principles which are developed in more depth in chapters 5 and 6.

Chapter 4 elaborates on the choice of research methods which are interviews, documentary analysis and legal research. It describes the approach to the interviews, data collection and analysis and ethics approval. It also describes the method of legal research which is used in the next chapter.

Chapter 5 of this thesis (Toy 2013) argues that fundamental principles of information privacy underlie the latest policy suggestions and legislative reform documents regarding information privacy in the US and the EU, and that these principles are capable of supporting the approach taken to information privacy in a number of countries. The fundamental principles are more modern than the approach taken in information privacy laws in some countries, but the process of judicial interpretation may allow some or all of the fundamental principles to be recognised, even in countries that have information privacy laws that are no longer phrased in terms appropriate to modern challenges to information privacy rights. The proposed fundamental principles could be used as standards in privacy audits, even in the absence of legislative changes in some of the countries examined in this thesis.

Chapter 6 of this thesis (Toy and Hay 2015) examines 30 privacy audit reports issued in 5 countries to determine if there is divergence or convergence between the information privacy standards used in these privacy audits. This study demonstrates that there is considerable divergence between the standards used in many of the reports, but there is also some convergence even in countries that have markedly different information privacy laws. This finding demonstrates that privacy auditing standards are not always constrained to follow the information privacy laws in a particular country. It is also argued that the considerable degree of divergence may prevent privacy audits from being useful to users in different countries, and this is of particular concern where the auditee organization is multinational.

Chapter 7 details the results of the interviews. These are grouped into 10 themes and the process by which these themes are reached and the process of coding the interview transcripts is revealed. Unlike the previous two chapters, this chapter is able to examine the views of privacy auditors directly and this produces useful insights into the practice of privacy auditing. An essential result of this chapter is that the fundamental principles that are developed in chapters 5 and 6 are not inconsistent with the future of the practice of privacy auditing, and they therefore provide one potential avenue for the further development of the practice of privacy auditing.

Chapter 8 is the conclusion which demonstrates how the research methods and the results address the research questions. It also describes the contributions of the thesis to the academic literature about privacy auditing.

1.6: CONCLUSION

Historically there has been a lack of international leadership in the standards and methodologies used in privacy audits. This has resulted in an ad hoc approach to privacy

audits, where the various auditors are striking out in directions that are not necessarily aligned to one another. This research examines the potential for a stronger direction in the area of information privacy best practice as this applies to privacy audits. The goal is to suggest improvements to the practice of privacy auditing that may result in privacy audits being more effective and useful. Privacy audits may not achieve harmonization in the standards and methodologies that are used by different privacy auditors. To the extent that harmonization is not achieved, privacy audits may struggle to be of relevance to a broad class of users.

Integration of both the legal regime in place in a particular jurisdiction and also broader developments in information privacy may produce privacy audits that provide assurance to organizations that operate internationally. Increased international comparability may increase the relevance of privacy audits to those organizations that are subject to them and also to other users of privacy audits such as consumer advocacy groups, and provide a fertile source for enhancements in information privacy best practice.

Research on privacy auditing is necessary at this time due to increasing pressures from legislation and regulatory authorities for privacy audits to take place. Privacy auditors have not had a strong basis of existing research to complement their investigations. Existing privacy audits have sometimes required significant research by the privacy auditors themselves as an initial part of the investigation process, as was the case with the review of the Accident Compensation Corporation in New Zealand (KPMG and IIS 2012).

CHAPTER 2: LITERATURE REVIEW

Alan Toy

2.1: INTRODUCTION

With the notable exception of a PhD thesis in 1978, there are few studies which examine the practice of privacy auditing directly. However, there are a small number of studies in which privacy disclosures are examined along with aspects of privacy auditing. These are substantively different from the research in this thesis because privacy disclosures are not examined here. This thesis is focused directly on the practice of privacy auditing.

Due to the lack of direct studies of privacy auditing, the literature review does not focus solely on previous research but it also encompasses literature from the practice of privacy auditing itself. Such literature includes privacy audit reports from the five countries from which data has been collected for this thesis (Australia, Canada, Ireland, New Zealand and the United States). This literature enables insights into the standards used for privacy audits in those jurisdictions. It is essential for the research in this thesis because it demonstrates that difficulties may be faced by any attempt to harmonize the standards used by privacy auditors across different jurisdictions.

2.2: LITERATURE REVIEW

There have been only a small number of direct studies of privacy auditing although some studies have mentioned it obliquely and privacy auditing may be studied in a way that is similar to studies of other forms of auditing. The most relevant studies will be mentioned first, beginning with studies of privacy auditing itself and then moving one degree out to

studies that examine privacy disclosures and auditing. After this, studies that obliquely mention privacy auditing are surveyed followed by studies that do not mention privacy auditing but that may provide guidance on the ways in which privacy auditing may be studied. This final category includes studies of other types of non-financial auditing such as sustainability auditing.

The only direct study is a PhD thesis by Gelinas (1978). This was completed shortly after enactment of the Privacy Act of 1974 (US) which enacted privacy laws that cover information held by the federal government (but not information held by the private sector). This is a normative study focused on the argument that accountants can perform privacy audits. A lasting contribution of his thesis to the literature on privacy audits is Gelinas' argument that there should be Generally Accepted Privacy Principles (GAPPs). In later years, the American Institute of Certified Public Accountants (AICPA 2009) promulgated some different GAPPs, although they have not been used in many of the privacy audits examined in this thesis. However, there remains the possibility for the AICPA GAPPs to be used in Service Organization Control Reports, also termed SOC 2 reports (AICPA 2012). Two of the GAPPs proposed by Professor Gelinas in 1978 relate to the fundamental principles which are elucidated in chapter 3 of this thesis. These are: Openness (translatable to the fundamental principle of Transparency) and Accountability (which is a fundamental principle). The 2009 GAPPs promulgated by AICPA and CICA are different to Professor Gelinas' original formulation, and two of the ten 2009 GAPPs relate to fundamental principles. These are Notice (which translates to the fundamental principle of Transparency) and Choice and Consent (which translates to the fundamental principle of Consent).

This thesis departs from the methodology of the previous studies. This is because it directly studies privacy auditing and so it does not benefit from the quantitative methodologies employed by the disclosure studies, which have numerical data to observe.

Gelinas' study of privacy auditing uses some normative arguments, which is one of the methods employed in this thesis. However, his study did not use any other forms of data collection and analysis. This may be because, in 1978 when Gelinas' study was done, there were no privacy audits being conducted. This thesis studies the practices of privacy auditors using qualitative techniques and legal research that enable this study to examine practices that Gelinas could not observe.

2.2.1 STUDIES OF PRIVACY DISCLOSURES AND AUDITING

Cortez and Hay (2014) is one of the few studies of privacy auditing to use quantitative data. They examine whether there is any correlation between disclosure in an audited financial report regarding the information privacy practices of an organization and privacy breaches by that organization. In finding that there is a correlation, this study discovers an effect regarding frequency of privacy breaches by organizations that disclose prior to a breach, and an effect regarding subsequent disclosure by companies that have previously breached privacy. For example, organizations that have breached privacy are more likely to disclose their privacy practices afterwards, although there is some variation depending on the type of organization and the type of privacy breach. They present statistical summaries of the data and they perform multivariate analyses to expose the relationships that they report. Due to the fact that data regarding privacy audits is unavailable, this study uses privacy disclosure in 10-k reports as a proxy for the incidence of privacy audits.

Jamal, Maier and Sunder (2003) examine disclosures including privacy policies and privacy seals (such as TRUSTe)¹⁴ of 100 websites. After registering an account on each website, they examine resulting incoming emails to determine whether those websites are

¹⁴ TRUSTe is an organization that provides privacy services, including some that may fall under the broad definition of 'privacy audit' that has been adopted in this thesis. Available at: <http://www.truste.com/business-products/trusted-websites/> (site accessed 2 March 2015).

true to their promises regarding uses of personal information. This study looks at privacy seals, whether or not they include privacy audits, but not at other types of privacy audits. These privacy seals use four different privacy standards, which is evidence of fragmentation of approaches within just one jurisdiction (the United States). This finding is relevant to the research in this thesis, but not directly because the standards used by privacy seal organizations are not necessarily the same as those used by privacy auditors.

Jamal, Maier and Sunder (2005) is a second article in the same journal. Here they use the same procedure as that used in their earlier article, using privacy disclosure to examine regulation and conventions in financial reporting by gathering data from 56 websites in the United Kingdom. They argue that a web seal is analogous to a privacy audit (Jamal, Maier and Sunder 2005, 83) but this is not a perfect analogy. Some privacy audits have nothing to do with the activities of web seal organizations. No publicly available privacy audits by web seal organizations are available as a subject of research, therefore they are not explored in this thesis. The certification activities of web seal organizations are outside the scope of this thesis, which examines privacy audits directly (web seals being merely an application of privacy audits, and one that cannot be studied in detail using the methodology in this thesis).

However, this second article is a major support for this thesis in a different way. Part 3 of chapter 3 of this thesis elucidates the theoretical basis for the suggestion that privacy auditors may not use information privacy laws in a particular jurisdiction to provide standards for a privacy audit but may instead look to international best practice for information privacy. Jamal, Maier and Sunder argue that “[t]he limited evidence available on the interplay between law and social norms suggests that people ignore laws that are inconsistent with prevailing social norms” Jamal, Maier and Sunder (2005, 75). For reasons that will be explained further in chapter 3, this is an anti-positivist statement. Furthermore, this article adds to the discussion on principles versus rules in information privacy by stating that

“[d]etailed rules are supported by an inclination to enforce them by law, whereas general principles require judgment in an environment that values social norms” Jamal, Maier and Sunder (2005, 75). This supports the argument in favour of fundamental principles that is developed in chapters 5 and 6 of this thesis (Toy 2013; Toy and Hay 2015).

2.2.2 STUDIES OF PRIVACY THAT REFER OBLIQUELY TO PRIVACY AUDITING

Some studies have made reference to privacy auditing, although it is not their primary focus. Flaherty (1989) is the first cross-national study of information privacy/data protection. This is a descriptive and normative work that details the historical roots of data protection practices in several countries. Flaherty points out that in West Germany, the federal Data Protection Commissioner was conducting privacy audits in the 1980s. These are described as audits of information systems in which “[t]he audit team attempts to point out security weaknesses in an information system and to evaluate local controls for data protection” (Flaherty 1989, 58). Thus, it appears that these early privacy audits were very closely related to audits of information systems (although care should be taken to avoid confusion between the two types of audits which are now seen as separate as described in section 6.3.2 of this thesis). In France, the National Commission on Informatics and Liberty performed investigations, and by at least the late 1980s was conducting “audits” (Flaherty 1989, 204). In Canada, the first privacy audit by the federal Privacy Commissioner took place in 1984-1985 and this was influenced by the practices used in the early audits in West Germany (Flaherty 1989, 266).

Bennett and Raab (2003) is a descriptive and normative work that focuses on the politics of protection of personal information. They examine the policy imperatives behind governance mechanisms for personal information. They describe the role of data protectors such as privacy commissioners, and this includes the auditing role of commissioners in Germany and Canada, and also in the Netherlands (Bennett and Raab 2003, 110).

Elliott (1997) is a normative study that discusses opportunities for accountants to branch out into other types of assurance services, including assurance services regarding personal data of consumers (Elliott 1997, 68). The point is made that accountants have a strong auditing tradition which will assist them to provide these types of assurance, and that the demand for such services exists and this demand will be met by others if accountants choose not to. This supports the suggestions in this thesis because this thesis argues for advances in the practice of privacy auditing that may improve the relevance of privacy audits to beneficiaries. Improved relevance may lead to increased deployment of privacy audits.

Boritz and No (2011) is a study that uses documentary analysis to review the literature regarding e-commerce and privacy, finding that there are opportunities for further study, including in the area of privacy assurance services. They search four journal databases using particular search terms to identify articles that examine privacy and e-commerce, identifying areas in which further research is needed. They discuss the scope of a privacy assurance engagement, which “can cover: (1) either all personal information or only certain identified types of personal information, such as customer information or employee information; and (2) all business segments and locations for the entire entity or only certain identified segments of the business...” (Boritz and No 2011, 25). This is a useful summary because, as will be seen later in this thesis, it echoes the statements of some of the interviewees regarding the potential scope of a privacy audit. This article also supports the research in this thesis in a major way. It is stated that “[r]esearch is needed to examine to what extent and how GAPP and related Trust Services are being used in e-commerce and how they compare to other privacy principles such as the U.S. FTC’s FIPs and OECD guidelines” (Boritz and No 2011, 36). The FTC’s FIPs (Fair Information Practices) are discussed in chapter 5 of this thesis and they are compared to other privacy principles such as those in the OECD guidelines (Toy 2013).

Smith, Dinev and Xu (2011) also use documentary analysis to classify the literature across a range of disciplines relating to information privacy. They identify different understandings of privacy ranging from the view of privacy as a right in some legal literature to privacy as control in some information systems literature. They identify strong normative arguments for privacy, but they argue that more empirically based studies should be done (Smith, Dinev and Xu 2011, 1005). They also advise more of a focus on privacy in its international dimension (Smith, Dinev and Xu 2011, 1007). This is relevant to this thesis because it employs empirical techniques by using documentary analysis and interviews to examine the practices of privacy auditors.

Hui, Teo, and Lee (2007) use a field experiment to study the perceptions of consumers relating to privacy practices of organizations. Participants were invited to visit a website and to fill out a survey (and a follow up survey) on the website to indicate their perceptions. This study finds that the existence of a privacy policy on the website of an organization engenders a greater level of trust among consumers, leading to an increased level of disclosure of their personal data to an organization that displays a privacy policy. However, they also find that the display of a privacy seal on the website of an organization does not have any effect on the willingness of consumers to disclose data about themselves to that organization. In their discussion of this result, they note that “given that our subjects were familiar with TRUSTe, one possible explanation for its insignificance in the experiment is that the subjects did not trust it, and hence that their behaviour was not affected by its presence” (Hui, Teo, and Lee 2007, 27). In order to increase the effectiveness of privacy seals, they recommend more privacy reviews and audits. As with other studies in this category, this study does not directly examine privacy audits, and it is not apparent that this type of methodology would be effective to examine privacy audits because there is

insufficient evidence that consumers have an understanding of privacy audits that would allow them to respond in a meaningful way to questions about privacy audits.

2.2.3 STUDIES OF OTHER TYPES OF NON-FINANCIAL AUDITING

Some studies examine the rise of other types of assurance, and this is relevant by analogy with privacy assurance because this is a new type of assurance service. Radcliffe (1999) uses ethnography to study efficiency auditing. This study uses a form of *triangulation* which involves using multiple research methods “including interviews, passive observation and documentary analysis” (Radcliffe 1999, 344). The passive observation includes listening to audit planning meetings. The purpose of Radcliffe’s interviews is mainly to validate the correctness of the results of the documentary analysis and the passive observation.

“Triangulation and use of multiple methods provided broader and more reliable information than any one approach alone” (Radcliffe 1999, 344). Radcliffe’s study is an effective use of qualitative research to study a type of assurance, and this thesis also uses multiple research methods to study privacy auditing, although ethnography is not used, and the case study method is used instead. This thesis also uses legal research, which Radcliffe does not use, mainly due to differences in issues and subject matter between efficiency auditing and privacy auditing.

Free, Salterio and Shearer (2009) study auditability of MBA rankings, a novel type of assurance. They use interview data and archival sources (such as working papers from the audit firm itself and other sources such as newspapers and academic articles) to investigate this type of assurance. They find that “participating schools attend seriously to the requirements of the “audit”, and that they do so because they fear a loss of legitimacy if the “audit” should reveal exceptions” (Free, Salterio and Shearer 2009, 131). They note “the power of the idea of ‘audit’ – and its ready exportability from the financial audit context”

(Free, Salterio and Shearer 2009, 120). This thesis also uses interview data, along with documentary analysis and legal analysis. Working papers from privacy auditors are not available, but this thesis uses legal materials as an additional source.

O'Dwyer (2011) investigates the construction of sustainability assurance. He uses interviews and documentary analysis to investigate this topic. He conducts 36 interviews with staff spread across two of the Big Four professional services firms. These interviews took place over a period of five years because this is a longitudinal study which aims to ascertain the development of sustainability auditing over a period of time. There are some important differences between O'Dwyer's method and the method used in this thesis. This thesis does not aim to study the development of privacy auditing over time because it aims to suggest improvements that could be used by privacy auditors to enhance the practice of privacy auditing. This objective would be lost if the study were to continue for several years before reporting any results. Also, O'Dwyer gives a commitment of confidentiality to his interviewees, which is not appropriate for the study of privacy auditing. This is because the number of privacy auditors is very small, and in some countries there is only one privacy auditor in the category of regulator organizations. The discussion of results in this thesis would have been unduly restricted if the same guarantee of confidentiality had been given, therefore O'Dwyer's method is not followed precisely in this thesis.

2.3: PRIVACY AUDITS ACROSS NATIONAL BORDERS

A complex aspect of privacy audits is that the organizations that are subject to them often operate across national borders. This is not always the case however, as the ACC privacy audit in New Zealand is an example of an audit of a domestic agency. However, Google and Facebook have both had privacy audits. The Google privacy audit took place in the US and the Facebook privacy audit took place in Ireland. The main question that is raised when an

organization operates in multiple countries is whether it is subject to information privacy laws in all of those countries, or only some or none of them. It appears at least arguable that a single organization may be subject to the information privacy laws of more than one country (Toy 2010). However, this argument involves only the issue of substantive jurisdiction, and does not address enforcement and other practical problems. For example, issues regarding how a judgment of a New Zealand court may be enforced against an organization that is not established in New Zealand are not resolved by this argument.

Although there have been calls for harmonization of global standards for information privacy law, this may raise “unrealistic expectations” (Kuner 2013, 164). The differences between information privacy laws of different countries may therefore continue to exist. However, this need not present a problem for privacy audits. Privacy audits need not be a mechanical application of the information privacy laws within a single jurisdiction, but may instead apply standards for privacy auditing that may have more in common across different countries than information privacy laws do. This is not a resolved issue however, as some privacy audits do represent application of the information privacy laws of just one country. For example, the privacy audit of Facebook Ireland demonstrates this approach. On the other hand, the privacy audit of Google demonstrates a departure from application of information privacy laws, instead focusing on other standards for the audit.

It is common for initiatives for international harmonization of privacy auditing standards to contain suggestions that auditing may be used to examine compliance with standards, for example in relation to the ISO privacy standards.¹⁵ The APEC system of Cross

¹⁵ ISO/IEC 29100:2011, 19. Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123 (site accessed 15 February 2016).

Border Privacy Rules (CBPRs) provides for accountability agents¹⁶ which can certify that the privacy practices of an organization are compliant with APEC's rules.

As privacy audits in different countries often contain significant differences, it becomes necessary to consider the position in different countries separately. Five countries are selected as the context of the research; The United States, Canada, Ireland, Australia and New Zealand. They are selected due to data availability as all five are English-speaking countries and all have publicly available privacy audit reports. Also, interviews are possible with relevant people from four of the five countries (the exception being Ireland). Ireland is chosen as a representative country from the European Union (EU) because the EU has been very influential in the field of information privacy/data protection. Ireland is the place in which the privacy audit of Facebook Inc was undertaken so it is important to include this country. The five countries in which research on privacy audits is conducted in this thesis are now examined.

2.4: PRIVACY AUDITS IN AUSTRALIA

Australia has produced some of the earliest independent privacy audits. Australia Telecom appointed an audit panel in 1994, one member of which was an independent privacy auditor. This panel was established to “oversee the development and conduct of privacy audits of Telecom operations.” (Greenleaf 1994). The company (which had changed its name to Telstra) had its first privacy audit in 1995. This was an independent audit done by PwC, and was done following claims in 1994 that some employees of the company had recorded telephone conversations of customers without their consent. The audit examined both Telstra's compliance with its privacy policy, and legal requirements, and also compliance

¹⁶ Details of approved accountability agents can be found here: <http://www.cbprs.org/Agents/AgentDetails.aspx> (site accessed 15 February 2016).

with international privacy standards (Haines 1996). This demonstrates the importance of both a privacy policy and legal requirements as a set of standards for a privacy audit, and this is consistent with early guidance on privacy audits (Jerskey 1996, 4; Bean and Hott 2006, 24).

The Telstra audit is significant, not just for its examination of both legal and privacy policy standards, but also for its choice of international best practice as relevant criteria for a compliance-based privacy audit. Although Telstra's actual level of compliance with the standards has been discussed elsewhere (Greenleaf 1996), this audit is the first evidence of use of international standards as criteria for a privacy audit. Australia's use of privacy audits at this time was in advance of developments in other countries. Canada was soon to have privacy audits of organisations, but it had not established them at the time of the first independent Telstra audit.

Although the Office of the Australian Information Commissioner (OAIC) and the Australian Privacy Commissioner have previously had "no general power to "spot audit" the privacy compliance of organizations..." (ALRC 2008, 1581), the existing audits have been done as part of the Commissioner's function "to conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the information privacy principles."¹⁷ It is clear that this power to conduct a privacy audit applies to assess compliance with the information privacy principles. The Passenger Name Record data audit demonstrates this very narrow approach. This audit assessed compliance against the information privacy principles in s14 of the Privacy Act 1988 (Cth) (Office of the Australian Information Commissioner 2012). This audit represents an assessment of compliance against the minimum legal criteria.¹⁸

¹⁷ Privacy Act 1988 (Cth), s27(1)(h).

¹⁸ Further examples of OAIC audit reports that assess compliance against only the principles in s14 of the Privacy Act 1988 (Cth) include: Office of the Australian Information Commissioner. 2011. *National Document Verification Service, Centrelink – Audit Report*; Office of the Australian Information Commissioner. 2011. *Australian Federal Police (ACT Policing Branch) Audit Report*; Office of the Australian Information Commissioner. 2011. *ACT – Department of Disability, Housing and Community Services, The Office for*

The narrow approach currently used by the OAIC may include some industries in which additional legal requirements apply, such as the healthcare industry. Although there are some additional criteria in this area, consideration of them during an audit does not go outside compliance with the minimum legal standards currently in effect in Australia. An example is the Medicare Australia audit report, which assessed compliance against the Healthcare Identifiers Act 2010 (Cth), the Healthcare Identifiers Regulations 2010 and s14 of the Privacy Act 1988 (Cth).¹⁹

2.5: PRIVACY AUDITS IN CANADA

The Office of the Privacy Commissioner of Canada has conducted a number of privacy audits.²⁰ The Commissioner has powers to audit under both the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada) and the Privacy Act (Canada). These statutes cover two separate spheres; public and private. There are some important differences between these two spheres of operation as regards the audit powers of the Canadian Privacy Commissioner, so they will be discussed separately. As Canada is a federal jurisdiction, authorities at the provincial level also have powers to conduct privacy audits, although the interviewees from the Office of the Information and Privacy Commissioner for British Columbia stated that, while there is a fine line between investigations and auditing, no actual privacy audits had been conducted at the provincial level in British Columbia at the time of data collection for this thesis. Their office had conducted investigations, and was moving toward conducting privacy audits at the provincial level.

Children, Youth and Family Support Audit Report; Office of the Australian Information Commissioner. 2012. *National Document Verification Service – Department of Foreign Affairs and Trade – Audit Report 2012*.

¹⁹ Office of the Australian Information Commissioner. 2011. *Healthcare Identifiers Service – Medicare Australia Audit Report*. Another example that uses the same criteria is: Office of the Australian Information Commissioner. 2012. *Healthcare Identifiers Service – Department of Human Services – Audit Report*.

²⁰ Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 24 April 2013).

The Privacy Act applies to government institutions.²¹ Under this Act: “The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8.”²² Although the power to conduct these investigations under the Privacy Act appears to be constrained, the Canadian Privacy Commissioner has occasionally gone beyond simple assessment of compliance with sections 4 to 8. In 2001 the Canadian Privacy Commissioner audited the Canadian Firearms Program, and this audit used sections 4 to 12 of the Privacy Act (Canada) as a set of standards (Office of the Privacy Commissioner of Canada 2001, 8). This expanded scope includes sections of the Privacy Act that deal with information banks and rights of access. Even though the power to conduct investigations under the Privacy Act does not include compliance with this expanded list of sections, the organizations subject to the Privacy Act need to comply with those sections in any event.

PIPEDA is the statute for the private sector. It applies to personal information that “the organization collects, uses or discloses in the course of commercial activities...”²³ PIPEDA subjects these organizations to a much broader audit regime than is the case for organizations that are subject to the Privacy Act (Canada). Also, private sector organizations may be subject to audits using a broader range of standards than those enacted in PIPEDA itself. PIPEDA gives the Canadian Privacy Commissioner the power to: “audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is... not following a recommendation set out in Schedule 1...”²⁴ This power to audit the information management practices is arguably broader than mere use of the 10 PIPEDA principles set out in Schedule 1. The PIPEDA

²¹ Privacy Act RSC 1985 (Canada), s2.

²² Ibid, s37(1).

²³ Personal Information Protection and Electronic Document Act SC 2000 (Canada), s4(1)(a).

²⁴ Ibid, s18(1).

privacy principles are more in line with international best practice than those in the Privacy Act (Canada). The PIPEDA audit power could allow additional criteria beyond the 10 principles specified in PIPEDA itself to be used in a privacy audit.

Use of the Privacy Act (Canada) is effective implementation of the legal regime in place in that country as a relevant set of standards for this compliance audit. Sections 4 to 12 of that Act embody a number of rules that reflect the old paradigm for information privacy and are reminiscent of the privacy regimes in countries such as Australia and New Zealand. Use of rules in the Customs Act (Canada); and Treasury Board policies demonstrates further evidence of application of the legal regime within that jurisdiction as standards for the audit.

One Canadian privacy audit focused on the duty of certain federal institutions to produce annual privacy reports.²⁵ This audit assessed compliance mainly against Treasury Board Secretariat requirements. However, the standards used in this audit incorporated some of the requirements of other sections of this Act.²⁶ Another audit was the audit of Transport Canada's Passenger Protect Program. This audit used criteria in the Privacy Act (Canada) and the Aeronautics Act (Canada) to assess compliance, and it also "embrace[d] the audit standards recommended by the Canadian Institute of Chartered Accountants [(CICA)]."

(Office of the Privacy Commissioner of Canada 2009b, 13, 15) It is unlikely that this refers to the Generally Accepted Privacy Principles (GAPPs) (AICPA and CICA 2009) as no evidence of assessment against the GAPPs can be found in the report, aside from criteria that would also apply under the Privacy Act (Canada). Therefore, this statement is likely to refer to audit practices or methodologies recommended by CICA, rather than substantive privacy criteria.

A similar statement is found in a further audit of federal institutions, which followed the "spirit of the audit standards recommended by the Canadian Institute of Chartered

²⁵ Office of the Privacy Commissioner of Canada. 2009. *Audit Report of the Privacy Commissioner of Canada: Federal Annual Privacy Reports*. The legal duty to produce annual privacy reports is found in s72 of the Privacy Act RSC 1985 (Canada).

²⁶ *Ibid*, 10. This included the requirements of s8 of the Privacy Act RSC 1985 (Canada).

Accountants.” (Office of the Privacy Commissioner of Canada 2010a, 18) This audit also derived criteria from the Privacy Act (Canada), the Library and Archives of Canada Act (Canada), and the “Policy on Government Security and related standards.” (Office of the Privacy Commissioner of Canada 2010a, 17). As with the other audits mentioned in this paragraph, this is a narrow set of audit criteria that mainly takes account of the legal environment in which the particular subject organisation operates, without necessarily addressing modern privacy practices.

The GAPPs have been used as standards in at least one Canadian audit of selected federal institutions. Criteria for this audit included “modern privacy principles and best practices that are not enshrined in the *Privacy Act*” (Office of the Privacy Commissioner of Canada 2009c, 11). This audit was done under the Privacy Act (Canada), so there was no legislative requirement for any assessment beyond sections 4-8 of the Privacy Act. Nevertheless, the Canadian Privacy Commissioner has demonstrated a broader approach in this audit. The unusual element is that this report was done in the same year as some of the reports discussed in the previous paragraph, which used comparatively narrow criteria. A further audit of wireless environments in federal institutions used a set of criteria that included standards drawn from: “[T]he *Privacy Act*, relevant Treasury Board policies, Generally Accepted Privacy Practices, IT Governance Institute, Control Objectives for Information and Related Technology... and the Information Technology Infrastructure Library (ITIL) Framework” (Office of the Privacy Commissioner of Canada 2010c, 12). This demonstrates that the GAPPs were used, in addition to the relevant domestic legal requirements. Information technology standards were also used as criteria, which is appropriate given that the subject matter of the audit was wireless environments. This audit also followed the spirit of the CICA audit standards.

A Canadian audit that used a narrow set of standards that included only the PIPEDA principles and the CICA audit standards was the audit of selected mortgage brokers (Office of the Privacy Commissioner of Canada 2010b, 14, 15). As this audit was of a private sector organization, the authority for the audit came from PIPEDA itself, so the use of the PIPEDA principles in the audit is merely evidence of application of the existing legal regime in place, and does not demonstrate a broader approach, as use of the PIPEDA principles in audits of public sector organisations does. While some of the PIPEDA principles reflect fundamental principles, they do not reflect all such principles. These fundamental principles are central to this thesis and are discussed in more detail in chapters 5 and 6. The audit of Staples Business Depot is a further example of a narrow PIPEDA-based audit (with the CICA audit standards) of a private sector organisation (Office of the Privacy Commissioner of Canada 2011a, 22, 23). An equally narrow audit resulted from the examination of the Canadian Air Transport Security Authority. As a public institution, this audit was done under the Privacy Act (Canada) and applied, in addition to the CICA audit standards, criteria “derived from the *Privacy Act* and Treasury Board Secretariat policies, directives and standards directives related to the management of personal information.”²⁷ This is arguably an even narrower set of standards than the PIPEDA audits, as PIPEDA incorporates a small number of the developing fundamental principles (Toy 2013), while the Privacy Act rules are not translatable to any of the fundamental principles.²⁸

²⁷ Office of the Privacy Commissioner of Canada. 2011. *Privacy and Aviation Security: An Examination of the Canadian Air Transport Security Authority: Audit Report of the Privacy Commissioner of Canada*. 29. An audit that used the same criteria was: Office of the Privacy Commissioner of Canada. 2012. *Veterans Affairs Canada: Audit Report of the Privacy Commissioner of Canada*.

²⁸ An audit with equally narrow criteria was: Office of the Privacy Commissioner of Canada. 2011. *Audit of Selected RCMP Operational Databases: Audit Report of the Privacy Commissioner of Canada*. 19-20. This audit used audit criteria derived from the Privacy Act (Canada) and criteria from the Control Objectives for Information and Related Technology, and government policies and standards, plus the CICA audit standards.

2.6: PRIVACY AUDITS IN IRELAND

Ireland is the jurisdiction which contains Facebook's servers for all of its non-North American customers. This means that it is the location in which the privacy audits of Facebook Ireland Ltd have taken place. While this does not necessarily mean that Facebook could not be liable for breaching the data protection laws of another jurisdiction (Toy 2010), it makes Ireland an important country for this thesis to examine.

The Office of the Data Protection Commissioner of Ireland (ODPC) has done a number of audits, beginning in 2008.²⁹ These audits used the requirements of Irish Data Protection Laws as a set of standards (Office of the Data Protection Commissioner of Ireland 2008, 4; Office of the Data Protection Commissioner of Ireland 2009, 4). This is consistent with privacy audit advice offered by the Commissioner's office, which states that "[a]n audit by the ODPC checks for compliance against data protection laws only" (Office of the Data Protection Commissioner of Ireland 2014, 6). However, this guidance briefly states that "[o]rganisations audited are encouraged to achieve 'best practice' as opposed to mere compliance with data protection legislation" (Office of the Data Protection Commissioner of Ireland 2014, 4). The first audit of Facebook Ireland Ltd was "conducted taking account of the 8 principles of data protection."³⁰ Only one of the fundamental principles of information privacy international best practice is recognised within these, the principle of Proportionality. For a company that operates internationally, as Facebook Ireland Ltd does, it is arguable that international best practice is a highly relevant set of standards for a privacy audit, as defined in chapter 4 of this thesis. Companies that operate internationally may be subject to information privacy laws in the countries in which they operate (Toy 2010).

²⁹ Available at: <http://www.dataprotection.ie/docs/Audit-Reports/1293.htm> (site accessed 25 April 2013).

³⁰ Data Protection Commissioner of Ireland. 2011. *Facebook Ireland Ltd: Report of Audit*. 24; These principles emanate from the Data Protection Act 1988 (Ireland) and the Data Protection (Amendment) Act 2003 (Ireland).

As with the new provisions in Australia, the legal powers of the Office of the Data Protection Commissioner of Ireland to conduct privacy audits are tied to the requirements of the Irish legislation.³¹ This may limit the ability of the Commissioner to apply the fundamental principles described in chapter 6 of this thesis. The new proposed EU Regulation would require entities that hold personal information to “implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation” (European Commission 2012, Article 22(1)) and: “If proportionate, this verification shall be carried out by independent internal or external auditors” (European Commission 2012, Article 22(3)).

2.7: PRIVACY AUDITS IN NEW ZEALAND

New Zealand privacy audits have been done by private independent auditors. This was the case with the audit of the Accident Compensation Corporation (ACC) which was done by IIS and KPMG. This audit “goes beyond simply compliance with privacy law and addresses wider privacy challenges and opportunities including allocation of risks and individual trust.” (KPMG and IIS 2012, 23) It took account of guidance from other privacy authorities, and “[d]raws on privacy best practice including the concept of Privacy by Design...”. (KPMG and IIS 2012, 24).

In contrast to the broad set of standards used in the above audit, the audit of the Ministry of Social Development used only the requirements of the Privacy Act 1993 as a set of standards to assess privacy compliance. (Deloitte 2012, 6) In defence of this approach, the

³¹ Specifically, s10(1)(a) of the Data Protection Act 1988 (Ireland) and the Data Protection (Amendment) Act 2003 (Ireland) gives the Data Protection Commissioner the power to investigate where the provisions of the legislation may have been contravened.

focus of this audit was designed to be a review of the security of information systems in place in the Ministry, and privacy was merely a secondary line of enquiry (Deloitte 2012, 10-11).

2.8: PRIVACY AUDITS IN THE UNITED STATES

In the US, the first Google privacy audit by PwC was completed in 2012. The audit used the 5 principles in Google's privacy policy (PwC 2012, 1-2.). However, only 3 of the 7 emerging fundamental principles are part of this audit (Toy and Hay 2015). The audit did not specifically examine international standards, and this left the choice of standards entirely down to Google when setting its own privacy principles. The independent auditor carefully disclaimed that: "We are not responsible for Google's interpretation of or compliance with privacy-related laws, statutes and regulations applicable to Google in the jurisdictions within which Google operates." (PwC 2012, 14). This is a departure from the privacy audit standards used in privacy audits from Ireland, Canada, Australia and New Zealand. Privacy audits from all of these other jurisdictions have examined, at a minimum, the privacy laws applicable in the particular country where an organisation is based. The audit standards used in the Google audit are explicable due to the genesis of this audit being in the requirements of the FTC that Google should comply with its public statements regarding privacy. As the FTC uses laws regarding unfair or deceptive acts³² to enforce its requirements, and as these are not technically privacy laws, the independent auditors of Google saw no reason to examine compliance with privacy laws. Nevertheless, as Google operates internationally, it should be seen as important for it to comply with the requirements of international best practice.

³² Federal Trade Commission Act, s5 (US).

2.9: CONCLUSION

The literature review shows that there are few studies that have directly examined the practice of privacy auditing. The wider privacy governance literature does refer obliquely to privacy auditing however. This thesis uses some research methodologies that have not been used in previous studies of privacy auditing. Some of these are drawn from methodologies used to study other forms of non-financial auditing such as sustainability auditing. However, privacy auditing also requires some legal analysis of possible standards that could be used by different auditors. Therefore this study has a number of novel aspects.

Some jurisdictions have produced privacy audits implementing standards that diverge significantly from those in other jurisdictions. Privacy audits conducted under the mandatory audit powers in Australia have produced audits with a low level of international comparability. In Ireland, the audits of Facebook Ireland Ltd also demonstrate a focus on the legal regime of just one jurisdiction. However, the Canadian Privacy Commissioner has made some moves toward the use of international best practice. There is therefore a gulf between the practices of some privacy auditors when compared across different jurisdictions.

CHAPTER 3: THEORETICAL BASIS

Alan Toy

3.1: INTRODUCTION

The purpose of this chapter is to describe the epistemological foundation of the research conducted for this thesis. The philosophical perspective of the thesis is Critical Theory.³³ The use of Critical Theory means that this thesis departs from what may be considered “[m]ainstream accounting research” (Chua 1986, 610). The importance of Critical Theory for this thesis is that it has a transformative aspect: In this case, the enhancement of privacy auditing theory. The concern is that privacy auditing has not yet achieved a level of rigour that will enable it to be seen as useful and integral to the operation of organizations. Society is changing, and our conception of privacy is changing, but the law is not changing fast enough. Some privacy auditors, especially those that are regulators, are focused on the standards contained in national legislation. Other privacy auditors, such as the Big Four professional services firms are using standards in their privacy audits that are more modern than those contained in national privacy laws. This thesis investigates whether all privacy audits would be improved by the use of more modern standards. Privacy auditing, generally speaking, should use more consistent, more modern standards. This is why Critical Theory is an essential perspective for this research: positivist research about privacy auditing would not have an emphasis on change and would instead focus on what the practice of privacy auditing

³³ Critical Theory developed at least in part in Frankfurt in the 1930s (Alvesson and Willmott 2003, 2). It has motivations that include emancipation and freedom of human beings in the “struggle for the future” (Turner 2006). It has been suggested that “[t]hrough self-reflection one is freed from past constraints (such as dominant ideology and traditional disciplinary boundaries) and thus critical theory is emancipatory” (Gaffikin 2008, 151).

has involved up to this point. However, the most interesting questions about privacy auditing relate to its future, not to its past.

3.2: CRITICAL THEORY

The perspective of this thesis in terms of its worldview is a critical one. It has been suggested that “[o]ne crucial contribution of the critical project (however we define ‘critical’) has been to help scholars learn to expose the implicit contours of their worldviews” (Gray and Milne 2015, 6). The critical perspective challenges the basis of the current practice of privacy auditing with the aim of suggesting potential future solutions to any problems identified.

It has been argued that “steering media such as accounting and the law do not have a fixed position in the lifeworld-system complex and may be increasingly subsumed and internalized within systemic imperatives” (Power, Laughlin and Cooper 2003, 142). The lifeworld is a conception of everyday experience, while the system concept refers to functional areas such as the economy as a whole. In accordance with this argument, the basis of this thesis is that social imperatives may influence the actions of privacy auditors and that this may influence later changes in the law to accord with modern practice. Especially in the area of information privacy law, where it is difficult for legislators to predict the types of data flows that will occur in the future, the law may need significant guidance from social norms and ideals regarding the information privacy rights of citizens. Privacy audits are an ideal mechanism for the recognition and propagation of practices that are consistent with these social norms and ideals.

Postmodernism may also have relevance to privacy audits. Postmodernism emphasises the relationship between power and knowledge, especially in relation to information technology (Clegg 2006, 256). This school of thought has been used in the Information Systems literature to expound the concept of Gaze (Young et al 2012, 498)

which may be, through “systems of surveillance” (Foucault 1983, 223), a way of exercising power in society. Gaze is a technique to control those gazed upon by influencing them to self-police. This is done by imposing the threat of observation (even though not every individual will be actually observed). The concept of Gaze has analogies with the basis of information privacy rights in a legal sense, because autonomy and liberty may be restricted merely by the threat of the Gaze.

There are some important differences between Postmodernism and Critical Theory which demonstrate that the latter is the more appropriate perspective for this thesis. Critical Theory ultimately aims to suggest improvements to a practice such as privacy auditing. These suggestions are central to this thesis. Postmodernism does not share this ambition, and may suspect that any new form of consensus may cause new elites to arise and new illusions to be created (Clegg 2006, 273).

There is a distinction drawn between deductive reasoning and inductive reasoning. Deductive reasoning is appropriate once a major premise has been established, and it is then applied to a particular situation. On the other hand, inductive reasoning is appropriate where there are case examples, and a major premise must be developed from the specific scenarios. Lawyers use both deductive and inductive reasoning in legal analysis (Farrar 2010, 91-92). This thesis uses primarily inductive reasoning to develop a theory of privacy auditing, drawing on sources such as interviews and documents to assist with the exposition. The interviews and documents serve as particular examples of the practice of privacy auditing, and from these examples a theory is developed.

3.3: JURISPRUDENCE

As will be discussed in the next chapter, this thesis also uses legal theories to provide an enhanced basis for examination of the research questions which include the standards used

for information privacy laws in the countries that are investigated. This discussion would be incomplete without an examination of the impact of Jurisprudence (the study of the philosophy of law). While much legal research is highly content specific, focusing on expertise in one or more narrow areas of law, jurisprudence is a not uncommon angle of enquiry in law journals. In regard to less settled areas of the law, jurisprudence is most relevant because it is in these areas that more thought must be given to the correct basis for legal reasoning and thought. Jurisprudence is very relevant to the area of information privacy because it is a new and unsettled field (for example, in *Google Spain SL v AEPD*³⁴, the European Court of Justice decided that Google must remove links in its website to some personal information of European citizens, a decision that caused an important and immediate change in the way that Google operates). Privacy is, in fact, used as a primary example in support of the jurisprudential arguments of Dworkin (Dworkin 1977, 119). Dworkin has many critics, including Hart and Raz. These critics are proponents of legal positivism, a primary tenet of which is the idea that law can be identified only by its sources, and that it need not contain any moral considerations to be classified as law. Raz's theory is antithetical to the main argument in this thesis, and therefore the aspects of it that are relevant here must be met with counter arguments.

A primary line of enquiry in this thesis proceeds in the direction of identifying fundamental principles which may be balanced against each other and against other principles, in order to assess which forms a reason that can amount to 'law' in a particular case. In order to achieve this balancing of interests against each other, each principle must have a dimension of 'weight' to assess its impact. This idea is central to the fundamental principles because of the international dimension. In each country which is examined in this

³⁴ Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González (2014) European Court of Justice, 13 May 2014.

thesis, such principles may have a different ‘weight’ that demands a different outcome when balanced against other interests. The principles may be balanced against each other and also against other values in society. For example, in the United States, the principle of Freedom of Speech is of very great importance (Toy 2010, 227). In Europe, by contrast, this principle has less importance relative to privacy. A logical outcome may be seen in the area of consent to infringements of privacy, where the US is prepared to sanction some uses of personal data in the absence of consent, while the EU is more cautious about this. The FTC suggests the principle of Simplified Consumer Choice (FTC 2012) which states that consent is not required for some dealings with data of citizens. By contrast, the European Commission does not recognise the same exceptions, although some permissions may exist (European Commission 2012, art 6(1)(b),(f)). In this way, the fundamental principles may apply across different countries each of which may have different cultures. They do not cease to be valid principles simply because the culture in different countries may require a different balancing of interests there.

Legal positivists, such as Raz, have strongly criticised this position. Raz argues that: “Those accustomed to ‘balancing’ talk may think that the existence of a (morally) legitimate law establishing a duty to perform a certain action is a reason for it, to be added to other reasons for that action and balanced against whatever reasons there are against it. That is a very misleading and wrong-headed view” (Raz 2009, 7). Legal positivism cannot refer back to morally legitimate reasons for laws. It can only refer to the pedigree (sources) of laws as legitimate reasons for action (Hart 2012, 100). However, legal positivism appears to buck the trend of legal reasoning by judges in both the EU and the US. In both of those jurisdictions, balancing talk is bound into the reasons for decisions in information privacy cases.³⁵ Legal

³⁵ Please see Chapter 5 for a detailed discussion of balancing information privacy rights in the EU. The practice of balancing information privacy rights against other rights is less developed in the US but it is present such as in *Riley v California* 134 S. Ct. 2473 (2014) where the Supreme Court held that privacy interests must be balanced against law enforcement interests.

positivism appears to therefore be out of touch with the reality of judicial decision making and as such cannot be a proper approach to the philosophy of law, at least where information privacy is concerned.

Another point of distinction between legal positivism and other theories concerns what may be termed the parochial argument. This is the argument that the Law as Integrity theory of Dworkin only applies to Anglo-American legal systems and is incapable of recognising other systems as legal systems. This is because societies that do not have a concept of law cannot have law under that theory. Raz uses the example of Jewish religious rules and practices which “did, at an earlier stage of their development, govern the life of independent Jewish communities... [b]ut the concept of law is not part of the Jewish religion, and where such communities existed in the past they often existed in societies whose members did not possess the concept of law... [y]et beyond doubt theocratic Jewish communities did have a legal system...” (Raz 2009, 40). However, this conclusion is not as obvious as Raz makes it appear to be. If a society chooses to be governed by religious practices rather than law, then why should it be taken to have a legal system? If it is impossible to distinguish a legal system from religious practices, then there does not seem to be any reason to insist that it exists. It may be that a theocratic Jewish community is one that chooses to be governed by something other than law. The concept of law is therefore necessary for a society to be governed by law. If people in the society do not think of themselves as being governed by law, as a separate concept from religion, then it does not make sense to think of the society as having law, because it would be superfluous.

One of the most common arguments deployed in favour of legal positivism is that it is content independent. This means that a law can have any content, even a content that seems ‘evil’. Raz argues that: “No general theory of law can hope to succeed unless it is content-independent to some extent” (Raz 2009, 78). However, Dworkin’s theory is content-

dependent because it depends on moral values such as justice and integrity. The difference can be illustrated by an example. Through deliberate intention, or merely a mistake or oversight, the legislature passes a law in full compliance with the law-making machinery of the society. This is a law that compels all persons within a society to immediately kill at least one other member of that society. Raz's theory would treat this as a valid law, but Dworkin's theory would not because this 'law' is not in compliance with morality, it does not have integrity. The majority of people in society would probably believe that Dworkin's theory is correct. It is apparent that the law must be content-dependent and therefore, contrary to Raz's argument above, no theory of law that is content-independent will be successful, except in a society in which every single law is already in compliance with Dworkin's theory. Raz's theory therefore adds nothing to the explanation of the concept of law. Law-making authorities exist under Dworkin's theory, but they are constrained in their ability to make law. This is in accordance with what ordinary people would probably believe; that the elected representatives must act in a morally sound way.

Dworkin's Law as Integrity theory is complex in what it treats as integrity or morality. The complexity springs from the fact that different people have different ideas as to what morality consists of. For example, a person committed to the Jewish religion may have a very different idea of morality than that of a person committed to Buddhism. But it is not the morality of any individual in society that Dworkin has in mind, including individual judges. Dworkin sees morality as being a view of society as a whole, and his "theory identifies a particular conception of community morality as decisive of legal issues" (Dworkin 1977, 126). What would society as a whole regard as a moral thing to do in any particular instance? This is difficult to classify, but it is possible to ascertain it in individual situations, hence the possibility of a judge applying it to determine what the law is in a particular case. Judges interpret the law made by the legislature, and may exercise law-

making functions in individual cases. In conducting both of these exercises, they are guided by the morality of society as a whole (not their own individual morality). For example, a judge who also happens to be committed to the Jewish religion would apply the morality of society as a whole in making his decisions, not that of the Jewish religion. In this way, it is possible for individuals in society to disagree on morality, yet by living in the one society, they are implicitly agreeing to be bound by the law of that society as referenced to the morality of that society as a whole.

Of course, judges may not see themselves as applying morality when they decide a case. This is another criticism that Raz levels against Dworkin's theory: That "Judicial decisions in American Courts are vulnerable to the charge that they are wrong as a matter of American law. But it is irrelevant to their justification that they conform... with the correct theory of the nature of law" (Raz 2009, 84). Judges may make mistakes when deciding cases, although there are legal doctrines such as *per incuriam*³⁶ which operate to mitigate such errors. When judges decide cases, even though they may not refer to the morality of society as a whole explicitly, they may be taken as impliedly referencing it whenever they must impose a rule in a case, because every rule of law has moral reasons for being. This is what is truly meant by Dworkin's conception of community morality. Even a rule as to which side of the road to drive on has moral reasons for existence (such as the avoidance of accidents) and these moral reasons may be different in different countries (because historically people have become used to driving on that side of the road, or perhaps because most cars in the country have been configured for optimal driving on one particular side). Hart appeared to have not considered this when he stated that: "It does not matter which side of the road is prescribed by the rule of the road" (Hart 2012, 134). Raz's criticism may be shown to be incorrect because the correct theory of the nature of law and the correctness of a legal decision are

³⁶ Literally: without care.

more closely linked than he suggests. While a concept of law and a theory of law are not the same thing, the correct legal reasoning in a case must be consistent with Dworkin's theory of the law (either expressly or implicitly), or it will not be a correct decision. A judge may not expressly indicate in a judgment why their decision is consistent with the theory of law, but this does not necessarily mean that their decision is inconsistent with it.

Although they are necessarily linked in his theory, Dworkin still sees distinctions between law and morality, and between law and justice. He states the abstract idea that "legal rights are those flowing from past political decisions according to the best interpretation of what this means" (Dworkin 1986, 96). He therefore attempts to distance himself from the idea that law is a blueprint of morality. While this argument is correct in its aims, there may be a less complicated way to justify the distinction. Community morality is constantly changing. This can be seen in the change in values over time relating to bankruptcy, which used to cause the bankrupt to become a slave, then softened to a merely criminal offence, then further softened to mere civil penalties, and now appears to have softened even more to the point where facts entailing bankruptcy may no longer in fact result in it.³⁷

Changes to community morality occur before changes to the law, and changes to the law may be very slow to respond to this. Law is created by humans with limited resources, both legislative and judicial. These resources can do their best, but cannot be entirely up to date with the community's conception of morality. This may have the result that the law is not always consistent with community morality. Judges asked to interpret such a law may give it the most up to date interpretation that they can, taking into account modern changes in community morality, so far as this is possible. They may apply principles according to the correct weight they would be given under the current community morality. These principles

³⁷ An example is the "No Assets Procedure" under sections 361-377B of the Insolvency Act 2006 (NZ). This allows an alternative to bankruptcy for persons who meet certain criteria, and does not entail some of the consequences of bankruptcy.

may be reflected to a greater or lesser extent in the wording of a statute. The closer the wording of a statute comes to these principles, the easier it will be for citizens in society to adjust their conduct in accordance with the law.

This argument regarding changes in community morality is central to the research in this thesis. In selecting the standards to be used in a privacy audit, an auditor may need to make a decision to use either the information privacy laws in place in a particular country or the latest developments in international thought regarding best practice in information privacy. These may be found in documents containing proposals for legislative and/or policy reform regarding information privacy. The conception of community morality includes these documents as indicators of what society as a whole regards as the latest developments regarding information privacy rights. The latest developments may not yet be reflected in legislation or case law. This will be likely to be the situation in many countries because information privacy laws take much time to enact and to change, but their subject matter is greatly affected by rapid changes in technology.

Examples of the speed at which legislation in this area changes may be seen in New Zealand's review of its privacy law. The New Zealand Law Commission began this review in October 2006 and completed it in July 2011. The author was consulted by the New Zealand Law Commission at a round table meeting in 2010, and academic articles published by the author were cited at various stages of the review (New Zealand Law Commission 2011, 148, 274, 281; New Zealand Law Commission 2010, 138, 350, 353). However, the recommendations made have not yet been adopted in legislation by the New Zealand Government. Also, the United States has been toying with the idea of federal privacy legislation to cover consumers generally for some time now. The White House (2012; 2015) has introduced a draft Consumer Privacy Bill of Rights in both 2012 and 2015. Both of these bills demonstrate the same 7 privacy principles, at least 4 of which are adopted as

fundamental principles in this thesis (Transparency, Control, Respect for Context, Accountability) in addition to the idea of industry codes of conduct which is also adopted by this thesis. Prior to that however, other consumer privacy bills have been proposed in the US, the most notable of which is the bi-partisan Commercial Privacy Bill of Rights proposed by Senators Kerry and McCain from opposing political parties (McCain 2011) which contained different principles of information privacy compared to the White House proposals. However the US has not yet adopted any of these proposals in legislation. Information Privacy may therefore be seen as a primary example of an area in which community morality is changing quickly and there is a fissure between what has been enacted in the past and what community morality has evolved into. Privacy audits may bridge this fissure. Accountable organizations should have a process of continuous review of their accountability mechanisms, including privacy auditing (The Centre for Information Policy Leadership 2011, 7).

Privacy auditors may take Dworkin's theory as a way to apply the best interpretation of the latest developments in community morality regarding information privacy as standards in privacy audits. On the other hand, if a privacy auditor takes a positivist view of the law, then it may be difficult for such an auditor to apply the latest developments, and the danger exists that they may apply laws that do not reflect current morality unless they are interpreted in line with Dworkin's theory which is an interpretation that a positivist would not use. A privacy auditor that embraces legal positivism may decide that the information privacy laws in a particular country should be used in privacy audits there. They may overlay other standards on top of this however (as suggested in part 3.3 of chapter 6), negating the divergence between legal positivism and Dworkin's theory. These other standards would include the latest developments in information privacy best practice. The auditor may apply such standards out of regard for international best practice. There may remain concerns for those auditors who have statutory audit powers, where these state that they must apply the

information privacy laws of their country in a privacy audit. These concerns will be discussed in more detail in chapter 6. To apply standards that go beyond the criteria in their empowering statutes may be seen as going beyond their powers. However, Dworkin's theory allows the latest developments to be taken into account when interpreting the principles of information privacy and it is therefore a superior theory to that of legal positivism where information privacy is concerned.

Legal positivism then does not provide enough certainty in unsettled areas of the law. Arguments from cases in other countries that are not legally binding are relevant to such unsettled areas and therefore legal positivism cannot explain how the law is actually made. The ability of a judge to sense the morality of society as a whole and apply it in a particular case may not be perfect. There will always be cases that are not in perfect compliance with Dworkin's theory of law. But judges are very good at what they do, and they are selected because of their ability to judge in a way that most people would regard as 'right', and most people would refer back to morality of society as a whole when they argue about whether a judge has got it 'right' or not. This is so even if they happen to be members of religious groups whose morality differs from what most people in society would regard as 'right'. Raz criticises this as well. He claims that Dworkin's philosophy "contains a theory of adjudication rather than a theory of (the nature of) law" (Raz 2009, 87). But, with respect, Raz is incorrect because Dworkin's philosophy includes "two principles of political integrity: a legislative principle, which asks lawmakers to try to make the total set of laws morally coherent, and an adjudicative principle, which instructs that the law be seen as coherent in that way, so far as possible" (Dworkin 1986, 176; Dworkin 1977, 105-109), and provides some limits (for example, an 'evil' law validly passed by the legislature would not be considered a law in the usual sense). Hart argues that not all cases will be covered by a specific rule and in such cases "judgments of what is 'reasonable' can be used by the law" (Hart 2012, 132). But this

actually supports Dworkin's theory more than legal positivism because what is reasonable is decided by a judge taking into account the morality of society. Reasonableness cannot be decided without reference points.

3.4: CONCLUSION

Critical Theory provides a lens through which the practice of privacy auditing may be viewed. It allows a study of privacy auditing to emphasise areas in which the practice may have room for improvement. It is suggested that privacy audits may be improved by the use of standards that come closer to harmonization (Toy 2013). This would have the additional benefit that the standards could be updated to more modern criteria than are currently contained within national information privacy laws. Jurisprudential theories supplement the theory of privacy auditing that is developed in this thesis. The theory of privacy auditing that is developed in this thesis goes beyond the current observed state of practice to suggest improvements to the practice of privacy auditing that may enable the practice to be strengthened.

As stated in section 2.2.1, there is a possibility that citizens may ignore laws that are inconsistent with prevailing social norms. This is consistent with Dworkin's theory and this demonstrates that anti-positivist perspectives are present in the disciplines of accounting and law. Critical Theory therefore provides a theoretical perspective that can inform the approach taken to the research in this thesis from the point of view of all of the research methods used in this thesis. Furthermore, Critical Theory provides the opportunity to suggest improvements to the practice of privacy auditing. As will be seen from the results of the interviews, privacy auditing is not yet fully developed and therefore there are limited benefits from a traditional positivist analysis of privacy auditing.

As the literature review demonstrates, there are very few direct studies of privacy auditing and the process of privacy auditing has not yet developed to the point where any particular process can be said to represent a typical privacy audit. The research in chapter 7 of this thesis is the first academic research to use semi-structured interviews to investigate the process of privacy auditing directly. It demonstrates challenges to the practice of privacy auditing and the argument in this thesis is that these challenges may be addressed by fundamental principles for privacy auditing. This is the essence of the critical theory that this thesis employs: suggestions for change in practice, and for change in the theory of the practice of privacy auditing.

CHAPTER 4: DATA AND APPROACH TO ANALYSIS

Alan Toy

4.1: INTRODUCTION

This chapter identifies the selected methods for conducting the research. The research questions require an investigation of the practices of privacy auditors and an analysis of legal standards in information privacy laws. In accordance with this, the research methods used include a case study qualitative research method as well as documentary analysis and legal analysis. The convergence of these methods produces a study of privacy auditing that is founded on theories of auditing as well as jurisprudential theories. The use of legal research is an essential supplement to the auditing theory regarding privacy audits because many privacy audits rest solely on information privacy laws as a set of standards for the audit. However, the theory of privacy auditing developed in this thesis is more nuanced than information privacy laws. The research questions include an examination of auditing standards and methodologies used for privacy audits. These are not specified in privacy laws in sufficient detail to give guidance to a privacy auditor. An approach that uses only legal analysis would not therefore be capable of properly investigating the research questions in this thesis.

4.2: MULTIPLE RESEARCH METHODS

This chapter details the reasons for the choice of methodology. A case study qualitative research method is adopted, following a broad definition of this type of research: “Case study research in business uses empirical evidence from one or more organizations where an attempt is made to study the subject matter in context. Multiple sources of evidence are used,

although most of the evidence comes from interviews and documents.” (Myers 2013, 78). Consistently with the chosen method, this thesis does not use participant observation or fieldwork, which would be more appropriate to Ethnography (Myers 2013, 79). A number of semi-structured interviews are carried out to collect data from individuals. The interview data is reviewed using thematic analysis to identify themes that form the building blocks of a theory of privacy auditing. The research questions are answered by this because the theory of privacy auditing developed includes the standards and/or methodologies that are used for privacy audits and the issue of who benefits from privacy audits and the appropriateness of the benefits.

In addition to the interviews, documentary analysis is undertaken. This is essential for examination of the research questions because the standards used by privacy auditors are demonstrated in privacy audit reports. The documentary analysis examines publicly available documents such as privacy audit reports and audit guidelines, and cases and other resources available from databases and the websites of privacy regulatory authorities. The qualitative research in this thesis is necessary for the study of privacy audits, but legal research is also necessary to supplement it. This is because the legal basis of information privacy rights has not reached the point where it can be regarded as settled. Due to the tendency of some privacy audit reports to focus on the requirements of information privacy laws, it is important to examine the basis of these laws to determine if they have any common elements. This research includes analysis of congruence or dissonance between standards used in privacy audit reports, and an understanding of the legal basis used for some privacy auditing standards is a crucial element in this thesis. The combination of qualitative and legal research improves the validity of this study.

Legal research is therefore also used to investigate the research questions. The latest policy suggestions regarding information privacy demonstrate modern principles that could

be used in privacy audits. The legal research used in this thesis examines information privacy law and determines the impact that it may have on the practice of privacy auditing. This method of analysis involves assessment of the latest cases and legislation in the context of the relevant policy framework. Information privacy law is still in the process of responding to the challenges presented by Big Data and the rise of technologies such as online social networking. The development of privacy audits must take account of the legal framework. However, privacy audits may incorporate best practice that is not embodied in legal form. In this way, they may themselves be examples and sources of best practice. While information privacy laws may take some time to be able to fully protect privacy of personal information, the practice of privacy auditing may develop best practices that could eventually be adopted in national privacy legislation.

4.3: RESEARCH DESIGN

This section describes the methods for investigation of the research questions and further supports the choice of research methods. The first research method used in this thesis is a qualitative research approach using interviews to investigate the research questions. This research method is the basis of chapter 7. Qualitative research allows the perspectives of people involved with privacy audits to be uncovered and analysed and is appropriate to this thesis because this research is in a new and developing field. The richness of the data obtained from the interviews assists with the investigation of the research questions because it allows the standards and methodologies used in privacy audits to be uncovered and analysed, along with issues regarding the beneficiaries of privacy audits.

In addition to investigation of the research questions, the research also tests the application within privacy audits of the framework of fundamental privacy principles that are developed in chapter 5 (Toy 2013). The research is assisted by the approach taken because

the in-depth data obtained from the interviews is in a form appropriate for analysis of the principles used as standards within privacy audits.

Geographical limitations have the effect that no one from Europe could be found for the study, so there are no interviewees from Ireland. Cases from the US and the EU are important because these are two of the most dominant forms of information privacy/data protection regulation worldwide, especially among the countries that are part of the study. It has been claimed that the US and the EU vie for supremacy in the regulation of information privacy/data protection, with one commentator going so far as to claim that “Europe is the winner” (Bygrave 2014, 208). However, this thesis argues that it is important to find a middle ground between the two systems as together they provide the most up to date principles that are relevant to the study.

There are several methods of collection of the information:

- a. Analysing information including privacy audit reports and privacy policies. The author reviews these, and any other privacy related documents that organisations provide. The author analyses:
 - 1) Privacy audit reports and privacy policies which are available on databases and publicly available websites such as the Canadian Privacy Commissioner’s website.
 - 2) Cases, legislation and other authorities that are available on databases.
 - 3) Documents recommending policy and/or legislative reform regarding information privacy.
- b. Semi structured interviews with:
 - 1) Privacy Commissioners / Information Commissioners (and/or staff).
 - 2) Staff from other organisations such as the “Big Four” audit firms.

4.4: DATA COLLECTION

Six semi-structured interviews take place with seven interviewees (one interview has two interviewees). Interviews were sought from people involved with privacy audits. These included regulators and members of audit firms. The author identified some potential participants at an APEC privacy enforcement workshop that was held in July 2013 in Auckland. Potential participants were later invited by email to take part in the study. This was necessary because some of the participants were from outside Auckland or from outside New Zealand. Interviewees include regulators from Canada and New Zealand, and members of private organizations from New Zealand, the United States and Australia.³⁸

Contact with the interviewees was established through meeting them at privacy workshops and seminars in 2013. The interviewees were selected due to their relationship to privacy audits. Some had actually conducted privacy audits, others were regulators in the area of information privacy, and others were more incidentally related to privacy audit issues (such as analysts). For example, Marty Abrams is the Executive Director of the Information Accountability Foundation in the United States. This organization does not engage in privacy audits, but the Executive Director does have an understanding of the issues involved with such audits and he therefore fulfils the role of an analyst in this area. Subsequent contact with interviewees was conducted through email, at which time the participant information sheets and consent forms were distributed to the interviewees. All of the interviewees and the relevant organizations signed the consent forms. The interviews have been conducted via telephone to The United States, Canada, Australia, and Wellington (NZ). Interviews in person at the offices of the New Zealand Privacy Commissioner (Auckland office and Wellington office) also took place. The interviewees are senior members of the current community of

³⁸ A number of other potential interviewees were approached, but they declined to participate. This is a limitation of the study. However, the calibre and experience of the interviewees that agreed to participate in the study compensate for this to some degree because they provide a wide range of viewpoints about the subject matter of the research.

privacy regulators, auditors and analysts. This is of benefit to the research in this these because it allows rich insight into privacy auditing issues.

A set of open-ended questions is devised for the interviews. Given the lack of a previous interview based study of privacy audits, these are developed from scratch. The literature review identified a lack of published information about standards and methodologies used in privacy audits, and so the interview questions focused on these issues. There are 17 interview questions in the list, which cover (in addition to housekeeping issues regarding the interview itself): The nature of privacy audit services provided by the organization and the role of the interviewee in relation to those services; Standards used for privacy audits and challenges to the creation of such standards; Methodologies used for privacy audits and challenges to the creation of such methodologies; Factors used to improve privacy audit quality and the effectiveness of these factors; The issue of who benefits from a privacy audit; And updates to any legal requirements in the particular country which may impact on the standards and methodologies used in privacy audits. The interviews are semi-structured, so additional questions are sometimes asked in order to further investigate issues in the interviews. The interviews take place from September to November in 2013. During the interviews, the themes are explored in such a way that emerging issues could be covered, with reasonable flexibility in the ability to pursue these (so long as they are relevant to the research goals). Issues are explored in a different sequence that varies among different interviews. This is because the course of the conversation in different interviews makes it appropriate to examine some issues before others.

The dramaturgical model has been suggested as a conceptual framework for qualitative interviews (Myers and Newman 2007, 12). The interview is thought of as a drama, with actors, script, entry and exit. Under this model, the quality of the interview varies as does the quality of any performance. A higher quality interview will be one that discloses

more important information, increasing the quality of the data. It is therefore important to use correct technique in interviews, which includes giving the interviewee enough room to express themselves clearly. The amount of talking done by the interviewer needs to be carefully constrained, and appropriate empathy must be demonstrated. This model is kept in mind by the author during the interviews, and the author endeavours to produce an interview performance of high quality.

Seven people are interviewed. A schedule of the interviewees is contained in Table 1 at the end of this thesis. The total combined interview time is 6 hours, 35 minutes, 43 seconds. Each interview is a separate event, except for the combined interview of Tanya Allen and Jay Fedorak. Each interviewee is interviewed once, with the exception of Neil Sanson, who is interviewed twice. All interviews involved exactly two people (the author and the interviewee), except for the combined interview of Tanya Allen and Jay Fedorak which involves three people.

The interviews are recorded using a digital audio recorder. After the interview, this recording is transferred to a secure computer and the original recording is then deleted. Notes are made during the interviews to facilitate further questions within the interview itself and to facilitate later reflection on the issues raised in each interview. Analysis of these notes assists with analysis of the themes in the interviews. The author did not contract out the transcription process since it was thought that transcription by the author would allow a closer and more in-depth understanding of the data. The transcription process was completed in early 2014.

A number of different approaches to transcription have been suggested, including the continuum between naturalism and denaturalism (Davidson 2009, 39). Naturalised transcription includes “as much detail as possible” (Oliver et al 2005, 1275) whereas denaturalized transcription removes certain elements. The approach taken for the interview transcription in this thesis is chosen to provide the best possible data necessary for analysis of

the themes in the interview transcripts. Incomplete vocalizations are not transcribed, because the author is unsure what to transcribe in the case of a word that does not fully emerge. Any “ums” and “ahs” were also not transcribed, as they merely fill gaps in the speech, and do not add anything to the transcripts from which themes could be extracted. However, apart from this, all other spoken words are transcribed with as much accuracy as possible. This includes phrases such as “you know” because this may have some meaning or influence on the other spoken words. Commas and full stops (periods) are included in the transcription, but only if this is the best possible interpretation of the manner in which the interviewee has spoken. Grammar is not corrected in the interview transcripts. This was because the aim is to capture what the interviewees say, without imposing editing.

Some approaches to transcription, especially in studies that use Conversation Analysis (where the study of human language itself is important), include transcription of pauses, in-breaths and out-breaths, emphases and sharp cut-offs. However, this is not necessary for this thesis because the themes that emerge from the interview data do not require that level of detail, nor is discovery of the themes assisted by transcription of such occurrences. The use of non-verbal communication (such as gesticulation) is not relevant to this thesis, and it is not recorded or transcribed. It is not possible for the author to capture this, given that many of the interviews are over the phone to different countries (the interviewees rejected skype in favour of ordinary phone calls), and this research project neither requires nor allows the recording of such non-verbal communication.

The method of transcription appropriate for this thesis sits close to the denaturalism end of the spectrum because this “has less to do with depicting accents or involuntary vocalization” (Oliver et al 2005, 1277). Denaturalism attempts to present interview transcripts that are as accurate as possible, but it does not require the level of detail that is part of naturalism, and which would be unnecessary in the context of this study (Kvale 2007,

94-96). Within these limits, the method of transcription is chosen to provide the greatest possible accuracy of interview transcripts, and is appropriate for this topic because it allows the research questions to be examined without any “noise” in the transcriptions that may arise from unnecessary detail.

Accuracy is ensured by careful transcription, followed by listening to the recording a second time to check the accuracy of what has been transcribed. Furthermore, the interview transcripts are sent to the interviewees to ensure that they were accurate. Some of the transcripts therefore evolved after the interviewees clarified them (in some cases this is unclear from the recording itself, and in these instances square brackets are used to indicate the best interpretation by the author of what is said).

4.5: DATA ANALYSIS

Data from interviews is analysed using techniques such as conclusion drawing/verification and data reduction (O’Dwyer 2004). These processes go hand in hand and are used to reduce the bulk of the data corpus to a usable format. A process of reading and coding the interview transcripts is undertaken in order to identify themes in the data. Thematic analysis is used in this thesis. This is a standard qualitative technique for analysis of interview data (O’Dwyer 2011, 1239). It is appropriate to this thesis because it allows the research questions to be examined by drawing out the themes from the interview data to investigate the standards and methodologies used in privacy audits as well as the question of who benefits from privacy audits and the appropriateness of the benefits.

A “thick description” of the data is used to verify the themes. This involves sorting the extracts from the interview data into groups of similar ideas to present a description of the data prior to the application of any theories. Notes and rough diagrams are made during the interviews, and the author reflects on these when analysing the themes in the interview

transcript data. The themes from the interview data are compared with the documentary analysis to verify the themes. The comparison of interviews with documentary analysis is a useful qualitative technique (Radcliffe 1999, 344; Free 2009, 125).

It is difficult to identify themes in qualitative research without some rationalization of the data corpus because the interview transcripts will typically present a very large volume of data which will require time intensive analysis. In the case of this thesis, the transcripts of the interviews, when broken down through the process of allocation to the initial codes, come to around 40,000 words. When the data is analysed to identify the themes, it is possible to reduce this to around 20,000 words. Some of the interview data is able to be eliminated after this process because it merely duplicates ideas that are developed in greater detail in other parts of the data.

4.6: ETHICS APPROVAL

The interviews are with named participants. It is considered ethically sound to seek attributable interviews. The participants are asked for permission to use their names along with their statements. The decision is made not to seek non-attributable interviews from regulators and members of audit firms. This decision is made because in each country there are very few regulators and very few private audit firms involved with privacy audits. If the decision had been to seek non-attributable interviews, this would have limited the discussion of the results because particular countries would then not be able to be referred to. For example, any discussion of an approach taken by a regulator in New Zealand would be likely to identify that regulator, because the class is very small. It is therefore not possible to avoid identification of participants, even if non-attributable interviews are sought. Furthermore, interviews with anonymous participants may have raised secondary identification problems, where interviewees may have accidentally provided enough information in the interview to

be able to identify them or their organizations, and these portions of the interview transcripts would then be unable to be used. Attributable interviews avoid this problem, ensuring that all of the interview data is usable without masking any part of it from final reports about the research.

Ethics approval is granted by the University of Auckland. The interviewees are sent the ethics consent forms by email in advance of the interviews, and all give consent to use their names and the names of their organisations in reports about the research. Each interview is recorded, in accordance with the ethics documents.

4.7: DOCUMENTARY ANALYSIS

In addition to the interviews, the qualitative research in this thesis also uses documentary analysis. This research is the basis of chapters 5 and 6. Documents from five countries are part of this research: The United States, Canada, Ireland, Australia and New Zealand. The research is limited to these countries because they demonstrate some well publicised privacy audits, and due to language barriers the privacy audits of some other countries are not accessible to the author. A further factor limiting the choice of countries is that the contacts available to the author come mainly from an APEC privacy enforcement workshop held in Auckland in July 2013, and this mainly contained delegates from pacific-rim countries. In future, it may be useful to extend the work in this thesis to other countries. For example, information privacy has become of interest in Greater China (Hong Kong, Macau, Taiwan and the People's Republic of China).³⁹

The documents used in the research include privacy audit reports. These are publicly available reports and are identified from the websites of regulatory authorities such as the

³⁹ For a useful database in both English and Chinese regarding comparison of information privacy statutes between these countries, please see: <http://chineseprivacy.law.hku.hk/> (site accessed on 28 January 2015).

Federal Trade Commission and privacy commissioners and from other websites such as that of the Electronic Privacy Information Center (EPIC).⁴⁰ These privacy audit reports are all the publicly available reports that could be identified from the countries in the study, covering the period from January 1, 2006 to January 1, 2013. The limitation of time begins in 2006 because there are few publicly available privacy audit reports before this date. The limitation of time ends in 2013 because the data was used as the basis of an article submitted to *Auditing: A Journal of Practice & Theory* in 2013 (which was later accepted for publication). No confidential reports are obtained, therefore it is not necessary to protect the identities of any organizations that are subjects of these privacy audits.

The audit reports are analysed through a process of coding where the standards used in each audit are identified and coded. These are compared with the fundamental principles of information privacy that are identified in this thesis. A comparison is made between the standards used in each audit and the fundamental principles. As the fundamental principles are identified to be broad applications of information privacy, all known principles of information privacy should fit within them. This means that it is possible to assess which principles have not been applied in any particular privacy audit. Thirty privacy audit reports from the 5 countries in the study are identified and are analysed to assess their use of information privacy principles, and therefore their use of the fundamental principles of information privacy. Where the full breadth of a fundamental principle is not captured in the standards used in any particular audit, that fundamental principle is not considered used in the audit. While it would be possible to do a much more in-depth analysis of exactly which aspects of a fundamental principle were applied in each audit, this would not necessarily add much to the overall point of the research and would be beyond the scope of the present thesis.

⁴⁰ Available at: <https://epic.org/> (site accessed 28 January 2015).

There is also a more subtle analysis of fundamental principles of information privacy relating to other documents, apart from the privacy audit reports. These include reports proposing policy changes and legislative changes. The time period for identification of these documents is from January 1, 2006 to January 1, 2016. This time limitation is chosen to mirror the time period for identification of privacy audit reports, except that it is extended by an additional 3 years because further important developments occur during the course of the PhD thesis. The analysis of these reports is done by the author through a process of reading them to identify the themes relating to principles of information privacy. These themes are then compared with the themes from the other documents, to provide a list of information privacy principles. The principles are assessed for coverage of information privacy issues. Where a principle is merely a specific instance of a broader principle, the specific instance is not considered useful because its content is reflected in the broader principle. Each principle is put through this process which results in a list of seven fundamental principles that are distinct and not part of any other principle. This is a relatively straight forward process, but it is novel because such an exercise has not been attempted in the literature before.

The fundamental principles that result from the research are conceptualized to include all possible instances of specific applications that could fall within them. For example, where a data minimization principle is recognised, this is considered to be merely a specific instance of the broader principle of proportionality. Proportionality must be respected in the collection and holding of data, so that the minimum is collected and it is held for the shortest time necessary for the purpose for which it was collected. Collecting or holding data for longer than necessary would be disproportionate to the purpose of its collection. However, the principle of proportionality covers much more ground than this. It includes other aspects such as the weighing of privacy principles against each other or against other principles of the general law. If a right to freedom of speech is to be weighed against a principle of privacy,

privacy would only prevail if it is proportionate in the particular situation. Another example concerns security interests. To weigh security against privacy principles is relatively common. The President's Review Group on Intelligence and Communication Technologies (2013, 53) stated that "it is always challenging to strike the right balance between the often competing values of national security and individual liberty..." but this review also cautions that "[t]he purposes of surveillance must be legitimate. If they are not, no amount of 'balancing' can justify surveillance" (The President's Review Group on Intelligence and Communication Technologies 2013, 49). This confirms the main argument of this thesis, which is that fundamental principles exist and include the principle of Legitimacy (which has not been recognised elsewhere in policy documents in the US). While this review recommends that the principle of Legitimacy has a special importance, this is a concept that has not been fully developed in the US (the EU is ahead in terms of elucidating this principle), so it may not have a different quality from the other fundamental principles.

4.8: LEGAL RESEARCH

Legal research is also undertaken in this thesis. This research is the basis of chapter 5. To the author's knowledge, a definition of legal research beyond the basic skills has not so far been successfully elucidated in a way that has achieved acceptance (law PhDs generally do not have methods chapters, and books on legal research generally examine only the basic skills that are taught to undergraduate students). Therefore a novel explanation is attempted from the author's own knowledge and personal experience. In essence, legal research seeks to provide an innovative and correctly reasoned argument for or against a particular change in the law. Legal research may be considered normative because it aims to assess what should occur, rather than merely assessing what is already in existence (Farrar 2010, 10).

Correct legal reasoning requires an in-depth assessment of the arguments provided in cases or legislation as to why the law is a certain way, or why it should change. An argument that fails to take account of an important precedent in the form of a previous case or statutory provision is an unpersuasive argument and will be dismissed. Beyond this, the technique of building a persuasive argument is multifaceted and is central to law school instruction in legal systems that are historically based on that of the United Kingdom. Legal research may be thought of in a basic sense as being a skill that all law students must learn in order to ascertain what the law is on a particular issue. It is a central component of legal practice. There is therefore a strong link between legal research and legal practice.

These are merely expository skills, and the kind of research that is published in law journals goes beyond mere exposition to encompass novel arguments for or against legal ideals. Legal research typically allows novel issues to be examined in greater detail than would be possible in legal practice (However, legal practice involves many other issues in addition to pure legal research). One way to critique novel issues is through the lens of jurisprudence as outlined in part 3 of chapter 3. The depth of this type of enquiry goes beyond the analysis typically undertaken by lawyers in practice.

The author is responsible for trawling through the legal databases to find these precedents and other relevant authorities. A legal researcher often relies heavily on their own knowledge of the law, as gleaned from articles in law journals and from their own reading of the cases produced by courts in the world. It is not sufficient to consider cases merely from one's own country because arguments may arise in cases in other countries that are relevant to an issue that has not been fully elucidated yet. Although some areas of the law may be regarded as "settled", there is almost always room for further arguments in relation to a particular issue. This is especially so where the subject matter of a particular law changes

frequently. Information privacy is one such area. The technology that can affect information privacy rights is changing rapidly, and the law must try to keep up.

4.9: LEGAL RESEARCH IN THIS THESIS

The legal research undertaken in this thesis proceeds as follows: A construct or framework of fundamental principles is created to justify and “fit” the latest pronouncements of policy regarding information privacy rights. This framework is then tested against the information privacy laws in each of the five countries that are the subject of this thesis. From this, it is possible to see which countries have information privacy laws that differ from the latest policy developments in information privacy rights. Privacy laws are, in some cases, more than 20 years old. Although they have been amended, for the most part these amendments are minor and do not bring the law up to date with the latest developments.

The framework of fundamental principles is constructed in line with Dworkin’s theory (Dworkin 1977; 1986). It looks to the morality of society in the five countries that are the subject of this thesis to ascertain what principles are currently thought of as important for privacy protection. Privacy is a constantly evolving concept, not one that is fixed in time. The conception of privacy that our societies have will change as different challenges to privacy arise, most recently in the form of internet technologies. The concept of privacy does not ‘die’ merely because challenges have arisen. It does not fail merely because solutions to some of these challenges have not yet been fully elucidated. Legal positivism suggests that morality is a concept that cannot be easily changed, whereas the law is different because it can be changed (Hart 2012, 176). But this is to misrepresent to concept of law. Law may be seen as following changes in the morality of society, not leading it. Changes in technology that affect the imperatives behind information privacy law will take some time to flow through to the

law. This is because law making authorities have limited resources, so they cannot always be at the cutting edge of the legal needs of our society.

A guide to the morality of society as a whole may be seen in the recent policy statements regarding information privacy, combined with suggestions for legislative reform regarding information privacy rights (European Commission 2012; The White House 2015; Federal Trade Commission 2012). These are sources of arguments or justifications for what people expect regarding the principles and rules that should govern the privacy rights of citizens in society. They are written by official bodies that have been given the task of deciding what sensible rules should be in these areas. Even if judges do not refer to them explicitly, they are likely to be aware of the latest thinking in the area of information privacy rights, and may design their judgements to be consistent with it. This is particularly important in the privacy area because it remains a relatively unsettled area of the law which leaves much room for judges to provide guidance.

The approach to critical theory in this thesis influences the suggestions for a framework of fundamental principles. Due to the fast moving nature of information privacy issues, the law sometimes struggles to keep up with the latest developments in international suggestions regarding information privacy. Lawyers attempting to interpret legislation may use policy suggestions under a non-positivist approach to the law which allows them to ascertain the basis of information privacy rights. These rights may be seen as being founded in the fundamental principles. However, this is not a merely interpretive exercise. The fundamental principles are more sophisticated than the interpretation of the laws of just one country. They include the possibility for reconciliation of the approaches to information privacy taken in different countries. For example, the fundamental principles may be able to provide a consistent approach to information privacy in both the EU and the US.

4.10: CONCLUSION

The choice of research methods in this thesis allows the standards and methodologies used in privacy audits to be observed. The research methods include a case study qualitative research method as well as documentary analysis and legal analysis. These methods together provide a basis for the examination of the practice of privacy auditing that is stronger than any of these methods alone.

The qualitative research in this thesis uses interviews to investigate the standards and methodologies used in the practice of privacy auditing by different privacy auditors. It also allows the beneficiaries of privacy audits to be ascertained, along with the benefits of privacy audits to these people. Thematic analysis is used to extract the themes from the interview data. The legal research and documentary analysis supplements the qualitative research because it allows for analysis of the standards used in some privacy audits. The combination of these types of research is particularly appropriate to answering the research questions in this thesis.

CHAPTER 5: DIFFERENT PLANETS OR PARALLEL UNIVERSES: OLD AND NEW PARADIGMS FOR INFORMATION PRIVACY

Alan Toy⁴¹

ABSTRACT

The research questions require an analysis of the standards used by privacy auditors. Some privacy auditors use information privacy laws as standards for a privacy audit and therefore it is necessary for this thesis to be aware of information privacy laws in the five countries that are the subject of this thesis. This chapter considers information privacy rights in the context of increasing technological pressures. It argues that understanding of such rights is currently impeded by a lack of a consistent underlying theory, and by fragmentation of approaches across different jurisdictions. The proposed solution is to offer a set of fundamental principles that may underlie and justify information privacy rights in a number of jurisdictions. The fundamental principles take account of the latest developments regarding information privacy in the United States and the European Union. These principles embody a paradigm shift that may benefit human rights and consumer protection.

5.1: INTRODUCTION

Vast increases in the volume of personal data stored both nationally and internationally have brought the rights relating to that information into sharper focus. Our understanding of information privacy rights is capable of evolving just as our technology evolves. There have

⁴¹ This chapter has been published as: Toy, A. 2013. Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy. *New Zealand Universities Law Review* 25 (5): 938-959.

been suggestions that information privacy rights are no longer the most appropriate way to prevent processes such as data mining from delving into our lives (Rubinfeld 2008). Yet when the claim is made that privacy is dead, it overlooks the positive effects that information privacy may have on the development of trust in online interactions. There exists “widespread public perception that there are significant risks associated notably with online activity.” (European Commission 2012, 2). The development of the online environment as a place for consumer interactions and transactions requires this attitude to change. Enhanced understanding and effectiveness of information privacy laws is an important step in this process.

Information privacy rights have not yet presented a coherent theoretical basis. They are also fragmented in their application across jurisdictions. Competing interests such as technological innovation and the drive toward global processing of data threaten established information privacy paradigms.⁴² Current information privacy laws have sound objectives, but this has not prevented problems from arising due to new technologies such as social networking, cloud computing and mobile devices (especially mobile applications or apps). To deal with the conflicts that arise between these interests, an enhanced jurisprudential theory is required. Information privacy rights have a relatively short legal pedigree so they have had little time to develop this theory.

The theory should emphasise principles above rules as a method of determining where information privacy sits in the legal landscape. While principles have been a part of this area of law since its inception, they should be given even greater prominence in order to assist the coming of age that is necessary to achieve the goals that information privacy law must aspire to. Unfortunately, many of the standards that are currently seen as information privacy

⁴² Challenges for protection of personal data include addressing the impact of new technologies and improving the coherence of the data protection legal framework (European Commission 2010, 3-4).

principles are merely rules that have been misclassified. To find the principles that truly underlie information privacy rights, these standards should be reduced to a more abstract form. This will produce a set of fundamental principles that may provide guidance for global harmonisation of information privacy rights. In addition, recent moves toward enhanced cross-border cooperation will be assisted by a common set of standards.

The search for fundamental principles has taken on urgency with the recent development of proposals by bodies in both the United States and the European Union that suggest new principles as a basis for information privacy legislation. However, these proposals remain markedly different both in their emphasis on which principles are appropriate, and in the way in which the legislation will be implemented. This chapter suggests a paradigm shift that goes further than anything that has been proposed by combining the best elements of the United States' and European proposals. It proposes a set of fundamental principles for information privacy law that will provide a way forward by defining the ways in which existing and future competing interests may work alongside information privacy principles.

5.2: RIGHTS IN THE FORM OF PRINCIPLES

The existence of principles in the general law is now well established (Dworkin 1978, 82). Principles relate to an individual or group right. Information privacy rights have been enacted in the form of principles in jurisdictions such as Australia⁴³ and New Zealand.⁴⁴ However, the privacy principles that have been enacted in jurisdictions such as Australia and New

⁴³ The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) has altered the Privacy Act 1988 (Cth) by introducing the 13 Australian Privacy Principles (APPs) that will come into force in March 2014.

⁴⁴ Privacy Act 1993, s 6.

Zealand do not clearly articulate the fundamental principles (Gunasekara and Toy 2011, 533) that underlie information privacy law.⁴⁵

The approaches of the Australian Law Reform Commission (ALRC 2008) and the New Zealand Law Commission (NZLC 2011) have not recommended putting the fundamental principles into statutory form. Although both have argued for principles in information privacy statutes, the principles are complex and detailed, and (as will be shown below) are more properly classified as rules. Just two⁴⁶ of the Australian proposed principles could have been properly described as fundamental principles. However, Australia has now enacted 13 Australian Privacy Principles (APPs) that differ from those proposed by the ALRC. Of these 13 APPs, only one readily translates to a fundamental information privacy principle.⁴⁷

Opposed to the argument that fundamental principles exist in the law (even if not enacted in that form), stands the soft positivism approach of HLA Hart (Hart 2012, 250). In order for Hart's approach to implement the fundamental principles discussed in this chapter, it would be necessary to argue for a radical reform of privacy law. Hart's approach is less useful as a justification for the principles discussed later in this chapter because it is not able to ascertain the more abstract fundamental principles on which information privacy rights are based. Ronald Dworkin's approach, on the other hand, is a more natural justification for the fundamental principles that underlie information privacy law. Under this approach, it is unnecessary to argue for a change to statute law. Current Australian and New Zealand statutes are capable of supporting the idea that more fundamental principles underlie and justify the principles contained therein.

⁴⁵ With the exception of just one of the Australian APPs: Australian Privacy Principle 1—open and transparent management of personal information.

⁴⁶ See pt 5 of this chapter.

⁴⁷ Australian Privacy Principle 1—open and transparent management of personal information. This readily translates to the fundamental principle of Transparency; see pt 6 of this chapter.

5.3: CHALLENGES TO INFORMATION PRIVACY LAW

Information privacy law is now facing increasing global challenges. Much processing of information now occurs overseas; for example, data processed by online social networks (in the case of Facebook, much of its data processing occurs in the United States, in respect of its domestic customers, and in Ireland, in respect of its international customers). Further examples of international data transfers include the advent of cloud computing and the increasing ubiquity of online purchases. Online use of credit cards, such as to purchase airline tickets, also results (in many instances) in international transfers of data and the processing of that data in a different jurisdiction to that in which the customer resides. Technological innovations relating to the global transfer and processing of data have presented a landscape in which information privacy law is struggling to keep up. Application of obsolete standards is a major factor that leads to the difficulties faced in this area of the law. In its current form, it is true that “data protection regulation would have difficulty in getting to grips with online breaches of privacy” (Roth 2010, 535).

An example of disconnect between older standards and new challenges relates to the definition of Personal Information or Personally Identifiable Information (PII). The FTC has stated that “[t]here is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII” (FTC 2012, 20). It is clear that data can now be linked to a computer or internet-enabled device and that profiles can exist in respect of a computer that can be linked to an individual. This has led the FTC to recommend a definition of PII that includes “consumer data that can be reasonably linked to a specific consumer, computer, or other device ...” (FTC 2012, 22). This differs from previous definitions which did not refer to “linked” information.⁴⁸ Previous definitions of personal

⁴⁸ For example, in s 2(1) of the New Zealand Privacy Act 1993: “**personal information** means information about an identifiable individual ...”.

data were also given a narrow interpretation, and Lord Auld in *Durant v FSC* noted that “not all information retrieved from a computer search against an individual’s name or unique identifier is personal data”.⁴⁹

5.4: INTERNATIONAL INFLUENCES

An array of policy initiatives have contributed to the current state of information privacy/data protection evolution (Bennett and Raab 2003, 90). This has had a somewhat cumulative effect and “these efforts have produced a continuing process of policy convergence, as both the principles and instruments of privacy protection have grown increasingly alike and have been adopted by a greater number of countries” (Bennett and Raab 2003, 89).

The European Union (EU) has been a global leader in the field of data protection law. The 1995 Directive⁵⁰ was an important influence on data protection standards around the world. The Directive contains five “Principles Relating to Data Quality”.⁵¹ Arguably only the second of these (“collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ...”⁵²) is translatable to any of the fundamental principles suggested in this chapter.⁵³ It is clear from the rest of the Directive that “consent” is a relevant principle but it is not articulated as such.

Continuing in this vein, the EU wishes to “remain a driving force in promoting high data protection standards worldwide” (European Commission 2010, 5). However, this will not be achieved if the EU allows its approach to become outdated, thus creating the impetus

⁴⁹ *Durant v Financial Services Authority* [2003] EWCA Civ 1746, [2004] FSR 28 at [28].

⁵⁰ 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.

⁵¹ 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, art 6(1)(a)–(e).

⁵² 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, art 6(1)(b).

⁵³ Translatable to the principle of respect for context and the principle of legitimacy: See pt 6 of this chapter.

for the European Commission's newly proposed general data protection regulation (European Commission 2012). The European Commission recognises that (European Commission 2012, 18):

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly ... These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market.

5.5: PRINCIPLES OR RULES?

As both principles and rules exist in the law, it becomes necessary to examine the most appropriate vehicle for embodiment of information privacy rights. Principles are more flexible but this also entails that they are less precise and offer less guidance in specific situations. The generality of principles may be more of an advantage in the area of information privacy rights than in other areas of the law. This is because information privacy rights are more affected by changes in technology than other rights are. The flexibility to apply to innovative uses of technology should be seen as an important requirement of information privacy rights.

Consumer education is another factor that points in favour of principles. The Federal Trade Commission has "called for all stakeholders to accelerate their efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers" (FTC 2012, 71). Such education would be more effective if the principles were in a form that could be more easily remembered. A formulation of seven short principles is more appropriate for this purpose than a dozen or so detailed rules.

Principles have another important advantage over rules in the context of information privacy rights. Principles can inform future law making more readily than rules. This is because principles allow other interests to be weighed against them. Other interests may therefore be applied as they become relevant due to changes in technology or in social conventions regarding use of the internet. Principles survive even if outweighed in a particular context, as opposed to rules, which would require constant updating to cope with changes in technology. Due to the speed at which technology changes, information privacy rights are most appropriately governed by principles.

The Organisation for Economic Co-operation and Development (OECD) has been very influential in the area of information privacy principles. In 1980, it produced a set of guidelines (OECD 1980) that specified eight principles which have formed the basis of national information privacy laws in many jurisdictions. On a superficial reading, some of the OECD principles look like fundamental principles. However, a careful analysis reveals that the eight OECD principles are too detailed to be fundamental principles and that further reduction is necessary to reveal the underlying basis of these principles. For example, the concept of “consent” comes into the OECD’s Collection Limitation Principle and the Use Limitation Principle. This demonstrates that it is a concept that deserves its own category, as it is important for the implementation of appropriate information privacy practices.

Furthermore, the principles are quite detailed and many contain lists of rules that are incompatible with their designation as principles. In particular, the Use Limitation Principle and the Individual Participation Principle have lists of bullet points which contain quite prescriptive rules. The Individual Participation Principle has a list of four bullet points. One of these specifies the timeframe in which an individual’s information must be supplied, and the cost to the individual of the supply. This is evidence that the OECD guidelines contain some rules, which are not eligible to be principles under Dworkin’s theory. On the other

hand, some of these principles are appropriately designated as principles. For example: the Accountability Principle, and the Openness Principle. These principles are readily translatable to the fundamental principles of transparency and accountability (discussed below).

Although the original OECD guidelines were very influential, they were produced over 30 years ago, and technological challenges have now arisen that make it necessary to look to a new set of standards. The OECD has recently stated that “[o]ur current legal and policy frameworks – most of which were developed in the 1970s or 1980s – could take advantage of more recent approaches to protecting privacy in today’s environment” (OECD 2011, 41). It recommends the ‘privacy by design’ principle as a useful addition to the debate.

The Australian approach is a hybrid between principles and rules. The Australian Law Reform Commission (ALRC) has recommended 11 Unified Privacy Principles (UPPs) (ALRC 2008, 94). This large number of principles immediately draws attention to the fact that few of them are true principles, and many are simply rules. Of the 11 UPPs, only two could have arguably translated to a fundamental principle. These are UPP 3 Notification and UPP 4 Openness. These two are arguably translatable to the fundamental principle of transparency which will be described below. However, Australia has enacted 13 new Australian Privacy Principles (APPs), only one of which is translatable to a fundamental principle.⁵⁴ This demonstrates that Australia has taken an approach that favours rules more than the recommendations of the ALRC did.

The ALRC has stated that “the ALRC adopts a pragmatic approach to its regulatory model, drawing significantly on principles-based regulation as its foundation, but allowing for a reversion to more traditional rules-based regulation where appropriate” (ALRC 2008,

⁵⁴ This is: “Australian Privacy Principle 1—open and transparent management of personal information” which readily translates to the fundamental principle of Transparency; see pt 6 of this chapter.

241). This approach is based on the twin objections that: while principles are desirable, they lack certainty and so they need to be supplemented by rules; and that one set of principles may not achieve the policy objectives in all the areas covered by privacy legislation. However, this last objection is not consistent with Ronald Dworkin's analysis, which is not a fixed or rigid formula, but instead allows flexibility when applying principles (Dworkin 1978, 338-339). Principles may be given greater or less weight in a given situation and the application of policy interests may assist in this process. There is no restriction under Dworkin's theory that excludes policy from consideration in a given situation. The first objection of the ALRC, namely that principles lack certainty, is also unsustainable. The ALRC's approach goes against the grain of the latest international initiatives, which (as will be seen below) favour not merely a principles-based approach, but an approach that seeks to find fundamental principles that lie beneath and justify the currently articulated principles. These arguments apply with even more force to the 13 APPs that have now been enacted in Australia. These demonstrate an approach that favours rules even more than the ALRC proposal did. It is therefore even less appropriate than the ALRC proposal was for implementing a set of fundamental principles for information privacy law.

The latest suggestions by the New Zealand Law Commission (NZLC) are similar in their tenor to the Australian approach and therefore they are divergent from the latest developments in the United States and the European Union. The NZLC states, when discussing the possibility of a principles- or rules-based approach to privacy legislation: "We believe the Act currently gets the balance between flexibility and specificity right" (NZLC 2011, [2.12]) Although the NZLC strongly supports a principles-based approach to the Act, (NZLC 2011, 44) it does not advocate major changes to the way the privacy principles are currently articulated in the Privacy Act 1993. The 12 Information Privacy Principles (IPPs) in this Act are not readily translatable to the fundamental principles discussed in this chapter. It

is arguable that these IPPs may deserve the status of rules, not principles. The New Zealand IPPs are complex and repetitive in some instances. For example, the issue of authorisation (which is readily translatable to the fundamental principle of consent⁵⁵) is mentioned as an exception to four of the IPPs, and the wording is similar in each. The concept of consent is properly a fundamental principle of information privacy law, and should be articulated as such.

A major advantage of a principles-based approach to information privacy rights is that the principles can be weighed against other principles of the law in cases of conflict. It is important to balance certain interests against each other to achieve an appropriate ordering. Such an approach permits privacy principles to be recognised as human rights that may, in certain cases, outweigh other principles, or be outweighed by them. It will be shown below that some leading courts of the European Union have a well-established jurisprudence regarding the weighing of privacy principles against other principles in the law. The European approach would be a good model for other jurisdictions in this regard. However, this approach has not generally found its way into legal systems that are based on the common law system. This is not to say that it would not be welcomed there though. The Obama Administration has stated that (The White House 2012, 21):

[t]he rights of freedom of speech and freedom of the press involved in the collection and use of these documents must be balanced with the need for transparency to individuals about how data about them is collected, used, and disseminated and the opportunity for individuals to access and correct data that has been collected about them.

⁵⁵ In the information privacy context, the concept of consent should not be given its contract law meaning (Toy 2009).

To some extent, this weighing approach has support in the New Zealand Privacy Act 1993. However, it is rendered almost nugatory by other inconsistent provisions within that Act. Section 14 is a weighing provision that requires the Information Privacy Principles to be weighed against other laws to determine which interests are appropriate in a given case. Section 14 requires the New Zealand Privacy Commissioner, when exercising powers and duties under the Act, to have regard to interests “including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way”.⁵⁶ This provision is unfortunately inconsistent with s 7 of the Privacy Act 1993, a ranking provision that allows other laws to override the Information Privacy Principles (IPPs). The NZLC has recommended changes to s 7, largely on the basis that it is complex and difficult to interpret. The NZLC recommends a simple provision that confirms that the IPPs always submit to other laws where there is an inconsistency. However, this may not be the most appropriate way to deal with the difficulties caused by s 7. Instead, s 7 should be repealed and not replaced. It may be preferable to expand s 14, to require weighing of other interests when any action is taken by any agency subject to the Act. New Zealand could follow the European approach. The New Zealand Court of Appeal confirmed that a weighing approach is part of New Zealand information privacy law in *Harder v Proceedings Commissioner* where the majority stated:⁵⁷

The approach of the Commissioner and the tribunal in the present case does not suggest that [s 66(1)(b)] has been viewed alongside the balancing provisions of s 14(a). They require the Commissioner, and implicitly others involved in the interpretation and administration of the Act, to have due regard for the protection of important human rights and social interests that compete with privacy

⁵⁶ Privacy Act 1993, s 14(a).

⁵⁷ *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (CA) at [23].

5.6: THESIS OF THIS CHAPTER: SEVEN FUNDAMENTAL PRINCIPLES

The need for fundamental principles has been apparent for some time in information privacy law, and some suggestions have been made in this regard (Gunasekara and Toy 2011). Now, in the light of important recent developments, a new formulation is apposite. The new developments regarding fundamental principles have come mainly from the United States and the European Union. For example, the principle of privacy by design has emerged from statements made by official bodies in both jurisdictions. Unfortunately, not all jurisdictions have followed this new approach. Australia and New Zealand have remained with the older paradigm for information privacy law, which follows the OECD approach. This may simply be evidence of a lag effect, as the recent suggestions by the Australian and New Zealand Law Commissions were made before the new developments in the United States and the European Union, so they did not have the benefit of the latest international proposals. In any event, technology is changing and information privacy law must follow a new paradigm or risk failure to achieve its objectives.

Daniel Solove states that “[w]e do not need overarching principles to understand and recognize problems. Too often, attempts to identify such principles about privacy result in failing to address important problems. If we focus on the problems, we can better understand and address them. I aim to shift the approach to a bottom-up focus ...” (Solove 2008, 105). Solove’s analysis is contrary to the latest international developments. Problems about privacy often spring from new technologies, so Solove’s focus may become outdated. Instead, we need a fundamental set of overarching principles, supplemented by sectoral codes which would allow updating by industry groups. The main legislation should be based on a strong set of fundamental principles that would set a base line for protection of information privacy rights.

The thesis of this chapter is that seven fundamental principles underlie the currently enacted information privacy principles. They are higher level than previous privacy principles because they are the smallest number of discrete principles. All previous principles fall within the broad conception of these ones. The principles are derived by sourcing the latest information privacy principles from the US and EU documents and cases and comparing them with the older sets of principles. The exercise of reducing them to fundamental principles is a philosophical one that brings them down to the most basic conception of each principle. The fundamental principles are more flexible than existing regimes because other sets of principles contain rules that cannot necessarily be applied across different countries therefore the fundamental principles are a better format for harmonized standards than all other regimes.

These fundamental principles are an amalgamation of the best aspects of the latest international developments, and this demonstrates a continuation of the heritage of information privacy law as being sourced primarily in international instruments. The seven fundamental principles are: (a) privacy by design; (b) respect for context; (c) consent; (d) transparency; (e) legitimacy; (f) proportionality; and (g) accountability. In this context, the principle of consent means a special kind of consent akin to the concept of authorisation under the New Zealand Privacy Act 1993 (Toy 2009).

Strong support for the fundamental principles of privacy by design and legitimacy can be found in the proposal by the European Commission.⁵⁸ The principle of Privacy by Design is also recommended by the Federal Trade Commission,⁵⁹ and by the OECD.⁶⁰ The principles of respect for context, transparency and accountability are supported by the Obama Administration (The White House 2012, 10). “Consent” is supported in the form of

⁵⁸ See pt 8 of this chapter.

⁵⁹ See pt 10 of this chapter.

⁶⁰ See pt 5 of this chapter.

Individual Control by the Obama Administration, and it is included in the principle of Choice and Consent in the Generally Accepted Privacy Principles promulgated by the American Institute of Certified Public Accountants (AICPA and CICA 2009, 7). “Proportionality” comes through in the case law of the European Court of Justice and the European Court of Human Rights.⁶¹

“Privacy by design” was pioneered by Dr Ann Cavoukian (Cavoukian and Stoianov 2014, 3). It means that information privacy protections should be baked in to every stage of the development of products and services (FTC 2012, 22). For example, if a new app is developed, questions about information privacy should be addressed at the design stage as well as being implemented when the software code is written.

“Proportionality” could be used in two senses: balancing information privacy rights against other interests of the general law; and balancing information privacy rights against other information privacy rights. The principle of proportionality referred to in this chapter is broadly defined to include both of these aspects. In addition, “proportionality” in this model incorporates the concept of fairness, since an ideal way to judge fairness is to balance an action against other competing interests. “Proportionality” can also incorporate the concept of data minimisation as data should only be collected in proportion to the function it will serve. Collection of unnecessarily large amounts of information would be disproportionate to the purpose to be served.

The concepts of data security, sound retention/disposal practices and data accuracy also need to be addressed. The Federal Trade Commission believes these can be subsumed in the “privacy by design” principle (FTC 2012, 23). This is correct as regards security and accuracy, as these concepts are most relevant at the point of design, and problems with security and accuracy can best be remedied at this stage. However, it is incorrect as regards

⁶¹ See pt 7 of this chapter.

retention/disposal practices as these obligations continue beyond the point of design. This chapter proposes the principle of respect for context in order to address this deficiency: The data controller may collect/retain/use/dispose of data so long as the context in which it was disclosed is respected. The fundamental principle of respect for context is broad enough to include issues of data security (because any disclosure that is unauthorized must therefore be a context in which the data should have been protected by stronger security measures) and purpose limitation (because any limit on the purpose for which data can be used must also entail that the context in which data must be respected has the same limits).

Legitimacy also has two senses. First, it controls the collection/retention of data as this may only be collected for legitimate purposes. Secondly, it supplements the principle of proportionality when weighing other interests against privacy. A competing interest must be both proportionate and have a legitimate aim in order to have a greater weight than an information privacy right in a particular situation.

“Transparency” covers situations in which a data subject may wish to see what a data controller is doing with the data disclosed. It also assists in data accuracy as a data subject may, under this principle, request that data is updated. This concept is broad enough to include issues of data quality. Transparency means that data controllers should be more open, especially to the data subjects about the data held and if it is incorrect, data subjects may then see the problems and require correction.

“Accountability” makes data controllers responsible for data that they hold or have held. It requires data controllers to be careful with data that they transfer to third parties. For example, a data controller may be responsible if the third party did not demonstrate sufficient information privacy practices.

5.7: IMPORTANCE OF INTERNATIONAL INTEROPERABILITY

National information privacy rights have been affected by the impact of international instruments such as the 1980 OECD Guidelines (OECD 1980) and the APEC Privacy Framework (APEC 2005). This is evidence of a top-down approach that is particularly appropriate in this area. With increasing trends toward global processing of data, information privacy rights would be of little use if they could not apply to data that is transferred between different jurisdictions. The extent to which national information privacy laws may have extraterritorial jurisdiction is an issue of increasing significance (Toy 2010; Gunasekara 2007). Additionally, there has been agreement at the international level in favour of enhancing cross-border enforcement of information privacy rights (OECD 2007, 7). This has been applied in New Zealand.⁶²

International interoperability may be defined as the ease with which information privacy rights may be enforced across borders, either as an issue of extraterritorial application of information privacy laws or by enhanced cross-border cooperation among information privacy authorities. International interoperability would be enhanced if information privacy rights were more closely aligned across different jurisdictions. Development of a widely acceptable set of fundamental principles may assist in achieving international interoperability.

A set of fundamental principles would have the flexibility to apply to the legal systems in place in the United States and the European Union even though those jurisdictions may place different emphasis on some of the principles. For example, the fundamental principle of consent may receive different treatment in the United States, where the simplified consent model advocated by the FTC may be appropriate. In the European Union, the

⁶² The Privacy (Cross-border Information) Amendment Act 2010 amended the Privacy Act 1993 to give the New Zealand Privacy Commissioner the power to refer a complaint to an overseas enforcement authority if the matter is “more properly within the jurisdiction” of the overseas authority: Privacy Act 1993, s 72C(1).

principle of consent may require explicit consent in a different range of circumstances than in the United States. Such changes in emphasis are inevitable due to the different policy objectives in different jurisdictions. Policy objectives affect the weight of the fundamental principles of information privacy when they are weighed against other interests in the law. If a principle is outweighed in a particular situation, this does not prevent it from continuing as a principle that may influence future situations. Rules would not have the same flexibility as principles, and would fail to justify the approaches taken in multiple different jurisdictions. Principles are therefore more appropriate than rules as a means of embodying information privacy rights when they are applied across different jurisdictions.

For companies that operate internationally, a set of fundamental principles would also provide guidance. Any personal information that they collect and transfer across borders would be subject to the same set of fundamental principles, which would reduce legal complexity and therefore reduce the cost of compliance. Significantly different standards across the world create an impediment to companies that need to comply with the requirements of different information privacy laws.⁶³

Privacy audits may also benefit from increased international interoperability of information privacy principles. There is currently little convergence among the principles used for privacy audits. Some privacy audits use national information privacy laws as standards for their audit. This is the case with the audit of Facebook-Ireland. The Office of the Data Protection Commissioner of Ireland audited the privacy practices of Facebook-Ireland in 2011, and this audit was “conducted taking account of the eight principles of data

⁶³ Difficulties may also exist for organisations that operate domestically, but that outsource information overseas (such as those that use offshore cloud computing services). The New Zealand Law Commission has proposed that the domestic organisation should remain responsible under domestic law for any privacy breaches in respect of the information in this situation. The NZLC has recognised the difficulties that this model may cause to organisations that are subject to the requirement. It has recommended that the New Zealand Office of the Privacy Commissioner publish lists of countries that have privacy laws that would provide protection of an acceptable level relative to the Privacy Act 1993 (NZLC 2011, 280). However, such advice may not give sufficient guidance in specific situations, and may not absolve a company wishing to send data offshore of the need to investigate the information privacy laws of other countries.

protection” (Office of the Data Protection Commissioner of Ireland 2011, 24; Office of the Data Protection Commissioner of Ireland 2014, 13)⁶⁴ The first and fourth/fifth⁶⁵ of these principles are arguably translatable to the fundamental principle of proportionality,⁶⁶ but the others are not easily translatable to any of the fundamental principles.

Privacy audits may implement the Generally Accepted Privacy Principles (GAPPs) developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA and CICA 2009). The Canadian Privacy Commissioner has conducted several privacy audits, some of which have “followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants” (Office of the Privacy Commissioner of Canada 2011c, 29). The current GAPPs are articulated in the form of 10 principles that reflect the older information privacy principles currently in force in countries such as Australia and New Zealand. Only two of the GAPPs (Notice and Choice and Consent) are readily translatable to the fundamental principles identified in this chapter (respectively; “transparency” and “consent”). The other eight GAPPs reflect rules that are not closely representative of the other five fundamental principles. This leaves the GAPPs lacking in their application of the latest information privacy principles, and as a result they may not be the most appropriate set of standards for a privacy audit. In the light of changing technologies, the GAPPs should be updated to reflect international best practice, including the fundamental principles derived from the new approaches in the United States and the European Union. These new approaches are the latest and most up to date principles for information privacy and therefore they are the best foundation for fundamental principles that may be relevant in different countries.

⁶⁴ These principles emanate from the Data Protection Act 1988 (Ireland) and the Data Protection (Amendment) Act 2003 (Ireland).

⁶⁵ The positions of the fourth and fifth principles are switched between these audit documents. The fourth principle is the one referred to in the audit report and the fifth is the one referred to in the audit resource.

⁶⁶ See pt 6 of this chapter.

Sophisticated privacy audits go further than mere application of the information privacy laws of the jurisdiction in which the audit is carried out. They refer to international best practice such as the principle of privacy by design (KPMG and IIS 2012, 23-24). This is an enlightened approach that would enhance the audit as it takes account of international trends in information privacy standards. This approach to privacy audits would encourage international interoperability as it implements some of the emerging fundamental principles. Particularly for companies that operate internationally, this is the most appropriate type of audit.⁶⁷

5.8: EUROPEAN COURT OF HUMAN RIGHTS AND EUROPEAN COURT OF JUSTICE

The European experience has revealed a sophisticated balancing test for weighing information privacy rights against other interests. A well-established jurisprudence has developed (Wright and De Hert 2012, 45-49) that could be useful as a model for other jurisdictions. This case law has produced a test for balancing information privacy against other interests, but it has not produced the entire set of fundamental principles that underlie information privacy law. The only fundamental principles that have emerged from this approach have been “legitimacy” and “proportionality”, both of which assist with the balancing test, but which do not deal with the range of other information privacy rights. Other models could also be used, such as those of the European Commission, the Obama Administration and the Federal Trade Commission.⁶⁸

⁶⁷ The Data Protection Commissioner of Ireland, in its audit of Facebook-Ireland, has stated that it “should not however be interpreted as asserting sole jurisdiction over the activities of Facebook in the EU.” This impliedly recognises that an organisation may be subject to multiple territorial standards (Office of the Data Protection Commissioner of Ireland 2011, 21).

⁶⁸ See pts 8 to 10 of this chapter.

The approach taken is to balance other rights against privacy according to six principles: (a) in accordance with law; (b) necessary in a democratic society; (c) legitimate aim; (d) adequate safeguards against abuse; (e) consistent with other interests; and (f) proportionate. The principles stem from various legislative sources, as well as purely from case law. A major influence has been art 8 of the European Convention on Human Rights.⁶⁹ Other influential instruments have been art 7(e) of the Data Protection Directive⁷⁰ and arts 8 and 52 of the Charter of Fundamental Rights of the European Union.

The principle of legitimacy is evident in a European Court of Justice (ECJ) case.⁷¹ In this case, the federal government in Germany collected data on foreign nationals resident in Germany, partly for statistical purposes. This was in conflict with the data protection directive.⁷² The concept of “legitimacy” was discussed in this case, with the Court stating that collection of such information solely for the purposes of administering the legislation relating to the right of residence was legitimate, and was also consistent with the right to freedom from discrimination contained in art 12 of the Treaty Establishing the European Community.⁷³ However, the existence of such a register for the purposes of fighting crime was not consistent with art 12, since crimes may be committed by anyone regardless of nationality.⁷⁴ In certain situations, an interest may outweigh another interest, or be outweighed by it. This case demonstrates the use of a balancing test to weigh one interest against another.

⁶⁹ Council of Europe “Convention for the Protection of Human Rights and Fundamental Freedoms” (1950) Rome.

⁷⁰ 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.

⁷¹ Case C-524/06 *Huber v Germany* [2008] ECR I-9705.

⁷² 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, art 7e.

⁷³ Case C-524/06 *Huber v Germany* [2008] ECR I-9705 at [58].

⁷⁴ Case C-524/06 *Huber v Germany* [2008] ECR I-9705 at [78]–[81].

Another important ECJ case demonstrates the principle of proportionality.⁷⁵ In this case, a woman had posted some information about members of her church group on the internet. The ECJ stated that information privacy rights and interests needed to be weighed against other rights and interests in question, to ensure a fair balance.⁷⁶ It was also stated, without statutory basis, that there existed “general principles of Community law, such as inter alia the principle of proportionality.”⁷⁷ “Proportionality” requires that national legislation in member states is interpreted in a way that “take[s] account ... of all the circumstances of the case ... , in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed.”⁷⁸ This demonstrates that the ECJ believes “proportionality” has a very broad meaning that goes beyond a mere balancing test with other interests. The principle also includes an examination of the application of information privacy principles in an individual case, in order to judge their importance for the persons concerned. This aspect of the case raises the idea that even within the compass of the information privacy principles there may be scope for the application of the principle of proportionality. The fact that the ECJ gave no statutory basis for the principle of proportionality reveals that it is therefore consistent with Dworkin’s analysis (Dworkin 1978) – a principle that is found not in statutory form.

A case in the European Court of Human Rights (ECHR) also adds to the principle of proportionality.⁷⁹ In this case, a man had attempted to commit suicide on a public street by slashing his wrists with a knife. This activity was recorded by CCTV cameras. The footage was released to the news media without sufficient safeguards to protect his identity. The

⁷⁵ Case C-101/01 *Lindqvist v Sweden* [2003] ECR I-12971.

⁷⁶ Case C-101/01 *Lindqvist v Sweden* [2003] ECR I-12971 at [90]. The rights in question came from the 1995 Data Protection Directive and art 10 of the European Convention on Human Rights which enshrines the right to freedom of expression.

⁷⁷ Case C-101/01 *Lindqvist v Sweden* [2003] ECR I-12971 at [87].

⁷⁸ Case C-101/01 *Lindqvist v Sweden* [2003] ECR I-12971 at [89].

⁷⁹ *Peck v United Kingdom* (2003) 36 EHRR 41 (Section IV, ECHR).

release of information in this way was held to be disproportionate.⁸⁰ “Proportionality” in this case focused on “striking a fair balance between the relevant conflicting public and private interests.”⁸¹ The interest of the State in the prevention and detection of crime was very strong in this case, but it was outweighed by the complainant’s interest in his private life because the footage could have been easily altered in order to protect his identity, but it was not.

5.9: EUROPEAN COMMISSION

The European Commission has proposed a new Data Protection Regulation (the Regulation) (European Commission 2012). If adopted, this Regulation would become harmonised law across all member states of the European Union (EU), replacing the incumbent 1995 Directive⁸² which does not have the status of a regulation (and can therefore be implemented in different ways in different member states of the EU). Article 5 of this proposal provides a strong basis for fundamental principles. It states six principles (European Commission 2012, 43), four of which can be readily translated to five of the fundamental principles. These are: “(a) processed lawfully, fairly and in a transparent manner ...” (this translates to “transparency”); “(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ...” (this translates to two fundamental principles: “respect for context” and “legitimacy”); “(c) adequate, relevant, and limited to the minimum necessary ...” (although this does not translate exactly to “proportionality”, it is an important part of the principle of proportionality); “(f) processed under the responsibility and liability of the controller ...” (this translates to “accountability”).⁸³ The remaining two

⁸⁰ *Peck v United Kingdom* (2003) 36 EHRR 41 (Section IV, ECHR) at [87].

⁸¹ *Peck v United Kingdom* (2003) 36 EHRR 41 (Section IV, ECHR) at [77].

⁸² 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.

⁸³ The principle of Accountability is further backed up by art 22 which defines standards for protecting personal data, and even provides for internal or external audits.

principles of the proposed Regulation are easily subsumed in broader fundamental principles. For example, “(d) accurate and kept up to date ...” is part of the fundamental principle of transparency, and “(e) ... permits identification ... for no longer than is necessary ...” is part of the fundamental principle of proportionality.

The Regulation further provides that member states may pass legislation that limits the scope of the first five principles of art 5. However, these limits must only occur when there is another public interest (European Commission 2012, art 21(1)) that outweighs the art 5 right(s) and “... when such a restriction constitutes a necessary and proportionate measure in a democratic society ...”. This is therefore akin to a balancing test whereby other rights and interests that may conflict with information privacy rights are weighed to determine if they are more influential in any given situation. This is an important addition to the debate on information privacy. Only by treating information privacy rights as valid parts of the legal system, able to be weighed against other interests, can information privacy law assume a viable position as a human right. This objective may be achieved if the principle of proportionality is given an expansive meaning that includes this balancing test.

“Proportionality” is specifically mentioned in art 21, and it can bear a meaning that relates to other rights and interests of the legal system as a whole. Although the balancing test in art 21 is not part of the principles in art 5, it may still be translatable to a fundamental principle (the principle of proportionality).

“Proportionality” is not mentioned as a principle in the art 5 list, but it is mentioned as a principle in the preamble to the proposed Regulation, where it is stated that “the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality ...” (European Commission 2012, 39). The categorisation of proportionality as a principle coupled with its omission from the list of principles in art 5 may

be viewed as an internal inconsistency, and this demonstrates that there is room for other principles to emerge from the proposed Regulation. The proposed Regulation should be read as a whole to distil the principles that underlie it. In this manner, all of the fundamental principles may find a basis in the EU proposed Regulation. The two remaining fundamental principles are “consent” and “privacy by design”, and it may be observed that these can be found within different parts of the proposed Regulation.

“Data protection by design and by default” is art 23 of the Regulation (European Commission 2012, 56). It is also mentioned in the preamble to the Regulation, where it is called a principle (European Commission 2012, 27). This categorisation is not a coincidence, as it mirrors the treatment of the principle of proportionality. “Privacy by design” should therefore be seen as a fundamental principle on which information privacy law is based.

The concept of consent is also an important part of the proposed Regulation. “Consent” is part of art 6, which establishes the lawfulness of processing of data (European Commission 2012, 43). However, “consent” is not specifically categorised as a principle either in the regulation or its preamble. Nevertheless, “consent” is considered important enough to have an entire article dedicated to it (Article 7: Conditions for consent), and this coupled with the ubiquity⁸⁴ of consent as part of the Regulation, should indicate that it deserves the status of a fundamental principle. “Consent” is particularly important in the case of sensitive data, which the European Commission believes should not be processed in the absence of explicit consent of the data subject (European Commission 2012, 24).

Interestingly, the European Commission states that “silence or inactivity should ... not constitute consent” (European Commission 2012, 21). This is in direct contrast to the

⁸⁴ For examples of consent in a different part of the regulation, see arts 17(1)(b), 18(2), 20(2)(c) and 44(1)(a). Under art 79(6)(a), penalties for breaching the conditions for consent include fines of up to €1m for an individual or 2 per cent of the annual worldwide turnover of an enterprise.

suggestions of the Federal Trade Commission which would simplify consent, to the point where data may be processed for some limited purposes in the absence of consent.⁸⁵

5.10: UNITED STATES CONSUMER PRIVACY BILL OF RIGHTS

The Obama Administration has proposed a framework for enhanced information privacy laws in the United States (The White House 2012). The proposed Consumer Privacy Bill of Rights (CPBR) includes Fair Information Practice Principles (FIPPs). These comprise seven “comprehensive, globally recognized” (The White House 2012, 1) principles. The suggested legislation would be backed up by multi-stakeholder groups to decide on industry codes of practice. These industry codes may make exceptions to the principles in the proposed legislation if the FTC has approved the code in question. They would therefore be akin to a safe harbour: protection from the FIPPs for those companies that follow the industry codes of practice. In the absence of legislation, the industry codes will still serve a purpose as the FTC may refrain from exercising its other enforcement powers (to prohibit unfair or deceptive acts or practices)⁸⁶ (The White House 2012, 7) against an organisation that follows such a code (FTC 2013, 12). The first of the multi-stakeholder groups started on 12 July 2012 and was focused on app privacy, specifically on mobile apps.⁸⁷

The CPBR, if enacted, would be the first United States privacy legislation to apply generally to the private sector. Previous United States privacy legislation has followed a sectoral approach, with some industries being covered and others not. However, there would remain gaps in coverage of the proposed CPBR. It would not apply to certain sectors such as the financial services industry which is already covered by the Gramm-Leach-Bliley Act

⁸⁵ See pt 10 of this chapter.

⁸⁶ Federal Trade Commission Act of 1934 (US), s 5.

⁸⁷ The multi-stakeholder groups are convened by the National Telecommunications & Information Administration within the US Department of Commerce. Details of the process are available from: www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

(GLBA). This exception would not exempt entire organisations, merely the activities of those organisations that are already covered by GLBA (The White House 2012, 38).

CPBR would include seven principles (The White House 2012, 10), four of which are readily translatable to fundamental principles. These are: Individual Control (which is translatable to the fundamental principle of consent); Transparency (which is a fundamental principle); Respect for Context (which is a fundamental principle); and Accountability (which is a fundamental principle). In addition, the Focused Collection principle may be an instance of the principle of proportionality, but it does not cover the full breadth of this concept. The fundamental principles that are missing from the Obama formulation are: “privacy by design”, “legitimacy” and “proportionality”.

Even though “proportionality” is not designated as a principle in the CPBR, it is mentioned in the proposed framework. In particular, the Obama Administration states that “[t]he rights of freedom of speech and freedom of the press ... must be balanced with the need for transparency to individuals about how data about them is collected, used, and disseminated ...” (The White House 2012, 13). This indicates that the Obama Administration sees a role for a balancing test that can weigh information privacy rights against other rights of the legal system as a whole.

A strong theme underlying the formulation of the CPBR is the view of the Obama Administration that the internet economy is a major benefit to the United States and that to continue to enjoy this benefit, consumers must be able to trust the technology – “Protecting Americans’ privacy by preventing identity theft and prosecuting identity thieves is an important focus for the Administration” (The White House 2012, 6).

5.11: FEDERAL TRADE COMMISSION

The FTC in the United States identifies three main principles and seven subsidiary principles, for a total of 10 principles (FTC 2012). The main principles are: Privacy by Design, Simplified Consumer Choice, and Transparency. The seven subsidiary principles are not translatable to the fundamental principles, and are merely specific rules that address the application of the main principles. In this respect, they cover much of the ground already covered by previous articulations of information privacy laws, and “the Commission notes that the framework already embodies all the concepts in the 1980 OECD privacy guidelines, although with some updates and changes in emphasis” (FTC 2012, 23).

Of the main principles, Privacy by Design and Transparency are fundamental principles. Simplified Consumer Choice is related to consent, but it would implement several controversial measures that do not coincide with other formulations of the “consent” principle. In particular, the European Commission does not believe that silence can constitute consent.⁸⁸ This may be in conflict with the FTC belief that no choice should be required if data is processed within the context of the relationship between the data subject and the data controller (FTC 2012, 36). However, there may be a way to reconcile the approaches of the FTC and the European Commission. The FTC does not say that consent may be implied, or that silence may constitute consent, merely that consent is not required in some limited situations. The European Commission also recognises that consent is only required for some processing of personal data, and that a range of other permissions may exist (European Commission 2012, art 6(1)(b),(f)). In particular, the Commission recognises that, if processing is necessary for the performance of a contract, or is necessary for the purposes of the legitimate interests of the data controller then data may be processed in the absence of consent.

⁸⁸ See pt 8 of this chapter.

The main flaw of the approach taken by the FTC is that it gives insufficient consideration to balancing information privacy rights with other interests. A further criticism is that the approach focuses on individual rules at the expense of wider principles. Consequently, the FTC principles leave important gaps in coverage. An example is the statement of the FTC that their principles include all of the concepts in the original OECD principles (FTC 2012, 23). The FTC refers to the rules following the Privacy by Design principle as evidence of this coverage. However, the very fact of their inclusion in the Privacy by Design principle indicates the contrary. An example is the issue of ongoing respect for context beyond the point of design, which would not appear to be covered by the Privacy by Design principle.

Further criticism of the FTC approach springs from its exemption of activities that are covered by other sector specific laws such as GLBA. This creates a double standard that could lead to confusion. For some activities, financial entities may need to follow the requirements of GLBA, and for other activities, they may be subject to the ordinary privacy principles. The FTC downplays this by stating that, for such entities, compliance with the privacy principles such as Privacy by Design may be of benefit to them because it may assist them to comply with other obligations (FTC 2012, 16).

The FTC has correctly identified that “[e]fforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability” (FTC 2012, 10) However, although the FTC approach purports to be based on principles, this is not the way it comes across. The FTC, by engaging with stakeholders and deciding on quite specific rules appears to be favouring the bottom up approach. This has flowed through to the main principles identified by the FTC, which omit some important aspects as noted above.

The FTC approach does have benefits that should be recognised. The first of these is the recognition of “privacy by design” as a fundamental principle. The second is that the focus on specific instances is an important addition to information privacy law. Any approach that includes fundamental principles will fail unless it is backed up by guidance on how to apply those principles in practice. The FTC approach, by engaging with multi-stakeholder groups, will provide this guidance. In this respect, the FTC approach is a success as it is capable of operating in the absence of legislation to provide industry codes of practice that may assist the development of information privacy rights. The FTC approach should not be seen as a substitute for legislation however. It should operate in tandem with higher level legislative instruments to provide a comprehensive approach to information privacy law.

5.12: CONCLUSION

Information privacy law requires an enhanced underlying theory that is generally accepted across different jurisdictions. Only in this way can it achieve the twin objectives of jurisprudential emancipation and increased international interoperability. This underlying theory should stem from established European jurisprudence coupled with the latest suggestions for legislative reform in the European Union and the United States because suggestions for policy improvements in information privacy have come most recently from these regions. These sources present the foundation for a system of fundamental principles that may be applied to reconcile the place of information privacy law among other rights and interests of the legal system as a whole.

Unfortunately, the latest reforms and suggestions for reform have not been uniform across different jurisdictions. In particular, Australia and New Zealand have not progressed far enough from established approaches that no longer provide solace from increasing pressures generated by technological change. To overcome this lassitude, the Australian and

New Zealand statutes should be viewed through the lens of Dworkin's theory in order to ascertain the fundamental principles that underlie and justify information privacy law. This approach reveals fundamental principles that are a hybrid of the principles articulated in the United States and the European Union, and which are revealed by ascertaining the values underlying these principles. This hybrid of the United States and European Union approaches would have elements of each, but would be a stronger set of principles than merely a buffet of the best principles. Ultimately, the strength of a set of principles lies in its ability to justify the approaches to information privacy law taken in many different jurisdictions.

The research in this thesis is limited to the five countries that are the subjects of the research. However, the suggestions for harmonization argue for privacy principles that are flexible enough to be given different weight in different countries and this could be examined further in future research. It would be useful to consider the application of the fundamental principles to countries beyond the five discussed here.

CHAPTER 6: PRIVACY AUDITING STANDARDS

Alan Toy and David Hay⁸⁹

ABSTRACT

Privacy audits are an area of auditing practice that are becoming increasingly relevant to audit firms as well as to regulators such as privacy commissioners. Privacy audit reports can be a resource for consumers and groups representing them. However, there is limited consistency between the standards applied in privacy audits when compared across different auditors and across different jurisdictions. Inconsistency of standards reduces international comparability of privacy audits, thereby lowering their potential value to the entities subject to audit, and to users of the reports. We suggest a set of fundamental principles for privacy audits drawn from recent proposals for legislative and/or policy reform by leading official bodies in the US and the EU. We apply this framework to 30 privacy audit reports issued in five countries. The results show that few conform to the proposed fundamental principles. This inconsistency limits their value and effectiveness. This chapter relates to the standards used in different privacy audit reports and it is essential to addressing the first research question in this thesis.

6.1: INTRODUCTION

Privacy of personal information⁹⁰ has been an issue of considerable public interest in the twenty-first century. This is demonstrated by legal challenges within the United States such

⁸⁹ This chapter has been published as: Toy, A. and D. Hay. 2015. Privacy Auditing Standards. *Auditing: A Journal of Practice & Theory* 34 (3): 181-199.

⁹⁰ This term is used in the sense of personally identifiable information (PII), as it is relevant to information privacy regulation. However, there is debate about the accuracy of this term (Schwartz and Solove 2011).

as *Klayman v Obama*⁹¹ and *ACLU v Clapper*⁹² following the revelations by Edward Snowden about the collection of certain data regarding the telephone and internet activities of ordinary citizens. Challenges have also arisen in Europe in *Google Spain SL v AEPD*.⁹³ Furthermore, action by regulators has resulted in the imposition of fines such as the \$22.5 million civil penalty that Google paid under a consent order from the Federal Trade Commission.⁹⁴ Examples of issues related to privacy include privacy of personal information on social networks, and security of personal credit card information held on databases. Privacy audits are increasingly implemented as a response to privacy problems. This chapter examines the extent of convergence of the standards used in privacy audits conducted by various privacy auditors.⁹⁵

Privacy audits are of more value if there is consistency among them. This is due to the increasingly global nature of privacy issues. Users and the organizations that are subject to privacy audits, as well as consumers and lobby groups representing consumers, are aware that there are privacy issues and know that these are sometimes addressed by privacy audits. Generally accepted criteria for privacy audits would improve the usefulness of privacy audits because these users would be able to assess the relevance of privacy audits to entities that operate across different countries, and to compare the audits with privacy audits in other countries. If consistent standards are not developed, the onus would fall upon each different user to adjust their understanding of the findings in the audit report based on a range of

⁹¹ *Klayman v Obama* [2013] 957 F. Supp. 2d 1, United States District Court for the District of Columbia. Another example is the Supreme Court case brought by the Electronic Privacy Information Center against the National Security Agency (NSA): *In Re Electronic Privacy Information Centre, Petitioner* [2013] 134 S. Ct. 638.

⁹² *American Civil Liberties Union v Clapper* [2015] U.S. App. LEXIS 7531, United States Court of Appeals for the Second Circuit.

⁹³ Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) European Court of Justice, 13 May 2014.

⁹⁴ Federal Trade Commission (FTC). 2012. *Statement of the Commission*. Available at: <http://www.ftc.gov/os/caselist/c4336/120809googlestatement.pdf> (site accessed 3 December 2013).

⁹⁵ The term “privacy audits” is used for a variety of engagements, many of which are not strictly audits. This issue is discussed later.

technical differences between standards used in different privacy audit reports. In this chapter we suggest a set of fundamental principles for information privacy that could serve as suitable criteria for privacy audits. We assess 30 privacy auditing reports in five countries, and examine the extent of consistency among them and their consistency with these fundamental principles. We find that there is very little consistency.

6.1.1 STANDARDS USED IN PRIVACY AUDITS

Standards used in privacy audits come from a range of different sources. These include detailed privacy laws and general principles of information privacy sourced from recent recommendations made by leading official bodies in the US and the EU (European Commission 2012; FTC 2012; The White House 2012). Many of the standards used in privacy audits are at an early stage of maturity, lack consistency, and generally do not comply with these recommendations regarding information privacy.

There is as yet no international consensus on the precise meaning of privacy audits and similar services. In common usage, the term “audit” is used to refer to a range of services that do not meet the classification criteria for an audit in professional auditing standards. In one high-profile case, Google was required to have what was described in the FTC’s press release as a “privacy audit” (FTC 2011), and this term was discussed in the media, although the detailed report referred to itself as a “privacy assessment”. This chapter uses the general term *privacy audit* to include activities that may be considered (under formal definitions) assurance services or, sometimes, engagements to perform agreed upon procedures. Regulators in jurisdictions such as Ireland and Canada use the term “privacy audit” frequently. The Office of the Australian Information Commissioner (OAIC) refers to such reviews as “privacy performance assessments.” (OAIC 2011). The name is intended to reduce any negative associations with the word “audit” (ALRC 2008, 1584). Nevertheless, this

chapter will categorize these services as audits consistent with the broad definition that has been adopted and the discussion taking place in the news media.

In the chapter we suggest suitable criteria for privacy audits based on fundamental principles. These fundamental principles are identified from analysis of recommendations for legislative and/or policy reform by leading official bodies in the US and the EU (Toy 2013). We assess 30 publicly available privacy audit reports to examine the extent to which the fundamental principles are evident in the conduct of these audits. A fundamental principle is evident in a privacy audit report where the report states that it has assessed the activities of an organization against that principle, or against a concept that is readily translatable to the principle. In a number of the privacy audit reports we assess, national privacy laws are used as criteria for the audit. Some of the concepts within those laws can be readily translated to the fundamental principles. However, most of the standards contained in national laws, and some concepts that are termed “principles” in national laws are not similar enough to the fundamental principles to count as an application of those principles for the purposes of this study. We find that there is a large extent of divergence from the fundamental principles. However, there is some evidence of convergence of standards, particularly among more recent reports, and this is especially apparent in those reports produced by private organizations.

6.2: GENESIS OF PRIVACY AUDITS

Although it is a topical issue, privacy auditing has been in development for some time. It was identified as an area for potential growth for the auditing profession by the AICPA’s Special Committee on Assurance Services as long ago as 1997 (Elliott 1997, 67), and evidence has shown that “e-commerce companies adopt privacy-reporting standards and hire auditors to verify their compliance with these standards” (Jamal, Maier and Sunder 2003, 287). More

recently, privacy audits have become more widely used and more widely discussed in the areas of accounting, law, and information systems (Pavlou 2011, 985-986).

The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) have crafted what they have termed “Generally Accepted Privacy Principles” (GAPPs) (AICPA and CICA 2009). These principles appear to have had their genesis in early research by Gelinas, who was the first to investigate the possibility that accountants could perform privacy audits (Gelinas 1978, 113.). The modern GAPPs⁹⁶ are used in Service Organization Control Reports, also termed SOC 2 reports (AICPA 2012). However, the GAPPs are not generally used as standards for privacy audits.⁹⁷

6.2.1 TYPES OF PRIVACY AUDITS

Organizations that conduct privacy audits include both government-empowered regulators and private organizations with expertise in privacy auditing and assurance (e.g., accounting firms). A privacy audit is sometimes sought voluntarily due to a desire to enhance the public image of the organization (Nanos 2003, 3), and research suggests that organizations are more likely to have their privacy practices audited if they have previously breached privacy (Cortez and Hay 2014). However, it is more common for privacy audits to be conducted under mandatory powers of regulators.

⁹⁶ Recent GAPPs have not yet taken account of the latest proposals regarding privacy principles that stem from the US and the EU. The AICPA has made international comparisons regarding privacy principles (AICPA 2006), but this is based on existing laws such as the 1995 EU Directive, which would be overridden by the proposed EU Regulation (European Commission 2012). It also does not take account of the recent amendments to the Australian Privacy Act 1988 (Privacy Amendment (Enhancing Privacy Protection) Act 2012) (Cth).

⁹⁷ Of the 30 Privacy Audit reports examined in this chapter, only one specifically refers to the GAPPs: *Privacy Management Frameworks of Selected Federal Institutions* (Office of the Privacy Commissioner of Canada 2009c, 11). However, another refers to “Generally Accepted Privacy Practices”: *The Protection of Personal Information in Wireless Environments: An Examination of Selected Federal Institutions* (Office of the Privacy Commissioner of Canada 2010c, 13). In the context of the other Canadian reference, this may refer to the GAPPs, or it may refer to broader policy considerations.

Privacy audits include assurance engagements (which can be either reasonable assurance or limited assurance engagements), attestation engagements, direct reporting engagements, or engagements to carry out agreed-upon procedures. Assurance engagements under ISAE 3000⁹⁸ require certain criteria to be applied. The criteria applied in the engagement must exhibit the characteristics of relevance, completeness, reliability, neutrality and understandability. An example of a reasonable assurance attestation engagement is the Google privacy audit by PwC in the US. Google is required under the terms of a settlement with the Federal Trade Commission⁹⁹ to have biennial privacy audits during the 20 year period beginning 28 October 2011. The Google audit was an attestation engagement conducted by PwC, which examined compliance by Google with its own privacy program. This audit provided an opinion that attested to the assertion by the management of Google that Google's "privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information" (PwC 2012, 14). The decision by Google management to seek an attestation engagement rather than another more limited type of engagement could reflect the legal environment in different jurisdictions. The United States is able to enforce privacy through the circuitous route of preventing "unfair or deceptive acts or practices in or affecting commerce".¹⁰⁰ Non-compliance with a published privacy program has the potential for further action by the Federal Trade Commission.

Other privacy audits take the form of agreed-upon procedures engagements, such as the review of the New Zealand Accident Compensation Corporation (ACC). ACC is a government agency that provides personal accident insurance to New Zealanders. It holds a

⁹⁸ International Auditing and Assurance Standards Board (IAASB). 2013. *ISAE 3000, Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, para 24. Available at: <http://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga> (site accessed 4 June 2014).

⁹⁹ Agreement Containing Consent Order with a service date of October 28, 2011, between Google Inc and the Federal Trade Commission (US).

¹⁰⁰ Federal Trade Commission Act, s 5 (US). This applies at the federal level, as opposed to the state level where additional protections exist in varying degrees.

significant, and increasing, amount of personal information. The ACC engagement went beyond an assessment of New Zealand's applicable Privacy Act 1993, taking into account the latest policy developments in information privacy from other countries. The juxtaposition of the Google attestation examination and the ACC review demonstrates some interesting factors. Both of these engagements were done at the urging of regulators, but they were performed by private audit firms (PwC and KPMG respectively). Suitable criteria in the form of the fundamental principles of Consent, Transparency and Accountability were applied in both engagements. This demonstrates some degree of consensus on what privacy auditing requires, despite the fact that privacy laws in the United States and New Zealand differ significantly.

Agreed-upon procedures engagements often assess the extent of compliance by an organization with specific criteria, such as national privacy legislation. These types of engagements are assurance related, but they are not assurance engagements because "no assurance is expressed."¹⁰¹ The review by KPMG and IIS of the Accident Compensation Corporation in New Zealand is an example of this (KPMG and IIS 2012). Further examples include the Facebook Ireland Ltd audit (Office of the Data Protection Commissioner of Ireland 2011) and the audit of Data Protection in the Office of the Revenue Commissioners (Office of the Data Protection Commissioner of Ireland 2009).

Privacy audits are sometimes done in response to complaints to privacy commissioners, some of whom have the legal power to require an audit of an organization, or even to enter upon the premises of an organization to undertake such an audit.¹⁰² These are

¹⁰¹ International Auditing and Assurance Standards Board (IAASB). 2008. *ISRS 4400, International Standard on Related Services*, para 5. This standard specifically relates to procedures regarding financial information, but is relevant by analogy to privacy audits in circumstances where these are engagements to provide agreed-upon procedures. Available at: <http://www.ifac.org/sites/default/files/downloads/b015-2010-iaasb-handbook-isrs-4400.pdf> (site accessed 20 May 2014).

¹⁰² This is the case in Ireland, where sections 10(1A) and 24(2)(a),(b) of the Data Protection Acts 1988 & 2003 (Ireland) give the Data Protection Commissioner powers to arrive unannounced and to enter premises and to require information to be given to his authorised officers.

mandatory privacy audits, as the auditee organization must submit to an audit by the regulator. This situation may give rise to an agreed-upon procedures engagement, as was the case with Facebook Ireland Ltd (Office of the Data Protection Commissioner of Ireland 2011), or to a direct reporting engagement.¹⁰³

Direct engagements (previously called direct reporting engagements) offer an opinion based on the investigations of the auditor, in the absence of any assertion by management of the organization. Examples of this kind of privacy audit include the Audit of Veterans Affairs Canada and the audit of Staples Business Depot, both of which “followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants” (Office of the Privacy Commissioner of Canada 2012, 34; Office of the Privacy Commissioner of Canada 2011a, 23).

Regardless of the type of privacy audits in a given situation, all could benefit from the use of a standard set of principles because this would enable greater comparisons to be made between different audits. While it is useful to have different types of audits, use of the same principles of information privacy for all types of privacy audits would enable greater comparisons between different reports, and greater relevance in an environment that is marked by globalization. The principles suggested in this chapter are an example of how greater consistency could be achieved.

6.3: PRINCIPLES

Different audits draw on different sources of standards, such as national privacy laws or principles suggested by policy documents provided by auditee organizations or other

¹⁰³ Examples of this kind of privacy audit include the Audit of Veterans Affairs Canada and the audit of Staples Business Depot, both of which “followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants” (Office of the Privacy Commissioner of Canada 2012, 34; Office of the Privacy Commissioner of Canada 2011a, 23).

authoritative sources.¹⁰⁴ Where large differences between standards exist, reconciliation of the standards used in one privacy audit with those used in another audit is difficult, which reduces the potential utility of privacy audits across different countries. Lack of harmonization is therefore an impediment to privacy protection. A compelling argument has been made that this “circumstance offers an opportunity for U.S. technical leadership in privacy in the international arena, an opportunity that should be seized...” (President’s Council of Advisors on Science and Technology 2014, 52). Creating and adopting standards for privacy audits would go some way toward achievement of this goal.

6.3.1 FUNDAMENTAL PRINCIPLES FOR PRIVACY AUDITS

Information privacy has had the benefit of recent legislative reform and policy statements by official bodies such as the FTC. Incorporated within these suggestions are fundamental principles that are relevant to the latest challenges to information privacy. These will be referred to in this chapter as *international best practice*. For example, the principle of “Privacy by Design” has been suggested (FTC 2012, 22; European Commission 2012, 56). This principle is not found in existing national information privacy legislation in any of the countries in which audit reports have been examined in this chapter.

Development of a theoretical foundation for privacy audits could be productively grounded in the broader question of information privacy rights. If the basic information privacy rights of individuals can be established, a framework for privacy audits could emerge to verify whether such rights are respected or violated in any given privacy situation. A recent article proposes seven fundamental principles that could be used to constitute a theoretical framework for discussing information privacy rights (Toy 2013, 946). In this

¹⁰⁴ Policy documents include public reports by official bodies, e.g.: the principle of Privacy by Design has been suggested (FTC 2012, 22). Also included are privacy policies of companies subject to privacy audits, e.g.: the Google privacy audit refers to the principles in Google’s privacy program (PwC 2012, 17).

chapter we use this framework as a lens through which we view the publicly available privacy audit reports. These principles are based on recent suggestions by the US (The White House 2012; FTC 2012) and the EU (European Commission 2012) for legislative and policy reform regarding information privacy rights. These fundamental principles may then form suitable criteria for a privacy audit,¹⁰⁵ and could be supplemented by industry codes of conduct to give more specific guidance on practices in different industries (FTC 2012, 14).

The relationship between industry codes of conduct and fundamental principles is informed by the distinction between standards in the form of rules and those in the form of principles. The legal literature has defined principles as a type of standard having a dimension of “weight” compared to other principles that may “weigh” on an issue (Dworkin 1978, 26; Wustemann and Wustemann 2010, 14). Rules, on the other hand, are a type of standard that apply in an “all-or-nothing fashion” (Dworkin 1978, 24). This definition has been imported into the accounting literature, but not without a few changes. The industry codes of conduct contemplated by the FTC would be appropriate as rules to supplement the fundamental principles. However, the fundamental principles would still be useful even in the absence of industry codes of conduct. This is because the principles are applied at a higher conceptual level than rules. The substance of most of the GAPPs and much national information privacy legislation consists mainly of rules. The rules could benefit from the addition of the fundamental principles because they would add consistency and a conceptual basis.

There are seven principles proposed in an earlier chapter that provide coverage of the issues dealt with by other, more detailed principles in the legislation and proposals that make

¹⁰⁵ This chapter is focused on the distinguishing characteristics of privacy audits, as opposed to general auditing standards that may apply to different types of audit or assurance engagements. The principles used for privacy audits would not arise if there were no privacy audits, therefore these principles are privacy auditing principles, not general auditing principles.

up information privacy laws and standards in the relevant countries. The fundamental principles are:

- (a) Privacy by Design, which mandates that concern for privacy protections should be demonstrated at every stage of the development of a product or service;
- (b) Respect for Context, which governs dealings with data in accordance with limitations based on the context in which that data were initially supplied plus later indications if the use of the data has changed significantly;
- (c) Consent, which requires the input of the data subject to allow uses of their data;
- (d) Transparency, which allows a person to see what organizations are doing with their data, and requires that the organization repair inaccuracies in the data;
- (e) Legitimacy, which governs the appropriateness of dealings with data;
- (f) Proportionality, which controls both the extent of data that may be dealt with, and weighs the dealing against other principles of information privacy and of the general law to determine acceptable dealings;
- (g) Accountability, which ascribes responsibility for inappropriate dealings with data to the most appropriate parties having a hand in the dealing.

Evidence of application of suitable criteria in the form of these fundamental principles is found in some of the audit reports referred to in this chapter.

These principles can be supported by reference to recent privacy statements as shown in Table 2 at the end of this thesis. The European Commission's proposed Data Protection Regulation is consistent with the fundamental principles of Privacy by Design and Transparency and Legitimacy (European Commission 2012, Articles 5 and 23). The Federal Trade Commission (FTC 2012, 23) and the OECD (OECD 2011, 41) also advocate the principle of Privacy by Design.¹⁰⁶ The Obama Administration has signalled a basis for the principles of Respect for Context, Transparency and Accountability (The White House 2012, 10). The principle of Consent is supported in the form of Choice and Consent in the Generally Accepted Privacy Principles of the American Institute of Certified Public Accountants Inc. and Canadian Institute of Chartered Accountants (AICPA and CICA 2009, 7). Proportionality is founded in the case law of the European Court of Justice and the European Court of Human Rights (Toy 2013, 948-950).

The suitable criteria/fundamental principles of Consent, Transparency and Accountability (described in the Google audit report as, "meaningful choices", "transparent" and "responsible steward" PwC 2012, 17) were used as standards in the Google audit, just as they were in the Canadian audits that applied the principles in the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada). Those three principles are evident in both PIPEDA and the Google privacy program. This is evidence that some privacy audits are showing a degree of convergence that also coincides with international best

¹⁰⁶ The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have been updated in 2013, but the updated version does not incorporate the principle of privacy by design. Available at: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm> (site accessed 30 June 2014).

practice. Nevertheless, there is still wide divergence between the suitable criteria applied across most of the privacy audit reports discussed in this chapter.

6.3.2 PRIVACY AUDITS DISTINGUISHED FROM INFORMATION SECURITY AUDITS

Privacy audits are distinct from information security audits. Auditing security of information involves assessment of internal controls that protect information from unauthorized access.¹⁰⁷ However, even with a very high level of security, an organization may still breach privacy. For example, an organization may use customer information in a different and conflicting context from that in which it was disclosed. This information may never leave the organization, and security controls may never be relevant, but the organization may still breach privacy with this action. Information security audits are audits of systems and processes, as opposed to privacy audits, which are better described as compliance audits.¹⁰⁸ While IT auditors are able to conduct privacy audits (Singleton 2009, 1), a privacy audit remains distinct from an information security audit.

6.3.3 INTERNATIONAL REQUIREMENTS FOR ASSURANCE ENGAGEMENTS

Where criteria are not specified by national legislation, one of the biggest challenges in a privacy audit is to choose applicable criteria for the engagement. The *International Framework for Assurance Engagements* issued by the International Auditing and Assurance

¹⁰⁷ Privacy issues may, however, be relevant to information security audits, and ISACA (formerly known as the Information Systems Audit and Control Association) has recently announced selection of a new Privacy Task Force to identify privacy issues that may be relevant to this type of audit. This may fill a void left by the now withdrawn G31 Guideline on Privacy. Details of the new Privacy Task Force are available at: <http://www.isaca.org/About-ISACA/Press-room/News-Releases/2013/Pages/ISACA-Announces-Selection-of-New-Privacy-Task-Force.aspx> (site accessed 20 January 2014).

¹⁰⁸ An example of this is to determine to what extent an organization ‘complies with all or part of its Information Privacy Principle (IPP) obligations. As such, the OAIC’s approach to assessments draws heavily on compliance audit techniques...’ Office of the Australian Information Commissioner. 2011. *Privacy Performance Assessment Manual*.

Standards Board (IAASB) requires that criteria for an assurance engagement can “either be established or specifically developed”.¹⁰⁹ Established criteria would include national data protection laws or the GAPPs. Specifically developed criteria are developed for the particular engagement. An example would be the application of the principles in Google’s privacy program to the Google privacy audit. Established criteria may be applied in a privacy audit, but on top of these requirements may be laid further requirements that update the established criteria in the light of the latest international developments in information privacy. For example, suggestions from the US and the EU in 2012 may supplement the GAPPs or national data protection laws to shore up any principles that are lacking.

Privacy audits have been slow to develop, and they have not yet matured to the point where an underlying theoretical foundation has been fully developed. This lack of foundation has resulted in a lack of coherent direction for privacy audits. The framework of fundamental principles that we apply to privacy audits is useful to contrast the different approaches to privacy audits against each other. The benchmark we use for this is drawn from the latest suggestions for legislative and policy reform in the US and the EU.

6.4: ANALYSIS

The aim of our analysis is to determine to what extent the fundamental principles have been applied in existing privacy audit reports. Table 3 at the end of this thesis shows the application of suitable criteria for privacy audits based on fundamental principles and international best practice to 30 privacy audit reports. These are all of the publicly available privacy audit reports from countries that had significant publicity associated with their

¹⁰⁹ International Auditing and Assurance Standards Board (IAASB). *International Framework for Assurance Engagements*, para 46. 2013. Available at: <http://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga> (site accessed 4 June 2014).

privacy audits at the time of writing and they reflect the sample period of January 1, 2006 to January 1, 2013. Language barriers prevented the authors from examining all countries, while some countries, such as Hong Kong, Mexico and Singapore, did not have publicly available privacy audit reports.

We reviewed the 30 audit reports in conjunction with the fundamental principles. The process of coding the data involved an assessment of the statement within each audit report as to the standards used in the audit. This process was completed by the first author. Frequently (but in not all of the instances), the statement of standards referred to national privacy legislation. Where this occurred, an analysis was then undertaken of the national privacy legislation to determine its concurrence with fundamental principles as discussed above. It was then possible to ascertain which criteria had been used in the conduct of the audit. Where additional criteria were mentioned in the audit, beyond those in the particular national legislation, these were also considered applied in the audit. Where no national legislation was mentioned, the audit was reviewed to determine if some other set of criteria, such as the GAPPs, were used. All of the audit reports disclosed enough information to be able to ascertain the criteria that were used in each audit.

A particular fundamental principle was considered applied in a particular privacy audit if the audit assessed compliance against a criterion or criteria that were readily translatable¹¹⁰ to the principle. In this case, a “Yes” was recorded. Where a privacy audit report assessed compliance against a standard or standards that did not cover the full breadth and depth of a fundamental principle, a “No” was recorded. This classification included cases where a specific rule was referred to, rather than a fundamental principle. References to national legislation tended to result in “No” responses since much national legislation has

¹¹⁰ This term is used to mean that a suitable criterion/fundamental principle is substantially similar in content to a principle in national legislation or some other source of principles. For example: Australian Privacy Principle 1—open and transparent management of personal information. This readily translates to the suitable criterion/fundamental principle of Transparency.

statements of rules that fail to readily translate to the fundamental principles used in this chapter, however some national legislation does have statements of principle that are readily translated to the fundamental principles and this was accepted as a “Yes” result. A “No” was also recorded where standards used did not examine any part of a fundamental principle. The coding of the data was then reviewed by the second author. A level of agreement of 98.5% was achieved. The differences were discussed and resolved.

6.4.1 RESULTS

Among the audit reports, two applied four of the suitable fundamental privacy principles (Office of the Privacy Commissioner of Canada 2007; KPMG and IIS 2012). These audits took account of some international developments in privacy protection. Sixteen of the audit reports did not apply any of the fundamental privacy principles discussed above. This was due to their focus on national legislation as a set of standards. There may be legitimate reasons for the scope of these audits due to the legal mandate within a particular country to conduct a privacy audit, as mentioned below. The fundamental principles of Legitimacy and Respect for Context were not used as criteria in any of the audit reports. Although some standards, particularly national legislation, embody aspects of the fundamental principle of Respect for Context, the broad definition of this principle as a fundamental principle is not captured in its entirety by the national legislation in any of the countries from which audit reports were sourced.

6.4.2 PRACTICE IN PRIVACY AUDITS THAT ARE CONDUCTED BY REGULATORS

Some regulators, such as the Office of the Australian Information Commissioner (OAIC), have conducted privacy audits that focus on the extent of compliance by an organization with

local privacy laws.¹¹¹ To some extent, the approach of the OAIC accords with the legal regime in place in Australia,¹¹² which allows the OAIC to determine compliance by an organization with the Australian Privacy Principles (APPs).¹¹³ For the OAIC to apply standards drawn from international best practice in such an audit would arguably reach outside its mandate because the OAIC does not have the power to assess compliance against any standards other than the APPs. This restriction is echoed in some other countries, and as a result there are limits to the extent to which it is possible for privacy audits to be internationally consistent. For example, the legal powers of the Office of the Data Protection Commissioner of Ireland to conduct privacy audits are tied to the requirements of the Irish legislation.¹¹⁴ However, it is important to note that the proposed EU Regulation would require entities that hold personal information to “implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation” (European Commission 2012, Article 22(1)). This suggests that privacy audits in the EU may use the principles in the Regulation (should it be passed into law in this form) as a set of standards for the privacy audit. Those principles come close to the suitable criteria discussed in this chapter.

Other regulators have taken a different approach. The Privacy Commissioner of Canada has powers to audit under both the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada) and the Privacy Act (Canada). In general, PIPEDA applies to any organization in respect of its commercial activities,¹¹⁵ and gives the Canadian

¹¹¹ The Passenger Name Record data audit demonstrates this very narrow approach. This audit assessed compliance against the information privacy principles in s14 of the Privacy Act 1988 (Cth) (Office of the Australian Information Commissioner 2012).

¹¹² The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) has altered the Privacy Act 1988 (Cth) by introducing the 13 Australian Privacy Principles (APPs) which came into force in March 2014.

¹¹³ Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), s33C(1)(a)(i).

¹¹⁴ Specifically, s10(1)(a) of the Data Protection Act 1988 (Ireland) and the Data Protection (Amendment) Act 2003 (Ireland) gives the Data Protection Commissioner the power to investigate where the provisions of the legislation may have been contravened.

¹¹⁵ Personal Information Protection and Electronic Documents Act SC 2000 (Canada), s4(1)(a).

Privacy Commissioner the power to: “audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is... not following a recommendation set out in Schedule 1...”.¹¹⁶

It is apparent that this power does not require the audit to merely assess compliance against the 10 PIPEDA principles set out in Schedule 1. Instead, the power is to audit the “personal information management practices” of the organization. The breach by an organization of any of the PIPEDA principles triggers the power to audit, but does not constrain it. This audit power is broad enough in its scope to allow other criteria beyond the 10 principles specified in the legislation to be taken into account. International best practice could be included in such an audit without straining the wording or meaning of this statute.

The power to conduct audits of organizations under PIPEDA does not apply where the target institution is already subject to the Privacy Act (i.e.: government institutions).¹¹⁷ This means that the Canadian privacy audits that included both the requirements of the Privacy Act and the PIPEDA principles as relevant standards were truly attempting to take account of international best practice, as the PIPEDA principles cannot have been legally required if the audit was done under the authority of the Privacy Act. The inclusion of the 10 PIPEDA principles in some Canadian privacy audits¹¹⁸ may be seen as a step toward recognizing international best practice as a relevant set of standards, as some of these principles reflect international developments regarding information privacy. Three of the PIPEDA principles¹¹⁹ are translatable to emerging fundamental principles.

¹¹⁶ Ibid, s18(1).

¹¹⁷ Personal Information Protection and Electronic Documents Act SC 2000 (Canada), s4(2)(a).

¹¹⁸ Other audit reports that assessed compliance against sections 4-8 of the Privacy Act (Canada) and the 10 principles in PIPEDA include: Office of the Privacy Commissioner of Canada. 2008. *Privacy Audit of Canadian Passport Operations*. 32; and: Office of the Privacy Commissioner of Canada. 2009. *Financial Transactions and Reports Analysis Centre of Canada*. 33.

¹¹⁹ Personal Information Protection and Electronic Documents Act SC 2000 (Canada), Schedule 1.

One Canadian privacy audit has gone one step further in recognition of the requirements of international best practice. In 2007 the Canadian Privacy Commissioner audited a number of government institutions to determine their implementation of the Canadian Government's Policy on Privacy Impact Assessment. This policy required government institutions to engage in Privacy Impact Assessments (PIAs) that involve application of Sections 4 to 8 of the Canadian Privacy Act and the 10 PIPEDA principles (Office of the Privacy Commissioner of Canada 2007, 4). The audit criteria involved analysis of whether federal institutions were complying with those requirements and four additional criteria. Within these additional criteria can be found elements of developing international best practice that are not incorporated within either the Privacy Act or the PIPEDA criteria. For example, criterion 1(b) includes: "Initiation and definition of the scope of PIAs are completed in the early stages of the design or re-design of a program or service."¹²⁰ This criterion is an application of the principle of Privacy by Design, which is a fundamental principle (Toy 2013, 952). Furthermore, criterion 2 includes: "How does the PIA process in Canada compare to that of other jurisdictions (provincial and international)?" (Office of the Privacy Commissioner of Canada 2007, 29) This clearly incorporates international best practice as part of the privacy audit standards.

The second privacy audit of Facebook Ireland Ltd, conducted in the year following the first audit, mentions international best practice. The views of other data protection authorities were seen as relevant to this audit, and "[t]he fact that our recommendations were couched in terms of "best practice" rather than mere legal compliance facilitated such accommodation of other views" (Office of the Data Protection Commissioner of Ireland 2012, 3).

¹²⁰ Ibid, 29.

6.4.3 PRACTICE IN PRIVACY AUDITS THAT ARE CONDUCTED BY AUDITORS

Some privacy audits have been done by private independent auditors, such as the Big Four audit firms. This was the case with the audit of ACC which was done by KPMG and IIS. A privacy breach involving the personal information of 6,748 individuals became public in March 2012, and this led the ACC Board (in conjunction with the Office of the New Zealand Privacy Commissioner) to request an independent review of ACC's privacy practices. This audit took account of guidance from other privacy authorities, and "[d]raws on privacy best practice including the concept of Privacy by Design...." (KPMG and IIS 2012, 24).

In the US, the first Google privacy audit by PwC was completed in 2012. The audit assessed Google's activities against the 5 principles in Google's privacy policy (PwC 2012, 1-2.). Google operates internationally, and it is subject to information privacy laws in the countries in which it operates (Toy 2010). Google is also a member of the US Safe Harbor self-regulatory framework,¹²¹ and it must observe the principles in that framework. Examination of these issues could have been of use to Google, and to Google's customers. Three of the fundamental privacy principles (Consent, Transparency and Accountability) are translatable to principles in Google's privacy program, and they can therefore be considered applied as suitable criteria in the Google audit as Google's compliance with its own privacy program was examined by the auditor. However, application of the other suitable criteria/fundamental principles is not apparent in the Google audit.

6.4.4 DEGREE OF CONSISTENCY BETWEEN DIFFERENT TYPES OF PRIVACY AUDITS

Some privacy audits are beginning to reach toward international best practice, and this is best demonstrated with the audits by the Canadian Privacy Commissioner. It can also be seen in

¹²¹ Available at: <http://export.gov/safeharbor/> (site accessed 4 December 2013).

the privacy audits of Google and ACC. This shows an underlying desire to incorporate international developments, but fulfilment of this desire has generally not yet been achieved. While national privacy laws are always likely to lack harmonization, the latest policy developments in information privacy across different countries may be the source of more consistency among different countries.

6.5: CONCLUSION

Application of the suitable criteria for privacy auditing based on fundamental principles discussed in this chapter reveals that there has been significant divergence between standards used by different privacy audits. This has been particularly acute where the engagements are done by regulators, compared to private audit firms. This divergence includes cases where privacy audits use suitable criteria that are based on detailed provisions (sometimes described as principles) in national privacy laws.

There remains some convergence of privacy auditing standards however, and this has been the case even across different countries having different legal regimes. International best practice, in terms of policy developments regarding privacy, may be the source of more consistency among privacy audit reports. Convergence of privacy auditing standards may never fully occur, but to the extent that it does occur, it will improve the international comparability and relevance of privacy audits and their ability to provide assurance to organizations that operate internationally. It is important that privacy reports are comparable in order for users who are in many different jurisdictions to be able to find them relevant.

There are many research opportunities in the area of privacy auditing, and these will expand as more privacy audit and assurance reports become available. The underlying issue is whether privacy audits can be effective; and this breaks down into effectiveness of different types, including preventing or detecting breaches; and promoting the confidence of

users. This issue then leads on to whether effectiveness is best achieved by audits, or other forms of assurance, or other types of engagement; and whether these engagements should be mandatory or voluntary. Further issues including whether privacy assurance or other engagements should be done by private sector entities such as accounting firms, or by public sector agencies.

Future research questions that may be investigated regarding privacy audits could extend the work reported in this chapter to a wider range of countries, and to more voluntary privacy audits. At the present stage of privacy auditing, data availability is very limited. Empirical studies of the extent of privacy breaches and their relation to the company's awareness of privacy issues using proxy measures available in the annual reports may be a useful approach. Interviews with participants in privacy audits would also help to increase our understanding of issues such as who carries out these audits, what standards they apply, the outcomes of the audits and their value to users. Other questions that could be investigated as more data become available from greater use of privacy audits include the value of privacy audits measured by whether and to what extent privacy audits reduce the incidence of privacy breaches by measuring the incidence of privacy breaches before and after audits. The skills required, and training pathways, of those who would conduct privacy audits is another potential area for analysis. In the context of Big Data, "methods for auditing use in context and identifying violations of policy" have also been identified as areas requiring future research by the President's Council of Advisors on Science and Technology (2014, 51).

Research examining the effectiveness of privacy audits could then examine the differences in the effectiveness of various audit providers, including the Big 4 audit firms, other private sector providers and government agencies. Further issues include the extent to which stakeholders value privacy audits and their perceptions of them. These issues could be examined by behavioral experiments and surveys. Examining the views of service users who

have or have not been affected by a privacy breach would provide an interesting opportunity to examine the perceptions of users and their expectations. Audit methodologies and best practices could also be studied using behavioural experiments and surveys. This research could include analysis of how data protection authorities could synchronize their practices with those used by the accounting and auditing profession.

Another fruitful area for research involves examining the issue of whether more extensive regulation tends to increase or decrease the use of international best practice in privacy audits. The value of mandatory audits compared to voluntary audits has been studied in relation to audits of financial reports. Voluntary audits allow organizations to differentiate themselves through their decision whether to appoint an auditor (Lennox and Pittman 2011, 1665-1672). If this principle is applicable in the privacy sphere, then it may be appropriate for privacy audits to be voluntary rather than mandatory, and research questions could examine this issue.

Research opportunities also exist to examine the likelihood that an organization will seek a privacy audit. Analogies may be made with research in auditing financial statements. Research has shown that there are a number of factors that increase the likelihood that an organization will seek an audit of its financial statements. These factors include increasing loss of control (due to increasing hierarchical complexity of organizations) (Abdel-Khalik 1993, 49) and increasing organizational size (Chow 1982, 286). These factors may also affect the use of privacy audits. Insights could be gained by examining these issues through considering questions such as the determinants of voluntary privacy audits. The value to management of privacy assurance or other engagements could be investigated by looking at the levels of fees paid, and whether there are premiums for larger privacy audit providers or for industry specialists.

Privacy audit fees may also be investigated. Knechel and Willekens (2006, 1364) have shown that there is a complementary relationship between better corporate governance (such as the existence of audit committees, and independent board members) and increased resources spent on audits. However, their study also found that internal controls imposed on an organization by an exogenous regulator acted as a substitute for audits, and were not complementary to increased resources spent on audits. These questions might be examined in the context of privacy audits.

There are opportunities for studying the causes and effects of privacy breaches in other research methodologies as well. The market impact of privacy breaches, and privacy audit reports, can be examined using event studies.

There are also a wide range of other research opportunities in different cultures and different countries. These include the nature of privacy in countries that do not have institutions that protect the privacy rights of individuals, or where privacy is not regarded as important. In these cases, are privacy rights and privacy audits by Western entities such as Google and Facebook still regarded as important? And to what extent are there concerns about their domestic equivalent entities? These research questions and many others will be examined in future as more data becomes available.¹²²

¹²² The recent Target data breach in which credit card details of more than 70 million customers were stolen (Prah 2014) is an example of why this problem will continue to be important.

CHAPTER 7: STANDARDS AND METHODOLOGIES OF PRIVACY AUDITING AND DRIVERS OF THE PRACTICE

Alan Toy¹²³

7.1: INTRODUCTION

The FTC is the de facto privacy regulator in the United States (Solove and Hartzog 2014). It has regulated the conduct of important organizations such as Google, which is required¹²⁴ to have biennial privacy audits during the 20 year period beginning 28 October 2011. The first Google audit (PwC 2012) is a reasonable assurance attestation engagement, which examines compliance by Google with its published privacy program. But what is actually required when the FTC or other regulators require an organization to have a “privacy audit”?

This chapter aims to understand the motivating factors behind the standards and methodologies used by privacy auditors and how these factors translate into the practice of privacy auditing. Privacy auditing is mostly unexplored by academic research and little is known about the drivers of the practice of privacy auditing. This research helps to explain the current divergence of standards used by different privacy auditors and it suggests ways for privacy auditors to use more consistent standards.

Privacy audits are relatively new and they face challenges including the lack of a community of practice and the rapidly changing nature of technology. The view of some

¹²³ This chapter has formed the basis for a sole-authored conference paper entitled “Similarities and differences between the approaches of regulators and independent organisations to privacy audits” that the author presented at the 2015 conference of the Accounting and Finance Association of Australia and New Zealand (AFAANZ) in Hobart, Tasmania, on 7 July 2015. It has also formed the basis for a sole-authored conference paper entitled “Standards and Methodologies of Privacy Auditing and Drivers of the Practice” that the author presented at the 13th Australian National Centre for Audit and Assurance Research Research Forum 2015 (ANCAAR) in Canberra, ACT, on 4 December 2015.

¹²⁴ Agreement Containing Consent Order with a service date of October 28, 2011, between Google Inc and the Federal Trade Commission (US).

privacy auditors that privacy is an organizational issue provides a way to address both compliance with privacy laws and other privacy risks from social norms that may change more quickly than privacy laws themselves.

This research is based on 6 semi-structured interviews with privacy auditors and regulators and an analyst spread across Australia, Canada, New Zealand and the United States. This study is the first to document the views of privacy auditors regarding the standards and methodologies that they use. It also presents novel results regarding the drivers of the practice of privacy auditing and the interests of the beneficiaries of privacy audits. It builds on research that argues for the existence of best practices for privacy (Toy 2013; Toy and Hay 2015) and it extends this argument by providing reasons why privacy auditors may benefit from the use of best practices for privacy.

Existing research suggests that privacy audits suffer from divergence of standards (Toy and Hay 2015) and that privacy audits may be improved by the use of fundamental principles of information privacy as standards (Toy 2013). However, due to the nature of the data examined, the existing literature has not been able to do more than speculate as to the reasons why privacy auditing is the way it is. There is therefore a largely unexplored area in the literature regarding the drivers of the current practice of privacy auditing.

This research is important due to the growing importance of privacy audits to the accounting and auditing professions and the relative scarcity of privacy auditing studies in the accounting literature. The results of the interviews demonstrate that privacy audits face significant challenges such as the lack of a privacy auditing profession and the difficulty of raising the awareness of organizations and individuals regarding information privacy rights and duties.

7.2: LITERATURE REVIEW

Jamal, Maier and Sunder (2005) argue that information privacy rights should be embodied in general principles that reflect social norms (as opposed to laws that might be inconsistent with these norms). The results of the interviews in this chapter suggest that their argument is theoretically the correct approach but that it may take some time for this goal to be achieved. The results and theory from Toy and Hay (2015) and Toy (2013) are extended by this research which provides greater depth to privacy auditing issues and allows examination of the drivers of privacy auditing which has not previously been possible given the data used in existing studies.

Smith, Dinev and Xu (2011) suggest that more research is needed on the international dimensions of privacy and that empirical studies would be a good way to achieve a greater understanding of the issues. The research in this chapter addresses that call because this is empirical research and it has a focus on international issues affecting privacy audits. Gelinas (1978) suggests that there should be Generally Accepted Privacy Principles and this supports the argument in Toy and Hay (2015) that fundamental principles could be used to improve privacy audits. Despite the possibility of convergence of standards in the future however, the interviews detailed in this chapter demonstrate that there could be significant challenges in reaching this goal and that currently there are no accepted standards for privacy audits.

Elliott (1997) suggests that accountants have a strong auditing tradition, and assurance practitioners from accounting backgrounds may lead multidisciplinary teams where necessary to undertake assurance engagements (Huggins et al. 2011). There have also been calls for further research in areas outside audits of financial statements (such as CSR), which may lack the mathematical and systems rigor associated with double-entry accounting and “this is an area where qualitative research can be useful in conducting interviews and case studies as to how assurance providers cope with this loss of seemingly objective analysis” (Cohen and

Simnett 2015, 66). This suggestion would appear to apply with equal force to privacy assurance services.

7.3: DATA ANALYSIS

Thematic analysis is used in this thesis due to its capacity to provide insights into the complex themes arising from interview data. It has been suggested that “[t]hematic analysis is a method for identifying, analysing and reporting patterns (themes) within data. It minimally organizes and describes your data set in (rich) detail. However, frequently i[t] goes further than this, and interprets various aspects of the research topic” (Braun and Clarke 2006, 79). This is a useful method when “investigating an under-researched area, or... working with participants whose views on the topic are not known” (Braun and Clarke 2006, 83). This is appropriate to the study of privacy auditing because there is very little existing research on the topic and the views of participants are therefore not known in advance. Other methods of analysis look at just one theme in isolation, perhaps related to a single research question. Thematic analysis is useful for this thesis because this is a very new area of research, and the literature contains little guidance on themes that could arise. Flexibility is therefore an important attribute of the chosen method.

The themes identified in this chapter are those from the entire data corpus, and are not limited to some particular aspects. They are not limited to the research questions although the research questions are considered wherever possible. Themes relating to the entire data set are identified. It has been suggested that: “Through its theoretical freedom, thematic analysis provides a flexible and useful research tool, which can potentially provide a rich and detailed, yet complex, account of data.” (Braun and Clarke 2006, 78).

Coding is done manually, which is the alternative to using computer software to assist with the process (Braun and Clarke 2006, 89). The relative novelty of the research topic and

the absence of guidance on what themes might be found from the data mean that it is important for the author to get as close to the data as possible. Computer software may be of assistance where the interview data corpus is very large but that is not the case with this research topic. The author works through the entire corpus of data to extract the first codes. Each item of data is given equal attention, and there is no exclusion of items based on any perceived relevance or lack of relevance to the research questions. The codes are identified by extracting the meaning of each sentence of the interview data. There are several coding exercises. There is no limit placed on the number of codes identified – all codes that can be identified are included in the coding exercise. There is no limit to the number of sentences that can relate to one code, and one sentence can have more than one code. Generally, if a paragraph of sentences has just one code in it, it is coded once. However, if there is a break in focus within one paragraph, then a code is identified again if an interviewee returns to it later in the same paragraph. Collation of text relating to codes is then conducted. This involves taking extracts of the text of the interviews and collecting them together so that each code is now supported by text from various sources. Sometimes codes are supported by statements in the interviews, and sometimes statements go against these codes. There is therefore some contradiction in the data. Where this occurs, the statements supporting the code are collated under that code, and the statements that do not support it are also collated under that code, to enable a balanced final analysis.

Each code represents a distinct idea relating to privacy auditing. Interview data is allocated to these codes so that extracts from each interview that are relevant to each code are placed under a heading for that code. This enables the issues to be analysed more clearly. The author's own statements in interviews are not coded. Also, some text in interviews is not coded because it is simply irrelevant to the research. This includes housekeeping matters relating to the interviews. After the initial allocation of interview text to the codes, a second

analysis is done. This is a check to determine if any of the codes should be merged with other codes. This would only occur if there are insufficient differences in the interview text relating to one code compared to that relating to another code. Some codes are merged with each other at this stage.

The author identifies 30 codes in the initial analysis. At the conclusion of the second analysis, 10 codes remain. These are the distinct themes that exist in the data. As an incidental step at this stage, 4 of the codes are renamed to better reflect the interview data that relates to them. Table 4 and Figure 1 at the end of this thesis detail the coding scheme, showing the 30 initial codes, and the 10 final codes. Some codes are not merged with others. They are already correctly identified as distinct themes. These codes are directly elevated to the status of themes. There are 6 of these codes that directly translate into themes. The remaining 4 themes are codes that are renamed. This gives a total of 10 themes. The definitions of each of these 10 themes are presented in Table 5, along with examples of interview text that is allocated to the themes. All other codes prove to be merely subsets or instances of these 10 themes. The other codes are therefore merged (ie: subsumed) into these 10 themes. There are 34 boxes in the diagram (apart from the overall 'Themes' box). There would have been 30, except that 4 codes were renamed. Where this occurs, it is represented in the diagram as the old name of that code being merged into the new code. The limitations of the diagram mean that this is the best way to represent the renaming. The reason for the renaming is that some codes are initially incorrectly named. For example, the 'focus of national regulators' code contains text that relates more to the methodologies that national regulators see as appropriate for privacy audits, so it is more appropriately subsumed within 'privacy audit methodologies'.

After the second codes are determined, relevant extracts from the interview data are allocated to the code/theme headings. Because some codes are now merged, this results in

some overlap (some text is now redundant because it now exists twice or more under one code). Any text overlap is removed.

This chapter examines the practices of different privacy auditors by comparing the similarities and differences between them. It also uncovers drivers of standards and methodologies for privacy auditing. It is therefore necessary to investigate the standards and methodologies used by privacy auditors as well as who the beneficiaries are and the efficacy of the current practice of privacy auditing in serving the interests of the beneficiaries.

The research questions are:

1. What auditing standards and/or methodologies are used for privacy audits, where are they derived from, and how much convergence and/or divergence is there among standards used by different auditors?
2. Who benefits from privacy audits and are privacy audits an appropriate way to provide benefits to them?

The 10 themes address the research questions and they add to understanding of the practice of privacy auditing. Theme one addresses part of the first research question. It demonstrates that harmonization of privacy auditing standards may be difficult but desirable. The suggestion in this thesis is that fundamental principles supplemented by industry codes of conduct may be a possible path for this. Theme two discusses the definition of privacy audits and this is essential for understanding privacy audits because they have not been well defined in the past. Theme three discusses standards and methodologies for privacy auditing and this directly addresses the first research question. It also reveals differences between the practices of regulators and private auditors. Theme four reveals that privacy auditing is about more than just compliance with privacy laws. Some auditors see privacy as an organizational issue and this is consistent with the suggestions for fundamental principles advanced in this thesis. Theme five examines the skills of privacy auditors and it finds that there is a lack of training

and certification available which may present problems for both the auditors themselves and employers. Theme six investigates the Privacy Maturity Assessment Framework. This is an assessment tool for classifying organizations in terms of their understanding of privacy. It is interesting because it goes beyond mere compliance with information privacy laws and includes other criteria such as the principle of Privacy by Design (which is suggested as a fundamental principle by this thesis). Theme seven addresses the second research question by detailing the beneficiaries of privacy audits and the usefulness of privacy audits to them. Theme eight examines internal privacy audits and risk management by an organization and it therefore supplements the themes that address the first research question. Theme nine explores the impetus for privacy audits which may affect standards used in the audit and it therefore assists with answering the first research question. Theme ten discusses Privacy Impact Assessments and these are consistent with the fundamental principle of Privacy by Design that is advanced as a fundamental principle in this thesis.

7.4: THEME ONE: HARMONIZATION OF STANDARDS

The first theme is the issue of harmonization of privacy auditing standards. This is central to the research in this thesis because the question whether or not privacy auditors are using similar standards to each other impacts on the utility of privacy audits to stakeholders. It is argued that harmonization of privacy auditing standards would enhance privacy audits, but may be difficult to achieve. It is suggested that privacy auditors are a long way away from harmonizing the standards that they use, but that there is limited evidence of harmonization even among privacy auditors who operate in different countries having different legal systems (Toy and Hay 2015). While harmonization of standards is currently not usual, harmonization would be of assistance to users of privacy audits such as consumers who may be in different countries from that in which the audit took place. These users may derive more

benefit from a privacy audit that is subject to the same standards as privacy audits undertaken in their own country. Conversely, privacy audits done under markedly different criteria may be of limited use to users. For example, PwC stated in the Google privacy audit that “[w]e are not responsible for Google’s interpretation of or compliance with privacy-related laws, statutes and regulations applicable to Google in the jurisdictions within which Google operates.” (PwC 2012, 14). This statement reduces the utility of the Google privacy audit to consumers in all countries because they cannot rely on any assurance that Google is in compliance with any privacy laws at all. Nevertheless, there are aspects of the Google audit that are translatable to some of the fundamental principles discussed in Toy and Hay (2015), and this means that fundamental principles may provide a solution to the tricky issue of harmonization of privacy audit standards across different countries.

The weight of evidence from the interviews supports the view that harmonization would be a good thing for privacy audits but that it would be difficult to achieve with respect to substantive privacy standards, though it may be easier to achieve with respect to investigative audit standards. This supports the findings in Toy and Hay (2015) which demonstrate the lack of harmonization among standards. It also demonstrates that the argument in favour of fundamental principles from Toy (2013) is sound in its objectives.

Jay Fedorak (Regulator, Canada): *...you probably get a greater level of consistency around the methodology given that the privacy rules might be different, but even so, a lot of the privacy rules, for the most part, are going to be similar, so you’ll probably be able to develop some level of consistency there, but you probably get a greater level of it with respect to the methodology.*

The evidence shows that regulators have a greater focus on compliance with legislation in their own particular jurisdictions. This supports the results in Toy and Hay (2015) which demonstrate large differences between standards applied by regulators and other auditors. This is consistent with the general approach of regulators which gives greater importance to the legislative requirements in an individual jurisdiction than the approach taken by some of the non-regulator privacy auditors does.

However, some regulators are cautiously supportive of attempts to develop international standards, so long as differences in national legislation are recognised. The argument in favour of fundamental principles in Toy (2013) is consistent with this because it would allow different rules to be developed in different countries.

Jay Fedorak (Regulator, Canada): *personally, I can see a lot of value in working with international partners and sharing experience and trying to derive levels of consistency... and so I would say on a whole that we are, would be in general supportive of trying to develop sort of a consistent international approach, though recognizing that there are differences in legislation which might give some jurisdictions the scope to be able to do some things that the other jurisdictions can't.*

While it may be difficult to arrive at international standards that are specific enough to be applied in an audit, an international standard could be a starting point from which more detailed rules could be developed in a particular country. This is consistent with the argument in favour of industry codes of conduct that has been advanced in chapter 6 of this thesis (Toy and Hay 2015).

Neil Sanson (Regulator, New Zealand): *I think that any standard that could be applied across the different jurisdictions and cultures would of necessity be very high level, not something that you could directly use in an audit. It would be, as I said, a starting point which you would then have to expand based on the legal requirements in the jurisdiction you're covering. But it would hopefully keep the audit from focusing purely on the legislative requirements. One of the risks is that you look just at the legislation and say: "ok, we'll audit against the legislation". Doing basically a compliance audit. Hopefully, if you bear in mind either the OECD privacy principles, or an international standard that's at that similar high level, an auditor will look beyond simple compliance with the law and look at what is desirable from a privacy perspective, and assess how far the organization... what the organization can do to meet as far as it can that ideal.*

Privacy laws are often out of date due to rapid changes in technology. However, this thesis argues that an approach based on fundamental principles would enable a more enduring model. Industry codes based in these fundamental principles could be updated more frequently to deal with changes in technology, while the principles could last for a longer period than the rules currently enacted in information privacy legislation.

Marty Abrams (Analyst, United States): *... privacy laws are always dysfunctional. There's just no way around it. And they're dysfunctional because they're trying to anticipate what the information processing world will be like at some future point in time and we're not very good at that.*

Apart from privacy laws within different countries, there are currently no agreed standards that are used for privacy audits. This thesis suggests that the use of privacy laws alone as

standards may not be the best thing for a privacy audit because it would result in fragmentation of approaches across different countries. This is consistent with the findings in Toy and Hay (2015). It also indicates that the argument in favour of fundamental principles that could underlie the practice of privacy auditing is stronger (Toy 2013).

Different privacy auditors approach privacy audits differently, mainly because standards don't exist. Some legislation is not specific enough to produce a standard approach (privacy auditors may interpret legislation differently in terms of what it requires, and much privacy legislation is not specific enough to provide a standard approach).

Souella Cumming (Private Auditor, New Zealand): *Because, at the moment, in the absence of standards then, you know, KPMG's approach to it will be different from Deloitte or EY or PriceWaterhouseCoopers or IIS.¹²⁵ You know, so, because we will, you know, we'll do the same high level things in terms of look at the legislation, and... but there's nothing to say that, you know: this is the standard that, in complying with this piece of the legislation, this is what we would expect to see in place. So we'll all interpret that differently and therefore, you know, look for different sorts of evidence and conclude against that. So our assessment of one organization might be different from if Deloitte came in and did the same assessment because the standards don't exist.*

Older standards are not sophisticated enough to deal with current issues such as the concept of proportionality. This is also consistent with the argument in Toy (2013) that the latest fundamental principles are more up to date than the older standards such as those produced by APEC and the OECD. This thesis argues that privacy audits would be enhanced by the use

¹²⁵ Information Integrity Solutions Pty Ltd (IIS) is an Australian registered company that provides privacy and other services in different countries.

of fundamental principles as an underlying theory (which may include the fundamental principle of proportionality). This would enable greater consistency between standards in different countries.

ISO (International Standards Organization) standards may have potential for being a global standard in this area, but not all of the interviewees were in favour of ISO standards. ISO standards may be one way to implement the fundamental principles discussed in this thesis but they are not the only way. It is possible to use the jurisprudential arguments discussed in chapter 5 to ascertain the fundamental principles beneath existing information privacy laws. While this obviates the need for amendments to legislation or international standards, those who take a positivist approach to the law would still see formal standards as necessary.

There needs to be flexibility in privacy audit standards because of the great variety of companies being audited. This is because there are differences in the ways that auditee companies deal with data, which are greater than the differences between the ways that different companies treat, say, financial information. The argument in favour of fundamental principles in Toy (2013) would meet this requirement for flexibility. Principles are more flexible than standards in the form of rules. This is why they can be used in different countries, even though rules for specific industries may also be useful (Toy and Hay 2015). Privacy audits may follow a Socratic methodology (asking questions) which may involve a different process for each different organization. This may be necessary because of lack of conformity in the way that data is treated by different organizations.

Malcolm Crompton (Private Auditor, Australia): *One of the ways in which we have conducted some of these audits has actually been almost Socratic of simply following the nose. Each company's going about these issues in such different ways that you really have to*

approach it from where they're coming from... So [you] have to have some start points but you have to be flexible...

Privacy auditors face a major challenge which is that this is a new area and therefore there is a lack of experience to guide the practice. As privacy audits develop, privacy auditors may be able to implement more sophisticated approaches.

Souella Cumming (Private Auditor, New Zealand): *So this whole area, and I'm sure your research is showing this as well, it's well... the Privacy Act has been in place in New Zealand for twenty years... it's not a very mature market at all, in fact I think it's still very much at that developing stage. And so there's not an audit manual that you can buy about how to audit privacy essentially at this stage so...*

This thesis argues that use of fundamental principles for privacy auditing (Toy and Hay 2015) may assist to develop privacy audits. The current divergence of standards used by different privacy auditors is a natural result of the lack of maturity of the practice of privacy auditing. The use of fundamental principles would assist privacy auditors to develop privacy auditing into a more mature service.

It may be that information privacy has not yet reached the maturity to have harmonized standards. However, with technology as a driver, pressure may increase to develop global standards (for example: data is now being stored offshore in the cloud, and many entities now have customers in different countries).

7.4.1 SUMMARY OF THEME ONE

Harmonization of privacy auditing standards is a valid aspiration. Technology as a driver makes harmonization more important than it has been in the past. Provided they are specific enough, harmonized standards would keep auditors from merely focusing on the requirements of legislation as standards for a privacy audit.

However, harmonization of privacy auditing standards may be seen as more of an aspiration than a readily achievable goal. While harmonization is theoretically the correct approach, the fast moving nature of changes in technology and the differences between national privacy laws present formidable obstacles. Nevertheless, the aspiration is important because without continuous improvement, privacy audits may fail to achieve their objectives.

This thesis argues that use of fundamental principles of information privacy for privacy audits may provide a way for different privacy auditors to be able to come to grips with some of the challenges facing privacy audits. It may also reduce some of the differences between the approaches of regulatory organizations to privacy audits compared to the approaches that are taken by private auditors.

Gelinas suggests a set of principles for privacy auditing (Gelinas 1978) and this thesis suggests a different set of principles. The principles suggested in this thesis are more up to date with the latest developments in information privacy best practice. Two of Gelinas' suggested principles are translatable to the principles suggested in this thesis (Gelinas' principles of Accountability and Openness are translatable to the fundamental principles of Accountability and Transparency). The need for fundamental principles is therefore apparent from the very beginning of research on privacy audits.

Bortiz and No suggest that research is needed on the extent to which different standards for information privacy (such as the Generally Accepted Privacy Principles and the OECD Guidelines and the Fair Information Practices) can be compared to each other (Bortiz

and No 2011) and this theme examines how such comparisons may be useful for the practice of privacy auditing. This thesis argues that the myriad of different standards could be replaced by a set of fundamental principles that could justify approaches to privacy auditing taken in multiple different countries (Toy and Hay 2015).

This theme addresses both the first part and the second part of the first research question. It investigates the standards that are currently being used by privacy auditors and it finds that there are no accepted standards for privacy auditing. It shows that there is considerable divergence between the standards used by different privacy auditors. While complete harmonization is unlikely to occur, more convergence would be helpful to privacy auditors and this thesis suggests ways for that to be achieved through use of fundamental principles for privacy audits.

7.5: THEME TWO: DEFINITION OF PRIVACY AUDITS

The second theme is the issue of what is the proper definition of a privacy audit. This is essential to this thesis because methodologies and standards cannot be sensibly discussed otherwise. There are a wide range of services that are sometimes termed privacy audits. This may be due to the lack of maturity of the service, and has the result that privacy audits do not have a single universally agreed definition. A broad definition is used in this thesis because there is currently no basis for rejecting any particular definition. There are a wide range of services that may currently fall under a very broad definition of privacy audits. Toy and Hay (2015) argue that all types of services that may fall under the broad definition of privacy audits would be enhanced by the use of fundamental principles.

Souella Cumming (Private Auditor, New Zealand): ... *one of the dilemmas, and you talked about right at the outset is: like the word audit is, you know, misused or abused, you know,*

and it can mean anything from a review to, you know, a full audit, but a full audit needs to be an audit against legislation or an audit against standards, or an audit against something else. So the reader of an audit report needs to understand the limitations of those and they're not always clear in some of the audit reports that have been done...

Terminology for privacy audits is very important. Some interviewees are careful to avoid use of the term 'audit' as this may have negative connotations and may tend to make auditees reluctant to be subject to them. On the other hand, having a tightly defined term for privacy audits may hamper flexibility in the practice of privacy auditing. The ability of privacy auditors to benefit from flexibility in approach and focus could be constrained if the term is given a hard and fast definition. This is consistent with theme 1 (above), which argues that flexibility is required in privacy audits. The fundamental principles suggested in Toy (2013) would be flexible enough to be able to apply to different types of privacy audits.

Neil Sanson (Regulator, New Zealand): *You say "audit" and "privacy" are not well defined, and that's a problem, but also, in a way, that's quite useful in that it gives the flexibility to choose the approach and focus that is most likely to be useful to a particular organization and... while addressing a particular concern. You've got great flexibility there to hone in on where they can perhaps make the most improvement for, as a first step in improving... So a privacy audit, I could quite see the potential for the first privacy audit of an organization to perhaps be fairly general, or to focus on a particular area of business. But then a subsequent audit might have quite a different focus. They would still be both privacy audits. But you... often it would be too difficult to cover it all in one go.*

Different levels of assurance¹²⁶ might be appropriate for different types of organizations. Larger organizations with the potential to control the data of a large segment of the population base of a country would need a more in-depth audit. Each organization should have primary responsibility for determining the type of assurance that best suits its needs. But where the risks are very large, for example the personal information involved relates to a very large group of people in a society, the organization's ability to choose what type of assurance it needs might be restricted or limited.

Privacy audits could be done under an organization's internal audit function, or externally. If a privacy audit is done externally, it could be done by a regulatory authority or by a private organization such as one of the Big Four audit firms. Toy and Hay (2015) find large differences between the standards used by different privacy auditors, with the largest differences existing between regulatory authorities, who tend to focus on the requirements of their own legislation, and private organizations (who may be multinational) who have a broader focus.

Clients want a range of services relating to privacy, and private audit firms respond by offering a range of services including Privacy Impact Assessments, Privacy Health Checks, assessments against a Privacy Maturity Assessment Framework and full Privacy Audits. All of these services may be considered to be privacy audits under a broad definition, such as that adopted in Toy and Hay (2015).

Privacy audits are part of larger accountability processes within organizations. If an audit is done in isolation of management processes that act upon it, it is of little value. An audit is part of a sequence that begins with the principle of privacy by design (Toy 2013) and privacy impact assessments (these will be explained below under a separate code), then flows to audit.

¹²⁶ Audits are one level of assurance and are the highest level.

Privacy audits are offered by Big Four professional services firms using teams that include experienced auditors and privacy specialists. This increases the broad focus of the private auditors because they use specialists with different backgrounds to conduct their audits. Some regulators, such as the Office of the Information and Privacy Commissioner for British Columbia, also use auditors as well as privacy specialists.

Souella Cumming (Private Auditor, New Zealand): *And most organizations, in terms of the professional services firms' way that we approach it is that we would have a team of people who are experienced auditors, and then we'll get a subject matter specialist to do the privacy aspect of it or the, you know, focus on those particular areas.*

7.5.1 SUMMARY OF THEME TWO

Privacy audits are broadly defined in this thesis. This is partially due to the fact that they are not yet well developed. The term 'audit' may not be a necessary part of the definition of some services that could fall within such a broad definition. However, the fundamental principles could apply with equal effectiveness to all types of services that fall within the broad definition so there is no necessity in this thesis to further separate the services.

Flexibility is an important aspect of privacy audits and this fits with the flexibility offered by the fundamental principles. Large differences between the ways in which auditee organizations treat customer data require that privacy auditors are able to adjust the audit model to these different contexts.

There should be some limited ability for an organization to choose the type of privacy audit that it should be subject to. However this should not grant total freedom because some organizations that control data of a large segment of the population base are subject to larger

risks regarding information privacy and the privacy audits that are conducted in regards to these organizations should be of a sufficient standard to assess these risks.

This theme does not directly address the research questions, but it is necessary for this thesis because it is important to first define privacy audits before any further analysis can be undertaken. However, it does have relevance to the first research question because the definition of a particular privacy audit will have important implications for the standards and methodologies that are used in it. This theme finds that flexibility is currently part of the definition of privacy audits and that this is not necessarily a bad thing. The argument in this thesis that fundamental principles should be used for privacy audits would mesh seamlessly with this issue of flexibility because the fundamental principles are more flexible than standards in the form of rules.

7.6: THEME THREE: PRIVACY AUDIT STANDARDS AND METHODOLOGIES

The third theme is the issue of what methodologies are being used to investigate adherence to the standards used in privacy audits. This is important because the use of methodologies may be similar or divergent among different privacy auditors and this may point to differences in the quality of privacy audits. Due to the relative novelty of the service, privacy auditors have little previous practice to build upon when conducting a privacy audit. The result is a significant divergence of standards used in such audits (Toy and Hay 2015). It is reasonable to expect that this divergence of standards means that some privacy audits may be of lesser quality than if consistent standards are accepted by the privacy auditing community. The quality of privacy audits may be improved by having consistent standards.

Privacy audit methodologies differ depending on the type of privacy audit. Audits might not examine the whole organization at once. A privacy auditor may examine just one area of the organization at a time, as part of a process of continuous audits. However, audits

may also be one-off investigations that examine the whole organization. Privacy audits may be limited to particular data flows of classes of data across the organization (such as the data relating to a particular group of consumers) and/or they may examine particular areas of a business or particular systems within an organization.

Privacy audits may have benefits to organizations that are greater than just the audit report. For example, staff may benefit from the realization that there is a review process, allowing them to step back and reflect on their practices. These benefits may result in efficiencies, which may go some way toward mitigating the cost of the audit. Also, privacy audits may be an effective way of bringing concerns to the attention of senior management because privacy issues may not be visible to them otherwise.

The behaviour of staff within an organization may change due to the fact that a privacy audit has been announced. This is because the fact of the audit is a signal that management is interested in that particular aspect of the business, and staff may therefore be more concerned to ensure that their actions are correct. The way that management handles the announcement of a privacy audit may determine whether this change has a positive or negative effect on the organization.

Privacy audits may be followed by action by the auditee organization to address the recommendations in the privacy audit report, but this is not always the case, particularly because privacy audits are not yet well developed. The auditee organization may provide a list of responses or actions taken in relation to each recommendation, but most privacy auditee organizations do not do this yet.

Malcolm Crompton (Private Auditor, Australia): *Oh, absolutely. Sometimes the [organisation resists making any change], and at other times the organisation will come on board and say yep, thank you very much indeed, we'll get along with doing that. In particular with regard to*

government audits, quite often we see, in the public audit report, a list of the recommendations by the auditor and then a list of responses or comments or follow up action taken by the organization in response to that report. Again, unlike financial information governance reporting or other forms of performance reporting that are more mature, the privacy health check or auditing process generally hasn't reached that point. [Where there] is a report back.

Privacy audit methodologies by private auditors may require the auditee organization to produce documents that detail its understanding of privacy issues and implementation of these in its privacy management practices. Some auditee organizations are already in a position to provide these documents, but others may be taken by surprise because they may not have ever considered privacy issues or implemented any substantive privacy management practices.

Privacy auditors may also conduct interviews with relevant staff members of the auditee organization. These relevant staff members include more than just the privacy compliance team within an organization, and more than just the ICT team members. The privacy auditor should interview members of staff who are involved across the business, including the customer-facing staff members. This is because some privacy auditors see privacy as an organizational issue, not just the responsibility of the privacy compliance team or some other disparate unit within the organization. Privacy as an organizational issue includes all the staff within the organization having responsibility for the privacy management processes within the organization. This is consistent with the suggestion that fundamental principles should be used in more privacy audits (Toy and Hay 2015) because privacy is more than merely a compliance issue. Privacy as an organizational issue reflects

the understanding of the organization of a whole as to the privacy issues that are relevant to it and its customers.

There is also an iterative process which involves the privacy auditor forming some initial conclusions, then seeking feedback from the organization before refining those conclusions. This process can be repeated, and is often more in-depth than is the case for a financial audit.

Malcolm Crompton (Private Auditor, Australia): *it's a pretty simple methodology, Alan, and it's really got probably three strands to it if you think about it. One of them is on the basis you are asking the organization to give you to the best of its ability papers that will demonstrate what it thinks it's doing. That's in terms of personal information holdings that they have. You know, you're just dealing with employee information, are you dealing with client, customer or citizen information. Are you dealing with sensitive information as defined in law or as perceived by the public? Trying to get as much information on the papers as you can. And that really varies hugely across companies. Sometimes that's highly informative and sometimes it's probably the first time the company's been asked those questions from a privacy perspective. And then the second thing that may be happening at the same time is the parallel process or as a serial process after having a first look at the papers is a series of interviews with relevant people where you're trying to speak to people who are if you like the business or delivery end so you're not just trying to deal with the people who are the privacy compliance officers. You're not trying to deal with just the people who do the ICT platforms. You're actually trying also to deal with the people who are delivering the business product or services of that company or organization as well. So that's your third leg, sorry, your second leg. Then after that we will do some iterative process that says: on the basis of what we've seen so far, this is what we think. And that of itself is often quite a lengthy process, again*

because privacy is often in the eye of the beholder. It's very hard to get it right the first time round including where you're dealing with an organization that hasn't had to think about privacy very much before. So you actually have to go back and say this is what you're seeing, get back some response and then refine and re-write so some of that's like an audit cycle as it is, but the iterative process is probably [richer] than you may see in a pure financial audit.

Privacy audits examine more than just the risks of an organization. Governance and accountability processes are also an important aspect of a privacy audit. The ACC privacy audit implements an approach that involves a cycle starting with the board of directors and the leadership of the organization, then moving to the privacy program and accountability processes. While privacy risks are relevant, they are not the sole avenue of investigation during a privacy audit.

When investigating hard files such as documents, privacy audits may use methods of auditing that are very similar to financial statement auditing. However, privacy audits have some important differences from financial statement auditing. These include the use of site inspections as well as interviews with staff.

Tanya Allen (Regulator, Canada): *I think it would be a bit of a blend... when we're dealing with the actual hard files, you can use the accounting standards, but I think, for our audits, they would sit on more a different [format on the privacy audit side], where we will rely a lot on site inspection as well as interviews with staff in the agency.... Asking questions of the staff: When's the last time that they had taken privacy training? And [other questions] we could ask... that I don't think the accounting standards generally allow for that to be submitted as evidence.*

Privacy audits collect information in the same way as large research projects. This includes background information collection about the auditee organization. It also includes an assessment of the structure of that organization and the kinds of personal information that it collects and how it deals with this information. Information may also be collected from reviews of files and site inspections as well as interviews.

Privacy audits that are at the level of assurance reviews may examine whether the auditee organization has appropriate policies regarding privacy issues and sufficient resources allocated to implementing those policies. They may also examine whether the staff have the correct skill set to carry out those policies. A higher level of assurance may be achieved by examining the work papers of the auditee organization to verify that they comply with their policies.

In addition to interviews and documentary evidence, privacy audits may also include walk-throughs of systems within the auditee organization. This is similar to the standard non-financial audit methodology.

Neil Sanson (Regulator, New Zealand): *they tend to parallel very much the standard IT audit methodologies dealing with interviewing appropriate individuals, gathering documentary evidence, maybe doing walk-throughs of particular systems. And following the same sort of reporting standards, the same sort of... the ACC breach report is a pretty classic IT audit style report. So the methodology seems to be pretty much the standard non-financial audit methodology [that's] been developed over the last twenty or thirty years.*

Privacy audit quality benefits from peer review. Review by someone who does not necessarily have the subject matter or process expertise will also be of assistance because they may still be able to identify areas of weakness in the audit. Privacy audit quality may

also benefit from feedback from the client, if that feedback is implemented in subsequent privacy audits (or it may be built into an audit if the auditor seeks feedback before presenting the final report). There are few external reviewers available to ensure that privacy audits are of a certain quality.

The lack of external reviewers to verify the quality of a privacy audit may be due to the current lack of a substantial community of practice for privacy auditing. The differences between privacy audits by regulators and those by private organizations (Toy and Hay 2015) may hinder efforts to develop a community of practice for privacy auditing. Organizations are facing a challenge of managing personal information effectively, which is an issue that deserves the greatest level of attention at present. Improvements to the quality of privacy audits is an issue that should follow this.

Souella Cumming (Private Auditor, New Zealand): well, I'm not sure that there are... that there is anything particular in place about improving privacy audit quality because there's no real community of practice around privacy auditing as I say, its regulators do it, and they do it in a certain way, and the firms do it, and they do it in a certain way... I think the reason for that is that at the moment, the focus is on improving privacy quality or management of privacy in... by organizations, which has to happen first. I mean, an audit certainly can highlight gaps etcetera. But if the organization is not committed to managing personal information more effectively, or, you know, in a different way then, you know. So audit... the audit quality question, I don't think... I'm not aware of anything in that context.

Privacy audits by regulators may benefit from external review by other departments of government, such as the office of the Auditor-General. Collaboration between different government departments may help to improve privacy audits because it allows skills and

experience in different subject areas to be combined. Privacy audits require skills in both auditing and privacy, and collaboration between regulators such as Privacy Commissioners and Auditors-General may produce highly sophisticated privacy audits.

The Big Four audit firms have a global presence which translates into their privacy audit program in their view of what standards are appropriate for a privacy audit. This is consistent with the findings in Toy and Hay (2015), which show that privacy audits by private auditors tend to focus more on standards that have international relevance. These private auditors have a greater interest in international standards than national regulators do generally speaking, although some national regulators are also interested in the possibility of international standards.

Souella Cumming (Private Auditor, New Zealand): *Yeah, and again, some of that is jurisdictional because that's... they don't have... whereas, say KPMG's a global firm, you know, so you've got a different mandate or driver from that perspective.*

7.6.1 SUMMARY OF THEME THREE

Privacy audits currently lack a substantial community of practice. This may explain the range of different approaches used by different privacy auditors. If a community of practice were to develop more fully, this may have benefits for the audits themselves and also for organizations because it may encourage organizations to allocate sufficient resources to managing privacy.

Privacy audits may examine parts of an organization or the whole organization at once. They may be limited to particular classes of data within the organization, or they may be limited to particular business units or systems within an organization. This is consistent

with suggestions by Boritz and No (2011) as to the potential scope of a privacy assurance engagement and it extends their research by elaborating on methods for privacy auditing.

Privacy audits may include an examination of documents and interviews with staff members in an organization, and may include an iterative process which includes initial reports back to the organization before final views are formed.

Benefits to organizations from privacy audits may include efficiencies in data management practices and staff and management may gain benefits from reflection on their processes for managing customers' data. The changes that an organization experiences as a result of a privacy audit being undertaken may include an improvement in awareness of privacy issues among the staff of the organization. If action is taken by an auditee organization in response to a privacy audit then the audit may have further benefits but it is not yet apparent that auditee organizations routinely take action in response to privacy audits.

Privacy audits may be informed by the view of some auditors that privacy is an organizational issue and not just the responsibility of the privacy compliance team within an organization. This influences the audit. For example, staff interviewed may include those on the business or delivery end of the organization.

The quality of privacy audits may benefit from peer review, and from feedback from the client. However, peer review faces the challenge of a lack of a community of practice for privacy auditing. This difficulty is compounded by current differences in focus regarding the standards that are used in privacy audits by regulators and private auditors. Regulator privacy auditors may benefit from collaboration with other non-privacy focused regulators such as Auditors-General. While both regulators and private auditors may conduct privacy audits using teams that include audit specialists and privacy specialists, private auditors may have a greater focus on international standards as suitable criteria for the audit.

This theme gives insight into the first part of the first research question regarding privacy audit standards and methodologies. It goes more deeply into the standards and methodologies than is achieved in Theme One. This theme throws light on how privacy auditors actually conduct privacy audits and it finds that these methods are often idiosyncratic to the particular privacy auditor in question.

7.7: THEME FOUR: BEYOND A PURE COMPLIANCE APPROACH

The fourth theme is the issue of whether a privacy audit should be merely a compliance audit or if it should go further than the requirements of information privacy law. This is important because it demonstrates the drivers of standards and methodologies used in privacy auditing, and it may affect the utility of privacy audits to stakeholders. Some auditors such as KPMG and IIS believe that privacy is an organizational issue. This entails more than if privacy compliance is merely the responsibility of the privacy team within an organization that might be assigned responsibility for compliance. Privacy as an organizational issue means that it affects how an organization interacts with its stakeholders and how the organization is designed in order to allow privacy issues to be properly managed. This is not to say that compliance is not important, merely that it is one part of the story. If an organization sees privacy as a wider issue than mere compliance, then its compliance objectives should be met in the course of understanding the wider implications of privacy. This is consistent with the fundamental principles suggested in Toy and Hay (2015) which go beyond mere compliance with the information privacy laws that are in place in one jurisdiction. The fundamental principles are consistent with the idea of privacy as an organizational issue because they should influence all aspects of privacy management by an organization.

Souella Cumming (Private Auditor, New Zealand): *...but Malcolm and I have a, you know, we both share the same sort of philosophical base that actually this is an organizational issue, it's not a... you know, it's not owned by the privacy team, or it's not a legislative compliance aspect. It's about how you interact with your customer or your stakeholders and how you design your organization to make sure that you're doing that in a way that you do respect the individual in terms of their, you know, personal information. But also that you do comply. You know, so the compliance is kind of the result. If you design things properly, yes it's going to ensure compliance, but starting with the compliance aspect we didn't think was useful to ACC.*

An implementation of privacy as an organizational issue may assist an auditor to conduct a privacy audit in a more sophisticated way than a mere compliance audit. This is because the use of principles that contribute to privacy management can go beyond the standards contained in information privacy laws in just one country (Toy 2013).

When KPMG and IIS did the privacy audit of ACC, they conducted research to ascertain whether there were any standards that could be used for the audit. This research demonstrated that there are no generally accepted standards for privacy auditing. They did however discover that there were global best practices for information privacy that could inform their approach to the audit. The use of global best practices for a privacy audit, beyond merely a compliance approach measured against national legislation, is evidence of the use of fundamental principles which include the concept of privacy by design (Toy 2013).

Some privacy risks are not addressed appropriately by national legislation. These risks include the governance of function creep. In order to properly include these risks within a privacy audit, criteria beyond national legislation must be used as standards for the audit.

Malcolm Crompton (Private Auditor, Australia): *... what we are also doing is trying to understand governance processes, not just the set of principles, and we also look for some additional privacy risks that aren't really well enunciated in the privacy principles themselves for example: who bears the risk when things go wrong. The possibilities of function creep and the governance of function creep and other issues like that.*

If an organization understands privacy as an organizational issue, and takes steps to implement this correctly, then the privacy risks it faces are lower. For example, the privacy audit of ACC demonstrated that there was a lack of trust in the relationship between the organization and a significant proportion of its customers regarding how their personal information was being treated. This increased the risks to the organization from a more adversarial relationship.

Privacy issues are a matter of responsibility to the community, rather than just a matter of legislative compliance. While this doesn't make them necessarily a high focus for businesses to spend money on, it does raise the danger that privacy risks may be higher for organizations that do not understand privacy issues.

Blair Stewart (Regulator, New Zealand): *One of the reasons is I think some of these privacy compliance things go to a sort of responsibility to the community rather than just to the business. And so that's not the sort of thing people in business like to rush out and spend money on. I mean, you've got different business models and some of them will see the long term value in respect for their customers and confidence amongst the general public that they will go the extra mile, but many others will only be motivated by: "what does the law require me to do?" and; "what makes good sense for my business?"*

An auditor must take into account national laws in the country in which the privacy audit is conducted, and possibly also national laws in other countries in which the auditee does business. It is also important for the auditor to understand governance processes, which means going beyond privacy principles. Best practice may assist in putting a case to management of the auditee that other factors should be taken into account in the privacy audit, above the requirements of national laws. Competitive advantage or peer pressure may also be arguments that assist with this.

National regulators often see compliance as the top priority in an audit. This is in conflict with the broader view taken by private auditors. These findings are consistent with the results in Toy and Hay (2015) which show that regulators have a focus on the legislation within their own country as standards for a privacy audit.

Jay Fedorak (Regulator, Canada): *well, we think when we're looking at privacy investigation and privacy audits, the ultimate goal is to get that organization and other, and by the example of that organization, other organizations, to become more compliant with the privacy requirements of the legislation.*

7.7.1 SUMMARY OF THEME FOUR

Privacy as an organizational issue means that an understanding of privacy issues affects how an organization interacts with its stakeholders. It also affects how the organization is designed in terms of the ways that it manages privacy. If privacy is seen as an organizational issue then this entails that privacy compliance will be achieved but compliance is merely part of the story.

An appreciation of privacy as an organizational issue may enable a privacy auditor to conduct a privacy audit that is more appropriate for an organization than merely a compliance

audit. The use of the latest information privacy concepts from international sources could inform the practice of privacy auditing. Privacy auditors must address privacy as a compliance issue, but this does not preclude them from going further to address privacy as an organizational issue.

Jamal, Maier and Sunder (2005) argue that social norms may have greater weight than laws when there are inconsistencies between them. This idea is relevant to this theme because it suggests that information privacy laws may not be the most important criteria for a privacy audit and that best practices may be given priority.

While there are no generally accepted standards for a privacy audit, there are best practices for privacy that could be relevant to privacy audits. These best practices have been identified in this thesis as fundamental principles (Toy 2013; Toy and Hay 2015). The use of these fundamental principles could enable a broad range of privacy risks to be enquired into and this may go beyond the risks that are addressed by national legislation in any of the countries examined in this thesis. If an organization understands privacy as an organizational issue and implements this in its privacy management practices then the privacy risks that it faces may be lower.

This theme is directed toward the first research question, namely privacy audit standards and convergence of those standards. It supports the fundamental principles that are developed in this thesis because it shows why a pure compliance approach to privacy auditing is unlikely to produce desirable outcomes. Therefore a new approach that uses different criteria is preferred. This theme has a different focus from either Theme One or Theme Three because it addresses the question of why fundamental principles should be used for privacy auditing and it is very significant for this thesis because it gives support to the use of best practices rather than existing information privacy laws. This is therefore the most significant

theme if seen from the perspective of the thesis as a whole. The argument in favour of fundamental principles depends on this more than it does on the other themes.

7.8: THEME FIVE: SKILLS OF PRIVACY AUDITORS

The fifth theme is the issue of the skills that are required of people who would undertake privacy audits. This is important because it drives the standards and methodologies that privacy auditors will view as important and it may influence the quality of privacy audits and affect their relevance to stakeholders. There are currently a small number of talented people who have the skills to conduct privacy audits, and they have gained these skills through different paths. But this is not necessarily an enduring model because employers may find it difficult to access this small group. In order to build a professional group that understands privacy, and to ensure quality in their activities, a more structured process may be necessary. Current in-house privacy officers are beginning to build a community of practice regarding privacy, but this does not yet focus on privacy auditing skills. Privacy professionals may be necessary to fill the gap but there is currently little formal training for privacy professionals.

If organizations lack an understanding of privacy issues, they may struggle to effectively employ and supervise in-house privacy officers for their organization. Current in-house privacy officers may or may not have the skills necessary to perform their functions effectively. For example, organizations may be reliant on their privacy officer to conduct internal privacy audits. How can an organization judge whether or not the privacy officer is doing this competently?

There are some tertiary institutions that provide privacy training. This demonstrates that some moves are occurring to improve the training available to privacy professionals. However, this currently consists of a few scattered papers about privacy (at the time of writing, none could be identified from university websites which focus specifically on

privacy auditing). Nevertheless, there is global awareness of the need for increased certification for privacy professionals.

Some organizations have part time privacy officers. These employees have other duties, but may have 0.1 or 0.2 of their time devoted to privacy issues. These privacy officers may not have qualifications in privacy related areas. Privacy officers commonly have a legal background or an internal audit background, but this does not necessarily entail that they have knowledge or understanding of privacy issues.

Souella Cumming (Private Auditor, New Zealand): *But the other aspect then, and this comes back to my resourcing and capability is well, what's the skills and experiences of people undertaking the audit, you know, what are the qualifications, so, you know, their... they might have qualifications in, you know, other areas, but not in the privacy area, so certainly what we have found, both working with the clients that we have done privacy assurance work or privacy work with is that, as I say, mainly they are people who... it's a point one or a point two of their job, if that, and it's... they've got a legal background, or they've got an internal audit background, or they've got some other background, but they haven't been to a privacy training course other than whatever training they do within their own organizations. So you've got, particularly in New Zealand, but I think it is the same... is that this is a very new and emerging, sort of, professional area, and so therefore you've got a small pool of people. And the audit, the, you know, the audit component is maybe even less than that.*

Private audit firms conduct privacy audits using teams that consist of people with the skills necessary to undertake privacy audits. These include people who are experienced auditors and people who have privacy expertise. This demonstrates the multidisciplinary nature of privacy audits. It may also explain why the private audit firms have a different focus from

national regulators, although some regulators have staff with expertise in both audit and privacy. Nevertheless, the approach of the private audit firms appears to be to create teams that undertake the audits and who gain privacy auditing skills through this experience.

Tertiary education courses are currently focused on financial auditing. This focus may give students general auditing skills. However, while general auditing skills are useful to someone who is going to conduct a privacy audit, it would also be useful for a potential privacy auditor to have specific skills in privacy auditing. Regulators may offer training courses that can assist a person to gain privacy auditing skills. Professional bodies such as the International Association of Privacy Professionals (IAPP) also have seminars and training sessions. New Zealand has a group called the Privacy Officers' Round Table (PORT) which demonstrates the beginning of a community of practice for privacy professionals. The author attended one meeting of PORT (17 March 2015), which was focused on privacy issues and not specifically on privacy auditing issues.

Lawyers may have skills that can be adapted to conduct privacy audits, although training in auditing skills would be important, and training in privacy would also be important because some law schools do not teach courses on privacy. However, the costs could be prohibitive if a client is paying for a lawyer to do privacy auditing work at traditional lawyers' rates. Privacy audit work may not be considered legal work, so it should not incur the same costs as legal work.

Regulators employ staff to conduct investigations in the area of privacy. However, even though some of those staff are trained as lawyers, they do not work as lawyers when conducting their regulatory functions. It appears that legal training is one pathway of many that leads into the area of privacy. This lack of a clear pathway may discourage people from gaining employment as privacy professionals.

A half day course run by a national regulator such as the New Zealand Office of the Privacy Commissioner would be useful to assist a person to conduct a privacy audit, but not sufficient. This is because recognition of privacy is a mind-set that needs to be developed, not just a body of knowledge. An ideal skill base to conduct a privacy audit may be to have a team composed of both an auditor and a privacy specialist.

It is important to develop the skills of privacy auditors, but it is equally important to develop the privacy understanding of executive management. This is a challenge that should be met because executive management have the greatest influence over whether or not an organization decides to improve its privacy practices, or to have a privacy audit in the first place.

Neil Sanson (Regulator, New Zealand): *I think the likely biggest challenge at the moment in New Zealand is just the... developing the privacy understanding partly amongst those people who have the skills to audit, but even more so in some ways probably, amongst executive management.*

An auditor may productively gain privacy skills to enable them to conduct a privacy audit. The necessary understanding of privacy issues can be taught, and does not require a high level of technical knowledge (compared to IT auditing, which requires a significant mastery of programming skills). Auditors need a certain mental approach which will enable them to conduct an audit, and this approach would take some time to develop so a person who has already been trained as an auditor should be able to move into the privacy area after a sufficient training period in privacy issues.

Neil Sanson (Regulator, New Zealand): *I think that there are a lot of backgrounds which would give the sort of skills I was talking about. There's always been... in IT audit, there's always been a discussion whether it's better to get somebody who knows the subject matter, and then train them to look at it from an audit perspective, or whether it's better to get somebody with the mental approach that an auditor needs, and then train them in the subject matter. But I don't think... that debate has never sort of been resolved in the IT audit profession. Given that privacy is... privacy audit will not require the same level of technical knowledge then I think you are almost certainly best looking for people with the right mental approach and giving them training in privacy, and giving them a chance to learn that perspective.*

Privacy officers in organizations may not have the necessary training in auditing skills to allow them to conduct a privacy audit. Some privacy officers do not have an auditing background, although they may have knowledge of privacy issues. A sufficient period of training in auditing skills may assist a privacy officer to conduct a privacy audit. Having a team that includes a person with a background in auditing may also have the same benefits.

As seen in the next quote, Neil Sanson believes that privacy auditors require the following skills:

- a) The ability to communicate effectively with people from many different backgrounds such as management, technical staff, operations staff.
- b) To be able to assess their statements and to identify any gaps in their explanations.
- c) The ability to tailor an investigation based on communications with staff members.
- d) To be able to assemble evidence in a way that clearly demonstrates the extent of an organization's activities regarding privacy.

- e) The ability to quickly come to understand a system that the auditor may not have any prior experience of.
- f) The ability to write a report that clearly communicates the findings in the audit to management of the organization.
- g) An understanding of privacy issues.

Neil Sanson (Regulator, New Zealand): *One of the primary skills is the ability to talk with a range of people. Technical people, management people, and business operations people. All of whom basically talk slightly different jargons. To assess what they're saying, and what they're not saying. And to tailor the investigation based on that sort of information. So there's a key skill around being able to talk to people and draw information from that. There's also a need to be able to assemble the evidence very clearly. You've really got to be sure that you have documented proof of to support any findings. Otherwise basically they will not be accepted when you report them. The ability to quickly understand systems that you've probably never seen before. So there's quite a bit of mental flexibility required. Quick learning. The ability to write up a clear report that will... that's easy for management to understand. These are all standard sort of skills required of IT auditors. The same skills will be required of privacy auditors. I think the major difference will be that privacy auditors will not require quite as much technical knowledge of IT systems. And will have some understanding of privacy issues.*

Souella Cumming is of the opinion that privacy auditors require the following skills (many of these are echoed in Neil Sanson's quote above):

- a) An analytical ability that can allow the privacy auditor to understand processes in the organization that they are auditing.

- b) An ability to assess a risk using appropriate methodologies.
- c) An understanding of privacy issues.
- d) The ability to plan the audit and to undertake further work if required.
- e) The ability to make a judgment and form a conclusion for the audit.
- f) Specific industry experience would also be of benefit because it can assist in assessing risks, practices and processes within that particular industry.

Souella Cumming (Private Auditor, New Zealand): *well, in terms of the audit, you know, the... in terms of an audit obviously you're auditing against specific standards, but there's the... you know, you need to be analytical... not in a financial sense necessarily, but, you know, things like systems thinking or being able to deconstruct a process. So there's that analytical aspect of it, there's the understanding of risk and being able to really assess a risk. And, you know, there's various, again, methodologies that sit in behind and support that. And then, you know, certainly an understanding of the Privacy Act... But from an audit perspective, you need to be able to plan, you know, undertake further work, analyse information, make a judgment and then form a conclusion in terms of the specific audit objective, and then you might need specific industry experience, so if you're looking at the financial services sector, banks and insurance companies then someone who's got some sort of experience in processes, practices, risks in that area, or if it's a government agency that's a policy ministry versus a Ministry of Social Development that pays benefits, you know. So there's an industry knowledge as well as a subject matter knowledge around privacy.*

7.8.1 SUMMARY OF THEME FIVE

The number of people with the skills to conduct a privacy audit is small. A community of practice regarding privacy issues has begun to form, but this does not as yet focus on privacy

auditing. This situation creates barriers to the employment of privacy auditors and the implementation of their skills across different organizations. Organizations that lack an understanding of privacy issues may struggle to employ privacy officers and may fail to supervise privacy officers once they have employed them. Privacy officers within organizations may be very competent but there may be few ways to verify if they are competent in the absence of standards or certifications. Privacy officers that are part time may not have qualifications or training appropriate to their role.

Some tertiary institutions provide privacy training in the form of a few scattered papers about privacy but these do not appear to focus on privacy auditing issues. Training in privacy auditing skills may only exist within organizations that have conducted privacy audits such as regulatory organizations and private auditors.

Private auditors conduct privacy audits using teams containing privacy specialists and experienced auditors. Regulators may also take this approach. This demonstrates that privacy audits are multidisciplinary in the sense that there is no training specifically for privacy auditors. The training of people that conduct privacy audits comes from areas that are considered separate disciplines. This may explain why the group of people who can conduct privacy audits is small. Privacy regulators may be able to bridge this fissure by offering training courses to assist people to gain the skills to conduct a privacy audit, provided these courses are sufficiently lengthy and effective.

While this theme does not directly answer the research questions, it is an important general basis for addressing them. The skills of privacy auditors have a direct influence on the standards and methodologies used in privacy audits. The skills of privacy auditors may also have an effect on whether or not privacy audits are useful to the beneficiaries of the audits. This theme demonstrates that the skills of existing privacy auditors vary considerably

and this may explain some of the current divergence between the approaches that they take to privacy audits.

7.9: THEME SIX: PRIVACY MATURITY ASSESSMENT FRAMEWORK

The sixth theme is the issue of privacy maturity assessment. This issue is important because a framework has been developed in New Zealand that may provide assistance to privacy auditors in that country and it may affect the standards that are used in privacy audits. Privacy maturity assessments involve an examination of how far developed or how mature is an organization's commitment to understanding privacy issues and implementing appropriate measures to protect the personal information of the customers of the organization. In New Zealand, the Government Chief Information Officer has promulgated advice on Privacy Maturity Assessment, including a framework for this (GCIO 2014). This document outlines five different levels of maturity, ranging from Ad Hoc to Developing to Defined to Embedded to Optimised. This details aspects such as governance and leadership and compliance with legislation. This document also incorporates recent suggestions, such as the concept of Privacy by Design. It therefore represents an attempt to take into account international best practice, and this is consistent with the suggestions in Toy (2013) and Toy and Hay (2015).

The New Zealand Privacy Assessment Maturity Framework (GCIO 2014) was developed by KPMG and a public sector working group. It could contribute to standards against which the privacy maturity of an organization may be assessed. If an organization has steps to take to improve its maturity according to this model, it could be the subject of a privacy audit to assess its development.

Souella Cumming (Private Auditor, New Zealand): *That's something that KPMG has developed in conjunction with a public sector working group, and it is something that public sector agencies... there'll be an expectation that they do an assessment against that maturity... using that framework. And so that sort of starts to form a bit of a, you know, a base line. And if they are assessed at a lower level of maturity and their risk means that they should be higher, then they'll need to put in place a program of work to get to that. And then there'll be some independent audit of whether they have achieved that or not.*

Some organizations in New Zealand do not have a good understanding of privacy issues and therefore they have not assigned the right level of resources to managing those issues.

Organizations that have an obligation to have a privacy officer may have one with responsibilities that are not well developed in terms of maturity of understanding of privacy issues. By contrast, an organization that is more developed in its understanding of privacy issues may have a more pro-active privacy officer who may manage a program of work designed to ensure that privacy breaches do not occur. A challenge for New Zealand organizations may be to allocate the correct level of resources to the role of privacy officer, given the level of risk from a privacy breach. Some organizations may not understand the risk and may not have the appropriate level of resources allocated to managing it.

Organizations that operate solely in New Zealand may have a less sophisticated understanding of privacy issues than multinational organizations. This may be due to the large number of small and medium size organizations in New Zealand. This presents a challenge to New Zealand organizations when deciding what level of resources to allocate to privacy.

Blair Stewart (Regulator, New Zealand): *yes, well I think, I mean one of the realities in New Zealand is, and I think it would be the same in most countries, but it's certainly [marked] here, is... [that] there's a lot of small and medium enterprises, and [only] a few big ones. Even the big ones don't necessarily have the sophisticated approach to aspects of compliance that multinationals coming from other countries do...*

7.9.1 SUMMARY OF THEME SIX

Privacy maturity assessment is a process that examines the understanding and implementation of appropriate privacy management practices within an organization. It aims to assess the level of maturity of the organization's privacy practices and to determine what it must do if it wishes to become more mature.

Organizations that do not have a good understanding of privacy may not have assigned sufficient resources to managing it. On the other hand, an organization that has assigned the correct level of resources to privacy may have a pro-active privacy officer who may enable the organization to avoid privacy breaches.

In New Zealand, a privacy maturity assessment framework has been developed by KPMG in conjunction with the public sector. This framework allows organizations to assess their progression along the maturity scale. If an organization takes steps to improve its maturity according to this framework, it may use a privacy audit to assess its development along the privacy maturity scale. New Zealand organizations are particularly at risk from privacy breaches because they have a less accurate assignment of resources to managing privacy risks than multinational organizations do.

This theme addresses the first research question because it examines the standards that are used in some privacy audits. It also supports the fundamental principles that are advanced in this thesis. Some of the standards that are used in the framework are consistent with some

of the fundamental principles (such as Privacy by Design, and Accountability) and therefore they indicate aspects of international best practice that cannot be found in the existing Privacy Act 1993 (NZ).

7.10: THEME SEVEN: INTERACTION WITH STAKEHOLDERS

The seventh theme is the issue of identification of the stakeholders of privacy audits and the assessment of how privacy audits may be useful to them. This is important because it addresses the research question relating to who benefits from privacy audits and the value of the benefits to these people. Expectations regarding privacy interests are not yet well developed among the general public in some countries, including in New Zealand. In addition to this, some New Zealand companies lag behind their overseas counterparts in their express recognition of privacy as a stakeholder interest (Gunasekara 2013, 292). However, public privacy breaches do tend to generate public outrage even in New Zealand. To address this issue, privacy audit reports may be made public, which provides accountability. This fits in well with the theory from Toy (2013), which suggests Accountability as a fundamental principle of privacy audits.

Privacy regulators/enforcement bodies are also beneficiaries of privacy audits. They are sometimes the direct party to which the privacy audit must be delivered, and the privacy audit may have been done under an order by the regulator/enforcement body.

Marty Abrams (Analyst, United States): *I actually think the organization itself is the major beneficiary of a privacy audit, because they begin to understand what they have to improve on... However, if I'm under an FTC consent order, I still have a requirement to send the results of that FTC consent order to the FTC.*

Privacy audit reports may be made public, which provides a type of accountability in that the public can then assess the organization's privacy management practices by reading the report. If privacy audit reports are submitted to regulators then this is another type of accountability. These types of accountability may or may not coexist with the power of regulators to actually impose any form of penalty if the report is not favourable. Nevertheless, accountability may still be demonstrated by the technique of making the report public.

Regulators may take confidence in the results of a privacy audit report, and the public may also take confidence from the results if the report is available to them. In addition to Accountability, the principle of Transparency is also served by making a privacy audit report public. This is because it may allow the public to ascertain more about the privacy management practices of an organization than if the report is kept secret from them.

Blair Stewart (Regulator, New Zealand): *We were wanting the confidence that they were compliant, and in turn we wanted the public to know that.... We wanted the companies to be making representations to the public about their compliance. So we didn't want them just to make assurances to us. So we wanted that level of accountability. So I think that... in that instance it was being used to serve interests of transparency and accountability.*

The general public gain a benefit from privacy audits. The privacy practices of organizations who are handling the data of the general public may be improved following a privacy audit, if they had been found lacking prior to that audit. This may be the case if the organization has committed to addressing recommendations for improvement, if there are any such recommendations in the privacy audit report.

The next beneficiary of a privacy audit is the organization as a whole, or perhaps parts of an organization such as the Board. The organization may be subject to a compulsory

privacy audit by a regulator, or it may have commissioned the privacy audit by a private auditor. If the privacy audit report discloses a clean bill of health, the organization and/or the board can take confidence in that. If the report suggests improvements then the organization can address these in order to have confidence in its privacy management practices.

The public gain the largest benefit from a privacy audit. This will only be the case if the privacy audit is successful in that it correctly identifies any possible failings in privacy management by an organization and offers strategies to remedy these. An ineffective privacy audit will not be of assistance. The suggestion in Toy and Hay (2015) is that different privacy auditors may be doing different things in privacy audits. While this does not necessarily entail that the different audits are of different quality, it does raise concerns that the audits may not be of the same quality. If some privacy audit reports show that the auditors did not consider the same principles of privacy management as other auditors, the issue of quality leaps to the foreground.

The aim of a successful privacy audit should be to suggest a process that achieves the objectives of the business most effectively, in terms of privacy management practices within the organization. If the privacy audit is successful, it will suggest improvements that carry the least cost to society as a whole as well as to the organization. It is not clear if there is a trade-off between members of society as a whole compared to the organization. However, the negative publicity associated with a privacy breach may mean that there is little difference.

Neil Sanson (Regulator, New Zealand): *well the benefit really accrues to... the largest benefit really accrues to the public. In that a successful audit will lead to a process that achieves the business objective or need in the most effective and best controlled way. And, given... [we're] dealing with government agencies that are required to do their activities by legislation, so the collection of personal data and the holding of personal data and the processing has to be*

done as required by law. So, if that is done in an efficient way with the most effective protections against misprocessing or loss of the information, duplication of the information, then that will tend to result in the process being done with the least cost, either monetary cost, or cost in the amount of data that's held, to the public.

Members of the public are consumers and so their information is held by organizations that they interact with. This is why members of the public are the beneficiaries of privacy audits. The organization may be considered to be a secondary beneficiary of a privacy audit due to having the ability to implement the suggestions in the audit report to reduce the likelihood of a privacy breach. It may be necessary to distinguish between parts of the organization because different parts, such as the board of directors, may have more influence over the privacy management practices of the organization than other parts do. If the board has a strong privacy management agenda then this has an important effect on the organization. In the absence of this, it is difficult for other parts of the organization to manage privacy effectively.

If privacy audits are successful and any recommendations are followed by an organization then the privacy management practices of that organization may improve. This may also include an increasing compliance with information privacy laws. The ultimate beneficiary of this is citizens whose personal information is held by organizations.

Organizations may benefit from privacy audits even if they are not the auditee. If privacy audit reports are made public, there may be an effect on other organizations which may gain a greater understanding of privacy issues simply by reading the report. This may encourage the readers to examine their own privacy management practices, and may lead to improvements.

The auditee organizations themselves may benefit from privacy audits because they may suffer financially if they commit a breach of privacy. Penalties may be imposed on them, if this is possible within the country or countries in which they operate. Consumers may be encouraged to deal with organizations that protect their data and not to deal with those that have insufficient privacy management practices.

Privacy audits may also benefit citizens (which may extend to the entire population base of a country) by providing a model example of privacy management practices. This can happen even if the audit report shows suggestions for improvement because the organization may follow the suggestions, and thereby improve its privacy management practices to be a leading example to which other organizations may look in order to improve their own practices.

Privacy auditors themselves may also benefit from privacy audits because they may gain increased skills in conducting audits. Other privacy auditors may benefit by being able to see what has been done and what worked well in a particular audit. This is especially important due to the underdeveloped nature of the practice of privacy auditing. There are currently few examples to assist privacy auditors to improve their practices.

Tanya Allen (Regulator, Canada): *and that, and as we conduct audits, I think especially because we're just starting the program, once we get the first few audits out the door, our own researchers, our own auditors will have, I'm sure, recommendations for improving both the tools, the methodologies, how we go about collecting it, and as well we intend to follow up with any audited agency to look at the implementation of our recommendations. And during the follow up, we can ask questions about, you know, how did the audit work for you? Basically. And they are our stakeholders as well as people that we will be auditing, so their view and input will be used to build a stronger program.*

Organizations may also benefit from successful privacy audits in a less obvious way. The relationship between an organization and its customers or clients is of vital importance because it influences the perception of adverse events. If a good relationship exists, there will be fewer repercussions from adverse events. Privacy audits, if successful in improving the information management practices of an organization, may engender a greater level of trust between an organization and its customers, which may make their relationship less adversarial. The adverse reaction from any negative event such as a privacy breach may be mitigated by a less adversarial relationship

In the public sector in particular, customers often do not have a choice of different agencies. People who are unwilling to be customers of an organization may nevertheless find themselves obliged to deal with it, if it is some aspect of the state that is relevant to them. For example, most citizens must deal with the tax system, which means dealing with the organization responsible for that. If this unwillingness is added to other factors, such as mistrust of the information management practices of the organization, this can spell disaster. If a privacy breach occurs in the context of several factors that lead to a poor relationship between an organization and its customers, the customer may seek to take advantage of this breach, possibly leading to a bad outcome for the organization.

7.10.1 SUMMARY OF THEME SEVEN

The recognition of privacy as a stakeholder interest is not well developed in some companies. This is particularly true in New Zealand. Privacy breaches may generate public outrage in New Zealand even though privacy interests are not well developed among the general public in this country. Making privacy audit reports public may address these issues by providing a

type of accountability to the general public. This allows the general public to read the report and thereby gain some insight into the privacy management practices of the organization.

Privacy regulators are also the beneficiaries of privacy audit reports (if they did not do the audit themselves). This is especially the case where the regulator has required the audit to be done under an enforcement power. Some regulators (such as the New Zealand Privacy Commissioner) do not have any powers to take action to enforce the suggestions in a privacy audit report, but the technique of making the report public may be the next best thing.

If suggestions for improvement are made in a privacy audit report and if the organization takes steps to implement these suggestions then the general public may gain a benefit from this, especially if the organization is one that interacts with a large portion of the general public. The organization as a whole may also gain a benefit from a privacy audit report because it may be able to improve its privacy management practices by following suggestions for improvement. Parts of the organization such as the board may also gain a benefit from greater knowledge of the practices of the organization. Organizations that have public privacy audit reports may gain a benefit from increased public relations which can improve the relationship between them and their customers. This can lower the risks from privacy breaches because customers may be less willing to exploit privacy breaches.

The quality of a privacy audit is of vital importance to the stakeholders. This is because an ineffective privacy audit may not correctly identify areas in which the organization may improve its practices. If different privacy auditors are doing very different things in a privacy audit then this raises questions about whether the audits are all of sufficient quality. The highest quality privacy audits will correctly identify weaknesses in privacy management practices and will suggest improvements that correctly address these issues while carrying the least cost to the organization and to society as a whole (if other alternatives are available that are inferior).

Other organizations may benefit from a privacy audit because they may be able to follow any suggestions in a public privacy audit report that are relevant to them. The auditors themselves may benefit from a privacy audit because they will increase their skills and experience in conducting privacy audits which may lead to increases in quality of privacy audits. Elliott (1997) suggests that accountants have a strong auditing tradition and this is relevant to this theme because this may assist them to provide privacy assurance services that stakeholders see as useful.

This theme directly answers the second research question because it examines who are the beneficiaries of privacy audits. It also details the appropriateness of privacy audits as a mechanism to provide benefits to them and this further supports the fundamental principles in this thesis. This theme indicates that the quality of privacy audits is important for stakeholders to be able to find them useful. A privacy audit that does not take account of the latest international best practices may struggle to achieve this.

7.11: THEME EIGHT: RISK MANAGEMENT AND INTERNAL AUDIT

The eighth theme is the issue of how privacy audits may relate to the internal audit functions within an organization and how they may assist with the process of risk management by an organization. This is important because it may affect the standards and methodologies that are used in privacy audits. Discussion about privacy governance is moving from a consent model to an accountability model. Consent is less relevant because the situations in which individuals can give meaningful consent to uses of their data are increasingly limited. Much data is now collected in the absence of consent by individuals, or in a situation where the individual has little power to refuse consent. For example, if an online service is offered on a “take it or leave it” basis with little room for negotiation. The increased collection of data has led to the age of Big Data.

The danger is that “big-data predictions, and the algorithms and datasets behind them, will become black boxes that offer us no accountability, traceability, or confidence. To prevent this, big data will require monitoring and transparency, which in turn will require new types of expertise and institutions” (Mayer-Schonberger and Cukier 2013, 179). Privacy audits need to take account of the internal governance processes within an organization. Privacy audits by an external auditor may be a good way of verifying the efficacy of the internal privacy audit program of an organization. This can increase the accountability and transparency of the organization.

Private auditors that conduct risk management work may assess the privacy risks of an organization under that function. This can assist an organization to decide whether it requires assurance by an external party regarding controls over its privacy risks.

Souella Cumming (Private Auditor, New Zealand): *And because in our broader work, we do a lot of work in the risk management and the internal audit space. So, from a risk management perspective we can work with an organization to really understand what their actual risks relating to personal information are, and then how significant they are, and then whether they need assurance over the controls that are in place to manage those.*

Privacy audits may benefit from an approach that is focused on the risks to an organization in terms of its privacy management practices. While an approach that is focused solely on compliance with legislation may be able to ensure compliance, it does not necessarily address the bigger picture. Private organizations that conduct privacy audits may focus the audit on identifying privacy risks and on assessing the controls within the organization that mitigate those risks.

Both internal and external privacy audits may be useful to an organization. Internal privacy audits have the advantage that the internal auditors are very familiar with the organization, and external privacy audits have advantages that the auditors have more of an overview of the standards within different organizations and what is required for best practice in privacy management. A combination of both internal and external privacy audits may be of greater assistance to an organization than just one type alone.

7.11.1 SUMMARY OF THEME EIGHT

Privacy audits may be done as part of the internal operations of an organization. These internal privacy audits may occasionally be verified by external auditors to ensure their consistency and quality. External privacy auditors may conduct privacy audits as part of their risk management work. A combination of both internal and external privacy audits may provide a very robust approach to the issue of accountability.

The assessment of privacy risks may go beyond the mere compliance aspects of a privacy audit. These risks may not be well enunciated in privacy legislation so a broader approach is sometimes necessary.

This theme supplements investigation of the first research question because it addresses the standards and methodologies used when privacy auditing in part of the internal audit operations of an organization. It also documents differences between the methodologies that are used by internal privacy auditors and external privacy auditors, finding that external audit is useful to maintain quality.

7.12: THEME NINE: IMPETUS FOR PRIVACY AUDITS

The ninth theme is the issue of why privacy audits are being done. This is important because an understanding of the drivers of a privacy audit may impact on the standards that are seen as relevant for that audit. Impetus for privacy audits can come from lawmakers or regulators, who may mandate that privacy audits are required by certain organizations (in some countries). However, some countries currently have regimes that do not give strong powers to lawmakers or regulators to require privacy audits (such as Australia and NZ). Nevertheless, privacy audits have still been done, even in such countries. This may be due to consumers avoiding doing their business with organizations that have poor privacy management practices.

Increased powers to require privacy audits would have the effect of increasing the need for better privacy audit standards, and for increasing the skills of people who can conduct privacy audits. These increased powers may result from pressure on lawmakers by citizens who wish organizations to improve their privacy management practices. Pressure from lawmakers may lead to more rigorous privacy audits, especially if that pressure is in the form of a legal requirement to conduct a privacy audit. In this case, the organization may wish to avoid further sanctions and so it may have an incentive to have a privacy audit that is relatively broad in its scope.

Marty Abrams (Analyst, United States): *it depends on why you're doing the audit, ok? If I'm doing an audit to report to the Federal Trade Commission [because] I have to do an audit every other year and report the results of that, the fact that the results are going to be reported to the FTC means that if you are afraid of being found not in compliance with an FTC order then you have a high desire for the audits to be done in a fashion that truly is robust.*

Regulators in Australia and New Zealand are not in a strong position to require organizations to have privacy audits, and there is currently little pressure on organizations in these two countries until a public privacy breach has occurred. This has resulted in only a small number of privacy audits. This relative lack of pressure is a challenge for privacy audits, which may become more developed if this pressure increases.

Organizations are unlikely to ask national regulators to conduct a privacy audit in the absence of a requirement to do so. However, organizations do sometimes approach such regulators in order to check that any new initiatives they might be contemplating are in compliance with the advice of the regulators.

Jay Fedorak (Regulator, Canada): *we haven't had anyone come to our organization and say: please come and conduct a privacy audit. We get organizations who will come and say: we're making a program change. We're introducing a new program, we're going to try and do something in a new way. We're developing a new information system. Here's our evaluation of what we think the privacy implications are. Will you have a look at it, and give us your advice or your, you know, concurrence as to whether we've come to the right conclusion. So we don't really have somebody coming and saying: would you do a systematic audit for us? But they do come to us with, sort of, questions around... their ensuring that they're in compliance with the legislative requirements. There may be certain organizations that may hire contracted service providers that might do some kind of privacy reviews on things before they go public with things, but I'm not aware of anyone coming forward and requesting a privacy audit. We know that the public bodies within the jurisdiction of the Auditor General sometimes go to the Auditor General and request audits of certain programs and things, but we haven't heard of any of them relating directly to privacy.*

7.12.1 SUMMARY OF THEME NINE

The impetus for privacy audits may come from regulatory organizations which may have powers to require an organization to submit to a privacy audit. Regulators in some countries may not have powers to force a privacy audit to be conducted. However, privacy audits may still be conducted in such countries under political pressure. Pressure from regulators may lead to improved standards for privacy audits, or this may come from public pressure if consumers demand more effective privacy audits. These pressures may also increase the frequency of privacy audits. Organizations may be unwilling to ask a regulator to conduct a privacy audit in the absence of a requirement to do so.

This theme assists to answer the first research question because it suggests that standards are affected by the motivating forces behind privacy audits. Audits that are mandated by the enforcement powers of a regulator are more likely to be robust. Where regulators lack strong enforcement powers, there is less incentive for privacy audits to have a certain quality.

7.13: THEME TEN: PRIVACY IMPACT ASSESSMENTS

The tenth theme is the issue of privacy impact assessments. This is important because they need to be distinguished from privacy audits but they are still related to the fundamental principles that are advanced in Toy and Hay (2015). Privacy impact assessments are important for an organization to undertake at the beginning of development of a new product or service. Although information privacy laws do not always require this, it is part of best practice as suggested by Toy and Hay (2015). Privacy impact assessments are the beginning of a process of assessment by an organization of its own privacy management practices. The principle of Privacy by Design (Toy 2013) is broader than the concept of privacy impact assessments. Privacy by Design is relevant even at the stage of forming an idea for a new

product or service but privacy impact assessments are a formal process that is undertaken when the idea for the new product or service has been formed. This thesis argues that privacy impact assessments may be considered to be within the principle of Privacy by Design, and is an important part of it.

In British Columbia, there is a legislative requirement for some public bodies to conduct a privacy impact assessment when considering certain courses of action. These are compliance reviews that assess a new system or program with respect to information privacy laws.

Jay Fedorak (Regulator, Canada): *well there is a requirement in the legislation for certain public bodies who are doing certain types of things to conduct what was called a “privacy impact assessment”. So what that is, is it’s essentially a compliance review with respect to the requirements of the legislation as how they apply to a new system, a new information system or a new program that would involve personal information. We do annually get a certain number of those. I... probably somewhere between the extremes of extremely rare and extremely common, somewhere in the middle...*

The Big Four audit firms do privacy impact assessments, often as part of their advisory activities, but these may also be considered assurance activities. They focus on new policies and business processes and appropriate controls for management of privacy within that.

Souella Cumming (Private Auditor, New Zealand): *So that’s on the advisory side, and then on the assurance side... Privacy Impact Assessments are actually quite interesting as to where they sit... they are probably more in that advisory side because you’re doing an impact assessment either around, you know, a policy or a business process and then, from there, the*

appropriate controls will be designed into hopefully the policy mechanism or the business process going forward. So, we do Privacy Impact Assessments...

7.13.1 SUMMARY OF THEME TEN

Privacy impact assessments are important for organizations to undertake at the beginning of development of products or services. These are a narrower concept than the fundamental principle of Privacy by Design, but they do reflect some aspects of it. Some countries (such as Canada) have legislative requirements that organizations must conduct privacy impact assessments. While privacy impact assessments are often done by an organization internally, private audit firms may be able to assist with this process.

This theme is relevant to the first research question because it discusses standards for privacy audits that are congruent with aspects of the fundamental principles advanced in this thesis. It also distinguishes privacy impact assessments from privacy audits and this is an important part of the definition of privacy audits. While a broad definition is taken here, there are some things that fall outside the definition such as these services. Despite falling outside the definition however, privacy impact assessments still have some parallels with privacy audits and may be able to inform the future development of privacy audits. This is because privacy audits may be seen as a way to check the appropriateness of the findings in a privacy impact assessment.

7.14: CONCLUSION

The interview themes demonstrate that harmonization of privacy auditing standards, while desirable, faces some significant challenges at present, including the lack of a community of practice which hampers opportunities for peer-review of privacy audits and impedes the

opportunities for training of those who would conduct privacy audits. Nevertheless, there are important drivers of harmonized standards. The view of some privacy auditors that privacy is an organizational issue is a critical finding of this research and this is a major support for the argument for harmonized standards. Drivers also include challenges from changing technology and the desirability of incorporating more holistic criteria for a privacy audit that can enable an organization to ascertain its privacy risks in a more comprehensive and effective fashion than is possible by using currently enacted information privacy laws as criteria. Flexibility is also an important aspect of privacy auditing and the range of assurance services that are termed 'privacy audits' need to be able to adjust to the sometimes idiosyncratic information management practices of auditee organizations. Privacy audits may examine parts of an organization or the whole organization at once. They may be limited to particular classes of data within the organization, or they may be limited to particular business units or systems within an organization. This is consistent with suggestions by Boritz and No (2011) as to the potential scope of a privacy assurance engagement and it extends their research by elaborating on methods for privacy auditing. The Privacy Maturity Assessment Framework that has been developed by KPMG in New Zealand indicates a modern method of privacy assurance that reaches toward harmonized standards. Beneficiaries of privacy audits may not as yet have a well-developed understanding of privacy as a stakeholder interest. Improvements in privacy audit quality may improve the usefulness of privacy audit reports to those who may benefit from them.

This thesis demonstrates that regulatory organizations tend to focus on their own legislation in the particular country in which they operate, while private auditors focus more on international policy developments in information privacy. National regulators are not opposed to the idea of harmonization of standards, but currently they do not see it as the main basis for a privacy audit. Both private auditors and regulators see challenges arising from the

relative novelty of privacy audits, and the lack of experience and community of practice.

While a small number of privacy auditors have excellent skills to conduct such audits, there is a general lack of a privacy auditing profession. There is also a general lack of awareness among the general public and among organizations that might be subject to privacy audits regarding their information privacy rights and duties.

There is a greater similarity between the methodologies in terms of the investigative audit standards that are being used by regulators and private auditors, and this may be a possible basis for reducing differences between the approaches of different organizations to privacy audits in the future. However, differences may still exist because the current use of methodologies may be idiosyncratic to the particular privacy auditor. Flexibility is an important part of the definition of privacy audits and this flexibility may be achieved through the use of principles rather than detailed rules for information privacy.

Privacy impact assessments and the privacy maturity assessment framework demonstrate that the use of international best practice for information privacy is an important part of privacy assurance services and that it may inform the approach taken to privacy audits. The impetus for privacy audits may also have an important impact on the service. While privacy audits that are mandated by regulators may be in one sense more rigorous, they are also more likely to be tied to the requirements of information privacy law in the country in which they are produced. By comparison, privacy audits done by private auditors may take more account of international best practice as embodied in the fundamental principles. The overlap between these two issues produces some interesting results and some exemplary privacy audit reports have been produced by private auditors where a regulator has required the audit to be done.

Please see Table 6 for a summary of issues relating to (i) principles, (ii) standards (and rules, including use of auditing tools), (iii) practice (operational issues, specifically

affecting the practice and practitioners) and (iv) implications for the future development of privacy auditing.

Further research in this area could contribute to knowledge about the market for assurance services, particularly given that privacy assurance is an unregulated market and therefore it may be more competitive than the financial statement audit market (Hay et al. 2014, 355). Similar suggestions have been made in regard to research about assurance of sustainability reports, especially where assurance could be provided from within the accounting profession or outside it, and “how performance of multidisciplinary teams can be enhanced” (Simnett 2014, 326).

CHAPTER 8: CONCLUSION

Alan Toy

8.1: INTRODUCTION

This study of privacy audits investigates issues closely related to the practice of privacy auditing and this is what distinguishes it from previous research on privacy audits. This thesis includes the first academic research in which privacy regulators and auditors have been interviewed. It also contains the first research study to examine publicly available privacy audit reports in order to determine what the practice of privacy auditing has consisted of up to this point, and where it might be going in the future. The research also analyses policy documents and proposals for legislative reform and suggests fundamental principles for information privacy that could be used as standards for privacy audits. If privacy audits in different countries can evolve to a more coherent approach that can give confidence to users in countries (that may be different to the one in which the audit report is produced) then privacy audits may gain greater relevance to a wider audience. This could enhance their utility and may result in greater demand by users of privacy audit reports. In turn, the privacy rights of the general population may be improved.

The number of privacy audits that have been done is small, but they have achieved a high degree of publicity. The professional services firms are now providing privacy audit services, along with other privacy auditors in the private sector. Regulators are also providing the service. Privacy is an important right and citizens need to be assured that organizations that control their personal data are implementing appropriate privacy management practices.

The myriad of different standards applied in previous privacy audits demonstrates a lack of a unified vision on the part of privacy auditors as to what the practice involves. This situation could be different in light of a clear set of standards for privacy audits. Some privacy auditors see the application of the information privacy laws within a particular jurisdiction as of paramount importance, but others take into account wider developments in international best practice in information privacy. These differences are not split cleanly along the lines of regulators compared to private audit firms because some regulators take into account the international developments while others prefer to focus on the requirements of their own legislation. International developments in information privacy may be of particular relevance from the perspective of stakeholders such as consumers who might reside in a different country from the audited organization.

As privacy audits mature, regulators and audit firms may develop new ways to train and certify new privacy auditors. This may enhance the practice of privacy auditing by building a community of practice in which privacy audits may achieve greater relevance to stakeholders and greater acceptance as a useful form of assurance.

8.2: ADDRESSING THE RESEARCH QUESTIONS

The research questions aim to investigate the similarities and differences between the practices of different privacy auditors. The research also strives to suggest improvements to the practice of privacy auditing that may make privacy audits more relevant to stakeholders.

The research questions are:

1. What auditing standards and/or methodologies are used for privacy audits, where are they derived from, and how much convergence and/or divergence is there among standards used by different auditors?

2. Who benefits from privacy audits and are privacy audits an appropriate way to provide benefits to them?

The research questions are examined through the lens of Critical Theory. This is an important perspective for this thesis because it allows the analysis to critique the practice of privacy auditing and to suggest improvements. Positivist research on the practice of privacy auditing faces significant challenges at present, including the lack of theory in a developing area. There is also a general lack of numerical data or other hard forms of evidence. It may be observed that privacy auditing is still in its infancy and the practice has some room to grow. Critical Theory is especially useful for determining the ways in which privacy auditing may improve. Critical Theory seeks to suggest improvements to practices with reference to (changing) social norms.

Consistently with the critical perspective in relation to the research questions, this research project builds a set of fundamental principles for privacy auditing that are based on interpretation of recent policy suggestions and proposals for legislative reform regarding information privacy rights. These fundamental principles are used to critique the practices of privacy auditors and to provide a way to measure the differences between what different privacy auditors are doing when they are asked to conduct a privacy audit.

8.3: LEGAL THEORIES

The research questions for this thesis include the standards used for information privacy laws in the countries that are investigated. Some auditors (especially those that are regulators) use information privacy laws in their own particular country as standards for a privacy audit. It is therefore necessary for this research to be alive to the differences between national information privacy laws in the different countries that are examined here. The analysis of

national information privacy laws requires a depth of analysis beyond basic expository skills. Such analysis cannot ignore philosophical legal theories (jurisprudence) regarding what the law consists of.

The jurisprudential theory that is the most natural support for the fundamental principles advanced in this thesis is Dworkin's theory of law as integrity (Dworkin 1977, 119). This theory allows the fundamental principles to be perceived as existing parts of the law and therefore necessary as part of the standards that are used by privacy auditors who focus on national information privacy laws as standards for a privacy audit. However, if a legal positivist perspective is taken then it would be necessary for this thesis to argue for significant changes in the law because in the absence of changes, most of the fundamental principles would be invisible to a privacy auditor who embraces legal positivism. The principles that would be applied by a privacy auditor who gives primacy to legal positivism would therefore be different to those who subscribe to Dworkin's theory of law.

8.4: JURISPRUDENTIAL PERSPECTIVE

Dworkin's theory (Dworkin 1977; 1986) is consistent with the framework of fundamental principles that is constructed in this thesis. These principles are ascertained from the latest pronouncements of policy and suggestions for legislative reform regarding information privacy rights (European Commission 2012; The White House 2015; Federal Trade Commission 2012). There are differences among the proposals and therefore the framework of principles is the best fit that can be achieved. This is done by taking all the principles that have been suggested in each of the five countries that are the subject of this thesis and adding them together. This produces the most comprehensive framework of principles. The broadest conception of each principle is used, and any narrower conceptions of each principle are simply subsumed within the broader principle. Different ideas require separate principles and

there remain seven distinct principles after this process is completed. These are the seven fundamental principles of information privacy that this thesis suggests may be used as suitable criteria for a privacy audit.

The existing information privacy laws in the five countries examined by this thesis are generally much less up to date than the fundamental principles suggested in this thesis. Information privacy laws take significant time to update through legislative channels and they may become out of date again by the time these processes are complete. None of the current information privacy laws in the five countries are completely up to date with the framework of fundamental principles, and some fail to implement the broadest conception of any of the fundamental principles.

Dworkin's theory allows privacy auditors to consider the fundamental principles as part of the law. It is appropriate because of the speed at which conceptions of information privacy must change to keep up to date with the latest expectations of privacy by society as a whole. Privacy auditors may use the fundamental principles as suitable criteria for a privacy audit and this may allow them to judge the appropriateness of the privacy management practices of an auditee organization in a way that is more consistent with modern ideas about information privacy. The law reform process may then have the benefit of fundamental principles that are used in practice by those auditors involved with privacy auditing. The practice of privacy auditing may lead developments in the legal landscape. However, Dworkin's perspective may consider that the fundamental principles are already able to be ascertained as part of the law (even if not specifically enacted). In this sense, privacy auditors are not changing the law themselves, merely applying the correct conception of the law. The fundamental principles as part of the law and the suitable criteria used by privacy auditors may therefore go hand in hand contemporaneously. One need not lead the other if both are using the modern fundamental principles. In this event, the legislation enacted as information

privacy laws in the five countries should still be reformed in order to more obviously reflect the modern principles, but it is not necessary that this happen (though it would make information privacy law clearer to the ordinary citizen who may not be a legal philosopher).

A positivist may take a different view, and may not accept the fundamental principles as part of the law. This would create difficulties for the practice of privacy auditing because it would perpetuate the differences between privacy audits that are done by national regulators (many of whom focus solely on their own national legislation as suitable criteria for a privacy audit). Positivism may reduce the value of privacy auditing to users who may be in a different country to the one in which the privacy audit report is produced.

Privacy issues are increasingly global in nature. The organizations that collect personal data of individuals are often no longer confined to just one jurisdiction. Users of privacy audit reports as well as the organizations that are subject to privacy audits may gain more from a privacy audit that considers information privacy in the context of the latest principles of information privacy. If privacy auditors can develop consensus or near consensus on criteria for privacy audits then the users of the reports may find it easier to assess the relevance of a privacy audit for people in more than one country. Users may then find privacy audits to be of greater relevance to them. This thesis has shown that there is currently little consensus between different privacy auditors on the criteria to be used in a privacy audit. There are also discrepancies between the fundamental principles discussed in this thesis and many of the 30 privacy audit reports that are examined here. This situation imposes limitations on the relevance of existing privacy audit reports.

8.5: EVOLUTION OF INFORMATION PRIVACY RIGHTS

Information privacy rights have become of greater relevance as the technology that can threaten these rights has developed. Although it is becoming less and less possible to prevent

the collection of our personal data, the focus may now turn to responsible management of the information held by the agencies that collect it. Privacy audits are one mechanism through which this management may be supported.

Legal challenges have arisen within Europe and the United States following revelations about the use of personal information by large organizations and the intelligence community. The privacy rights of citizens have been emphasised in cases including *Klayman v Obama*¹²⁷ and *ACLU v Clapper*¹²⁸ and *Google Spain SL v AEPD*.¹²⁹ This indicates an increased level concern by citizens and it also indicates that judges are responding to this concern in judgments. Possibly also responding to this increased level of concern, regulators have imposed privacy audits through their enforcement powers (such as the consent order binding Google).¹³⁰

A factor limiting the harmonization of privacy audit standards has been the lack of consensus in the legal community regarding the theoretical basis for information privacy rights. This is only relevant to the extent that privacy auditors see legal standards as being the epitome of suitable criteria for privacy audits. As is shown in this thesis, privacy auditors that are regulators are often in this camp. In addition to the underdeveloped nature of information privacy rights, such rights also face challenges from the impact of new technologies and innovative business models being adopted by multinational companies that control the data of individual citizens. Information privacy law is ripe for rationalization through enhancement of its jurisprudential theory.

¹²⁷ *Klayman v Obama* [2013] 957 F. Supp. 2d 1, United States District Court for the District of Columbia. Another example is the Supreme Court case brought by the Electronic Privacy Information Center against the National Security Agency (NSA): *In Re Electronic Privacy Information Centre, Petitioner* [2013] 134 S. Ct. 638.

¹²⁸ *American Civil Liberties Union v Clapper* [2015] U.S. App. LEXIS 7531, United States Court of Appeals for the Second Circuit.

¹²⁹ Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) European Court of Justice, 13 May 2014.

¹³⁰ Federal Trade Commission (FTC). 2012. *Statement of the Commission*. Available at: <http://www.ftc.gov/os/caselist/c4336/120809googlestatement.pdf> (site accessed 3 December 2013).

The theoretical basis for information privacy laws that is suggested in chapter 5 of this thesis is based on principles that may underlie and inform our approach to information privacy rights. Many national privacy laws already contain standards that are described as principles. However, most such principles are not up to date with the latest statements in policy documents and proposals for legislative reform in the five countries that are the subject of this thesis. Therefore they are better classed as rules, not principles. The fundamental principles suggested in this thesis are at a higher level of abstraction than many of the currently enacted principles or rules. They have a broad focus which allows for inclusion of the rules that currently exist in all of the five countries. The fundamental principles allow for flexibility because they may be given greater or less weight in order to accommodate social norms within each of the five countries, which may demand a different balancing of interests and therefore could potentially result in outcomes that are different across different countries. However, the fundamental principles could still be the same across the five countries. The weighing process is sophisticated and does not lead to abandonment of the principles if some may be outweighed in a particular case. The use of harmonized principles would produce greater convergence of standards than currently exists between the information privacy laws of the five countries.

Convergence of standards would be of assistance in the context of current debates about the interoperability of accountability mechanisms. There is a concern that lack of international leadership may result in a patchwork of different privacy laws that may unduly restrict the flow of data across different countries (Bygrave 2014, 44). To prevent this, there is pressure to have accountability mechanisms that can be recognised by multiple countries. Initiatives have been suggested by the OECD in the 2013 revision of the OECD privacy guidelines (Bygrave 2014, 47-49) and APEC, which in 2010 established a Cross-Border Privacy Enforcement Arrangement (Bygrave 2014, 78). The APEC initiative also

incorporates a Cross-Border Privacy Rules system which incorporates the concept of Accountability Agents. These agents may certify that an organization has sufficient internal policies to protect personal data that it transfers across national boundaries. However, there has so far been limited uptake of these initiatives (Bygrave 2014, 78). The use by privacy auditors of the fundamental principles suggested in this thesis would assist to promote the interoperability of accountability mechanisms such as privacy auditing and therefore this thesis is particularly relevant in the context of challenges facing information privacy on a global scale.

8.6: DEVELOPMENT OF PRIVACY AUDITING

The development of privacy auditing demonstrates a microcosm of the challenges that have been faced in the development of auditing generally, including developments in the area of financial auditing. In the financial auditing arena, for example, it has been argued that International Standards on Auditing (ISAs) are appropriately principles based, as opposed to rules based (Humphrey, Loft and Samsonova-Taddei 2014, 169) which echoes the argument advanced in chapters 5 and 6 of this thesis.

There have also been suggestions that the financial auditing world should move to “global convergence to high quality standards” (Humphrey, Loft and Samsonova-Taddei 2014, 165). This suggestion is echoed in the challenges that are faced in the area of privacy auditing, as developed in chapter 6 of this thesis. Although financial auditing has not yet adopted a single set of harmonized auditing standards, “the current cacophony of rules that differ from one location to another, and even sometimes conflict with one another, creates an added level of complexity to the conduct of transnational audits, and may prove to be simply unsustainable” (Fraser 2010, 308). Privacy auditing also faces these challenges, and the solution may be similar to that proposed for financial auditing.

Privacy auditing may also draw on the development of assurance of sustainability reports. There are issues that have been identified in relation to assurance of sustainability reporting such as “does risk identification work in the same way as it does for the financial statement audit? How is the process for determining material items changed when considering a variety of subject matter where many significant issues are not capable of being monetized?” (Simnett 2014, 332-333). These issues are very relevant to privacy auditing, which may also struggle with risk identification and flexible subject matter. The concept of multidisciplinary teams and how these work is also an issue for both sustainability and privacy auditing (Simnett 2014, 333).

8.7: CONTRIBUTIONS

This thesis makes several contributions to the literature on privacy auditing. These contributions fall into three broad areas; regulation, policy and theory. In addition to these specific contributions, some chapters of the thesis have been published as papers in academic journals and a chapter has also formed the basis for two conference papers presented by the author in 2015.

The first contribution of the thesis is to the regulation of privacy audits. The thesis argues for harmonization between standards and methodologies used by different privacy auditors. Privacy auditing may be improved by the use of more consistent standards by privacy auditors in different countries. The thesis examines international developments in information privacy best practice and it suggests a framework of fundamental principles that may reconcile the different approaches to information privacy that are taken in the five countries. The goal of this research is to suggest improvements to the practice of privacy auditing and this goal is consistent with the critical perspective of the thesis.

The second contribution of the thesis is to the policy environment surrounding privacy auditing. Chapter 5 of this thesis (Toy 2013) suggests that the latest policy documents and proposals for legislative reform in the five countries are capable of supporting a set of fundamental principles for information privacy that could underlie the information privacy laws in the five countries. The fundamental principles are drawn from official documents in the five countries and because the most modern suggestions come from the US and the EU, the fundamental principles are constructed predominantly from documents in those jurisdictions. Even in the countries that use older standards, such as New Zealand and Australia, the fundamental principles are relevant because under a non-positivist perspective of the law, they could be seen as already being part of the principles of the law in those jurisdictions.

The third contribution that is made by this thesis is to the theory of privacy auditing. Chapter 6 of this thesis (Toy and Hay 2015) examines 30 privacy audit reports that are gathered from publicly available websites in the five countries. It uses the framework of fundamental principles as a benchmark to ascertain whether there is divergence or convergence between the information privacy standards that are used in these reports. The chapter finds that there is considerable divergence between the standards used in many of the reports. It also finds that there is a limited degree of convergence between some of the standards used by different privacy auditors in different countries. This is interesting because it demonstrates that there is the opportunity for convergence of standards even if that is not currently being achieved in the majority of reports. The general degree of divergence demonstrates that significant difficulties exist if users of the reports are in different countries from the one in which the audit report is produced because the audit report may be seen as less useful if the standards used in the report are not applicable across multiple countries.

Chapter 7 of this thesis addresses contemporary issues in the practice of privacy auditing. It identifies a number of different themes or issues in privacy auditing that have not been elucidated in previous academic literature. Firstly, the extent to which there may be harmonization of standards used by different privacy auditors. The chapter examines any possible similarity between standards used by different privacy auditors. It investigates the extent to which privacy auditors are using standards that either converge or diverge from those used by others in the industry. Secondly, the chapter examines the definition of privacy audits. This is broadly scoped to examine the services that are offered by privacy auditors and how similar these services are to each other. Thirdly, the chapter investigates what challenges are faced by the practice of privacy auditing and what methodologies are employed by privacy auditors to meet those challenges. The chapter identifies difficulties faced in terms of the development of privacy audits and whether these difficulties can be overcome by methodologies that are used by different privacy auditors. Fourthly, the chapter analyses the potential for the practice of privacy auditing to move beyond a pure compliance approach. This analysis focuses on whether privacy audits should address only compliance issues or if they should have a broader focus. The chapter also examines the appropriateness of a broader focus, including the possibility that there are best practices for privacy that could be used in privacy audits. Fifthly, the chapter investigates the skills that privacy auditors require. The chapter also investigates whether these skills are readily available in terms of what training and certifications are available for privacy auditors. Sixthly, the chapter examines the privacy maturity assessment framework and how it relates to assignment of resources to managing privacy risks. The relevance of the fundamental principles of privacy auditing suggested in this thesis is part of this analysis. Seventhly, the chapter addresses the benefits of privacy audits to stakeholders. The chapter investigates who these stakeholders are and how privacy audits provide benefits to them. Eighthly, the chapter analyses whether or not privacy audits

can be integrated within the internal risk management operations of an organization, and how external privacy audits may supplement them. Ninthly, the chapter examines the motivating factors underlying the practice of privacy auditing and how they can affect the practice of privacy auditing. Finally, the chapter investigates the basis for privacy impact assessments. As part of this investigation, the chapter exposes the principles that these assessments use and whether these principles relate to the fundamental principles discussed in this thesis.

8.8: CONCLUSION

The practice of privacy auditing has had very little guidance in terms of the standards and methodologies that should be used. Privacy auditors have faced considerable challenges such as the lack of training and certification and the absence of possibilities for peer review. These circumstances have led to fragmentation of approaches to privacy audits. This thesis examines the practice of privacy auditing and it suggests possibilities for alignment of approaches among different auditors. Privacy audits may not follow the suggestions in this thesis but to the extent that they do not then the practice of privacy auditing may struggle to have relevance to a broad class of stakeholders and the ability of privacy audits to suggest improvements to the information management practices of an organization may be more limited. The use of national information privacy legislation as standards for a privacy audit is especially limiting if it does not take account of the more modern fundamental principles of information privacy.

If privacy auditors integrate both the legal requirements in their particular country and the international developments in information privacy best practice into the practice of privacy auditing then the privacy audits that are produced may be able to provide assurance to organizations that operate across multiple jurisdictions. An increased level of international comparability between different privacy audits may make privacy audits more relevant to

stakeholders and this in turn may enhance the privacy management of personal information of citizens. It may also provide a basis for further comparison and debate about best practice in information privacy as further technological challenges arise in the future.

Table 1: List of Interviewees

Name	Country	Role	Date	Duration
Marty Abrams	USA	Executive Director, Information Accountability Foundation	Friday 22 November 2013	56m, 52s
Tanya Allen	Canada	Lead Auditor, Office of the Information and Privacy Commissioner for British Columbia	Tuesday 24 September 2013	55m, 32s (this was the combined interview time for both Tanya Allen and Jay Fedorak)
Malcolm Crompton	Australia	Managing Director, Information Integrity Solutions	Monday 9 September 2013	36m, 32s
Souella Cumming	New Zealand	Partner, KPMG	Thursday 14 November 2013	1h, 1m, 27s
Jay Fedorak	Canada	Assistant Commissioner, Office of the Information and Privacy Commissioner for British Columbia	Tuesday 24 September 2013	55m, 32s (this was the combined interview time for both Tanya Allen and Jay Fedorak)
Neil Sanson	New Zealand	Data Matching Compliance Adviser, Office of the Privacy Commissioner for New Zealand	Thursday 14 November 2013 and Thursday 26 September 2013	44m, 21s and 57m, 1s
Blair Stewart	New Zealand	Assistant Commissioner, Office of the Privacy Commissioner for New Zealand	Thursday 12 September 2013	1h, 23m, 58s

Table 2: Fundamental principles and documents supporting them.

Fundamental principle	Supported by
Privacy by Design	FTC 2012, European Commission 2012, OECD 2011
Respect for Context	The White House 2012
Consent	AICPA and CICA 2009
Transparency	The White House 2012, European Commission 2012
Legitimacy	European Commission 2012
Proportionality	European law (Toy 2013)
Accountability	The White House 2012

Table 3: Evidence of suitable criteria based on fundamental principles of information privacy in privacy audits

Name of Audit Report / Suitable criterion/Fundamental Principle included	Privacy by Design	Respect for Context	Consent	Transparency	Legitimacy	Proportionality	Accountability
Office of the Australian Information Commissioner, <i>Passenger Name Records (PNR data) Australian Customs and Border Protection Service Audit Report (2012)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>National Document Verification Service, Centrelink – Audit Report (2011)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>Australian Federal Police (ACT Policing Branch) Audit Report (2011)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>ACT – Department of Disability, Housing and Community Services, The Office for Children, Youth and Family Support Audit Report (2011)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>National Document Verification Service – Department of Foreign Affairs and Trade – Audit Report 2012 (2012)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>Healthcare Identifiers Service – Medicare Australia Audit Report (2011)</i>	No	No	No	No	No	No	No
Office of the Australian Information Commissioner, <i>Healthcare Identifiers Service – Department of Human Services – Audit Report (2012)</i>	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit of the Personal Information Management Practices of the Canada Border Services Agency Trans-border Data Flows (2006)</i>	No	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>Privacy Audit of Canadian Passport Operations (December, 2008)</i>	No	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>Financial Transactions and Reports Analysis Centre of Canada (December, 2009)</i>	No	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>Audit Report of the Privacy Commissioner of Canada: Assessing the Privacy Impacts of Programs, Plans, and Policies (October, 2007)</i>	Yes	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>Audit Report of the Privacy Commissioner of Canada: Federal Annual Privacy Reports (2009)</i>	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit Report of the Privacy Commissioner of Canada: Passenger Protect Program Transport Canada (2009)</i>	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit Report of the Privacy Commissioner of Canada: Privacy Management Frameworks of Selected Federal Institutions (2009)</i>	No	No	Yes	Yes	No	No	No

Name of Audit Report / Suitable Criterion/Fundamental Principle included	Privacy by Design	Respect for Context	Consent	Transparency	Legitimacy	Proportionality	Accountability
Office of the Privacy Commissioner of Canada, <i>Audit of the Financial Transactions and Reports Analysis Centre of Canada</i> (2009).	No	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>The Protection of Personal Information in Wireless Environments: An Examination of Selected Federal Institutions: Audit Report of the Privacy Commissioner of Canada</i> (2010)	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Personal Information Disposal Practices in Selected Federal Institutions</i> (2010)	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit of Selected Mortgage Brokers</i> (2010)	No	No	Yes	Yes	No	No	No
Office of the Privacy Commissioner of Canada, <i>Staples Business Depot: Audit Report of the Privacy Commissioner of Canada</i> (2011)	No	No	Yes	Yes	No	No	Yes
Office of the Privacy Commissioner of Canada, <i>Privacy and Aviation Security: An Examination of the Canadian Air Transport Security Authority: Audit Report of the Privacy Commissioner of Canada</i> (2011)	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit Report of the Privacy Commissioner of Canada: Examination of RCMP Exempt Data Banks</i> (2008)	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Veterans Affairs Canada: Audit Report of the Privacy Commissioner of Canada</i> (2012)	No	No	No	No	No	No	No
Office of the Privacy Commissioner of Canada, <i>Audit of Selected RCMP Operational Databases: Audit Report of the Privacy Commissioner of Canada</i> (2011)	No	No	No	No	No	No	No
Data Protection Commissioner of Ireland, 'Data Protection in the Department of Social & Family Affairs' (2008)	No	No	No	No	No	Yes	No
Data Protection Commissioner of Ireland, 'Data Protection in the Office of the Revenue Commissioners' (2009)	No	No	No	No	No	Yes	No
Data Protection Commissioner of Ireland, 'Facebook Ireland Ltd: Report of Audit' (2011)	No	No	No	No	No	Yes	No
Data Protection Commissioner of Ireland, 'Facebook Ireland Ltd: Report of Re-Audit' (2012)	No	No	No	No	No	Yes	No
KPMG & Information Integrity Solutions Pty Ltd, 'Independent Review of ACC's Privacy and Security of Information' (2012)	Yes	No	Yes	Yes	No	No	Yes
Deloitte, 'Ministry of Social Development: Independent Review of Information Systems Security Phase 1' (2012)	No	No	No	No	No	No	No
PwC, 'Initial Assessment Report on Google's Privacy Program' (2012)	No	No	Yes	Yes	No	No	Yes

Table 4: Codes and themes

Names in bold become final themes as shown in Figure 1.

Initial code	Name of initial code	Action taken (if any)	Final code or theme	Number of people referring to theme
1	Classification: advisory or assurance	combined with: Definition of Privacy Audits		
2	Privacy impact assessments		10	4
3	Services offered by private firms	combined with: Definition of Privacy Audits		
4	Relevant legislation	combined with: Harmonization of Standards		
5	Actions taken by auditee	combined with: Privacy maturity assessment framework		
6	Offering privacy audit services	combined with: Definition of Privacy Audits		
7	Lack of privacy audit standards	combined with: Harmonization of Standards		
8	Privacy maturity assessment framework		6	2
9	Risk management and internal audit		8	5
10	Impetus for privacy audits		9	5
11	Not a pure compliance approach	renamed as: Beyond a pure compliance approach	4	6
12	Interaction with stakeholders		7	7
13	Privacy audits need further development	combined with: Harmonization of Standards		
14	Reasons why compliance approach not sufficient	combined with: Beyond a pure compliance approach		
15	Performance objectives of an organization	combined with: Risk management and internal audit		
16	Influence of technology	combined with: Harmonization of Standards		
17	Need for harmonization of standards	renamed as: Harmonization of Standards	1	7
18	Differences among privacy auditors	combined with: Privacy audit methodologies		
19	Focus of multinational private auditors	combined with: Privacy audit methodologies		
20	Focus of national regulators	combined with: Privacy audit methodologies		
21	Flexible standards	combined with: Harmonization of Standards		
22	Privacy audit quality	combined with: Privacy audit methodologies		
23	Privacy professionals	combined with: Skills of privacy auditors		
24	Public attitudes to privacy	combined with: Interaction with stakeholders		
25	Types of privacy audit	renamed as: Definition of Privacy Audits	2	6
26	Terminology for privacy audits	combined with: Definition of Privacy Audits		
27	Skills of privacy auditors		5	6
28	Cost of privacy audits	combined with: Skills of privacy auditors		
29	Difference between privacy standards and investigative audit standards	combined with: Harmonization of standards		
30	What privacy audit work entails	renamed as: Privacy audit standards and methodologies	3	7

Figure 1: Codes and Themes

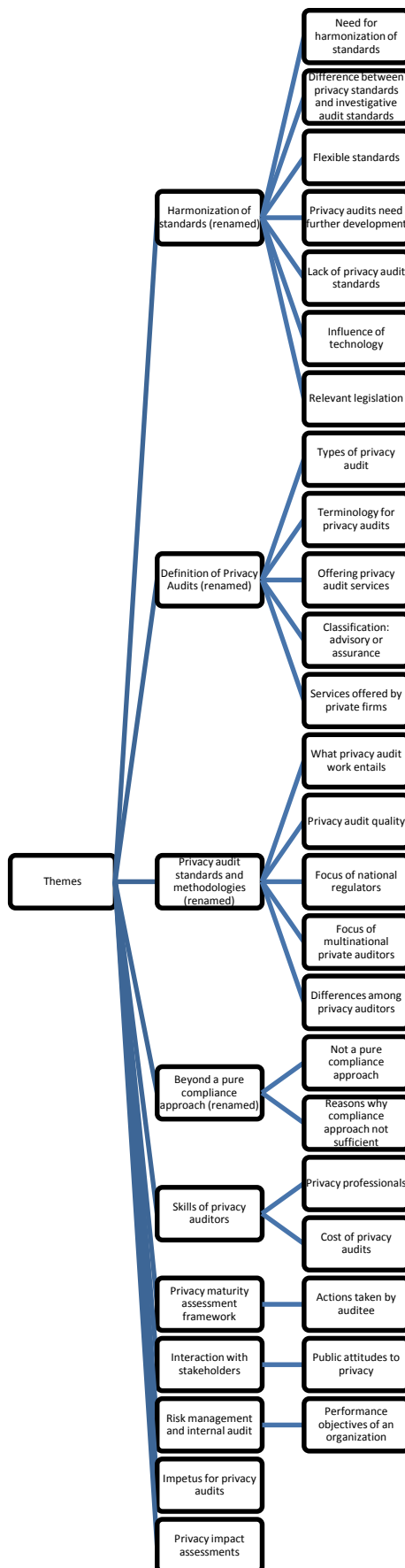


Table 5: Theme definitions and examples of allocated interview text

Theme	Definition of theme	Example of allocated text
Harmonization of Standards	Is there any similarity between standards used by different privacy auditors? To what extent are privacy auditors using standards that either converge or diverge from those used by others in the industry?	Neil Sanson: <i>there's... at that high level, it takes a long time for wording to be agreed, particularly when you've got different jurisdictions. The American legal approach and the European legal approach are quite different on privacy, so that means that an international standard has to be vague enough to be applied to either jurisdiction. And again, that's where the auditor has to tailor to the local laws, and then, at the next level down, to the organization they're auditing, and what sort of information it holds. So you need to do that focusing down</i>
Definition of Privacy Audits	What services are offered by privacy auditors and how similar are these services? Is it necessary to define the term "privacy audit" with a high degree of specificity?	Jay Fedorak: <i>well I think I'd have... first of all have to clarify that, up to today, we have conducted what would be more appropriately characterised as investigations, but we are just at the beginning stages of developing a more formal audit program. We, several months ago, hired Tanya as a Senior Investigator, Audit and Compliance, to help us develop and implement an audit program, so at this point, we... there may be some individuals in the sort of professional auditing community who, if they looked at our investigations up to this point, might conclude that we haven't in fact actually done what could be appropriately described as an "audit" yet, but we're moving towards that. But we have conducted a number of investigations where we go in and measure the compliance of organizations and public with their requirements under the legislation that we've been tasked to oversee. And, in doing so, we have conducted sort of thorough investigations where we're looking at policies, procedures, training, practices, and so we've done some fairly in depth investigations, and some people might use the term "audit" in a really loose fashion. Our own legislation does use the term "audit", but it doesn't really define what an audit would consist of, so...</i>
Privacy audit standards and methodologies	What difficulties are faced in terms of the development of privacy audits? Can these difficulties explain any of the problems faced by privacy audits? What methodologies are used by different privacy auditors and are these capable of overcoming the problems? Will this have benefits to organizations that are subject to privacy audits? Will this improve the quality of privacy audits?	Souella Cumming: <i>well, I'm not sure that there are... that there is anything particular in place about improving privacy audit quality because there's no real community of practice around privacy auditing as I say, it's regulators do it, and they do it in a certain way, and the firms do it, and they do it in a certain way... I think, the reason for that is that at the moment, the focus is on improving privacy quality or management of privacy in... by organizations, which has to happen first. I mean, an audit certainly can highlight gaps etcetera. But if the organization is not committed to managing personal information more effectively, or, you know, in a different way then, you know. So audit... the audit quality question, I don't think... I'm not aware of anything in that context.</i>
Beyond a pure compliance approach	Should privacy audits address mere compliance issues or should they have a broader focus? What should a broader focus consist of? In what ways would a broader focus be more appropriate for a	Souella Cumming: <i>...but Malcolm and I have a, you know, we both share the same sort of philosophical base that actually this is an organizational issue, it's not a... you know, it's not owned by the privacy team, or it's not a legislative compliance aspect. It's about how you interact with your customer or your stakeholders and how you design your organization to make sure that you're doing that in a way that you do respect the</i>

	privacy audit? Are there best practices for privacy?	<i>individual in terms of their, you know, personal information. But also that you do comply. You know, so the compliance is kind of the result. If you design things properly, yes it's going to ensure compliance, but starting with the compliance aspect we didn't think was useful to ACC.</i>
Skills of privacy auditors	What skills do privacy auditors require? Are there a substantial number of people with these skills? Are there ways for organizations to verify the skills of privacy auditors? Are there training courses for privacy auditors?	Jay Fedorak: <i>well, we don't actually have any accountants in the office, and we don't have anyone with professional accounting certification. Tanya has done performance audits in other areas in government, so she's bringing performance auditing skills with her into the office. The rest of the staff are going to have technical expertise with respect to the legislation and also general investigative expertise. So we're, in addition to being the lead on the development of the auditing program in terms of the methodology and the standards, Tanya's also going to be the real lead of the auditing team, and going to be doing some coaching and professional development by having the other... working directly with the other investigators and conveying her expertise, sort of, on the job.</i>
Privacy maturity assessment framework	What is privacy maturity assessment? How does it relate to assignment of resources to managing privacy risks? How does it relate to the fundamental principles of privacy auditing suggested in this thesis?	Souella Cumming: <i>But the other area that we have been working on, and this came through from the ACC independent review last year, was looking at organizations and providing them... doing what we call a maturity assessment of their approach to understanding of privacy. So that is, we look at a range of elements and assess the organization in terms of the maturity scale. So, you know, from sort of, KPMG's approach is based on a five scale from, you know, just that basic or ad hoc level through to a... you know, advanced and continuous improvement.</i>
Interaction with stakeholders	Who are the beneficiaries of privacy audits? How do privacy audits provide benefits to these parties?	Jay Fedorak: <i>[but], what our ultimate goal is with doing this is to achieve a greater level of compliance with the requirements of the legislation. And with a greater level of compliance, less likely to be privacy risks, risks of breaches, improper collection, use or disclosure of individuals' personal information. And so therefore it's the individuals whose personal information is at stake are the ones that are going to benefit the most. I guess, the result of the audit... organizations, whether they're the ones being audited, or the ones that read the outcome of our audit and decide that they're going to try and get their houses in better order as a result and are going to make changes based on the recommendations that we've put in the audit, or are going to learn from some of the issues that the audit uncovers so that they can make their own improvements in that sense. The organization itself, by having a better level of compliance, will benefit again from the, you know, increased level of security for their information, reduced chances of there being some kind of breach because breaches, in addition to causing a certain level of embarrassment for those in authority within the organization, often result in significant real financial costs in terms of sometimes financial compensation, sometimes the remedial action that's required when a breach happens, involves, you know, financial outlay. So in that sense, the organization themselves will also benefit.</i>

Risk management and internal audit	Can privacy audits be integrated within the internal risk management operations of an organization? How can these relate to external privacy audits?	Neil Sanson: <i>The advantage of the internal people is they know the organization well. The advantage of bringing in external people is they tend to have a bit more technical knowledge, and they also have experience with a variety of organizations. So there's actually advantages to both. Almost ideally, you'd want to, even if you normally used internal audit, you'd want to occasionally use an external provider. Using an external provider every year though would be quite expensive, and you have the disadvantage that generally they will not build up an accumulated understanding. One advantage of internal audit people is since they often will do the same audit more than once over the years, they will already have a good understanding when they they come into it the second or third time. And as I say, they'll often dig a bit further then, because they don't have to go over the same ground to get the basic understanding in quite the same depth because they already know that. They just need to confirm that their understanding is still valid, things haven't changed since they previously looked at it. And then they have time in their engagement to look a little bit wider</i>
Impetus for privacy audits	What are the drivers of privacy auditing? How can the motivating forces behind privacy audits influence the practice of privacy auditing?	Marty Abrams: <i>it depends on why you're doing the audit, ok? If I'm doing an audit to report to the Federal Trade Commission [because] I have to do an audit every other year and report the results of that, the fact that the results are going to be reported to the FTC means that if you are afraid of being found not in compliance with an FTC order then you have a high desire for the audits to be done in a fashion that truly is robust. But if I'm just trying to say to the outside world: you can trust us because we have audits of our program, I think that's problematic.</i>
Privacy impact assessments	What is a Privacy Impact Assessment and what principles do they follow? How do these principles relate to the fundamental principles discussed in this thesis?	Blair Stewart: <i>well I think, yeah, I mean you might almost need a terminology to make a distinction between those two things because I don't think everyone is distinguishing. But I think they are quite different. I mean, they might, at the end of the day, not be that different in their methodologies, I don't know. But certainly their objectives, and their duration, is different. One is to do with, it's being part and parcel of a compliance system in an organization. You know, it's not good enough just to have privacy impact assessment in your organization if you don't have a system for implementing that and then, you know, following it through, and then feeding the information back around again an what not. Just as it would be no good just having a privacy audit, and not having some process for judging changes.</i>

Table 6: Summary table for issues relating to privacy auditing sourced from interview data:

<i>Principles</i>	<i>Standards and rules, including use of auditing tools</i>	<i>Practice (operating issues, specifically affecting the practice and practitioners)</i>	<i>Implications for the future development of privacy auditing</i>
Older standards (such as the OECD principles) are not sophisticated enough to deal with current issues such as the concept of proportionality. APEC's principles do not adequately address issues of weight between different principles	Divergence currently exists between standards applied by privacy auditors, especially between those standards applied by regulators and other auditors. The general approach of regulators gives greater importance to the legislative requirements in an individual jurisdiction than the approach taken by some of the non-regulator privacy auditors does	Different privacy auditors approach privacy audits differently, mainly because standards don't exist. Some legislation is not specific enough to produce a standard approach	It may be that information privacy has not yet reached the maturity to have harmonized standards. However, with technology as a driver, pressure may increase to develop global standards (for example: data is now being stored offshore in the cloud, and many entities now have customers in different countries).
The use of global best practices for a privacy audit, beyond merely a compliance approach measured against national legislation, is evidence of the use of fundamental principles which include the concept of privacy by design	Harmonization of privacy auditing standards would be a good thing for privacy audits but it would be difficult to achieve with respect to substantive privacy standards, though it may be easier to achieve with respect to investigative audit standards	Privacy auditors face a major challenge which is that this is a new area and therefore there is a lack of experience to guide the practice	The differences between privacy audits by regulators and those by private organizations may hinder efforts to develop a community of practice for privacy auditing
The auditor must understand governance processes, which means going beyond privacy principles	International standards could be a starting point from which more detailed rules could be developed in each particular country	Privacy audits do not have a single universally agreed definition	A small number of talented people have the skills to conduct privacy audits but they may not be visible to companies

<p>The New Zealand Privacy Assessment Maturity Framework (GCIO 2014) was developed by KPMG and a public sector working group. It could contribute to standards against which the privacy maturity of an organization may be assessed and some of the standards it uses are consistent with the fundamental principles advanced in this thesis</p>	<p>ISO (International Standards Organization) standards may have potential for being a global standard in this area, but not all of the interviewees were in favour of ISO standards</p>	<p>Flexibility is required in privacy audits</p>	<p>There is currently a lack of formal training for privacy professionals which may impede the development of this profession</p>
<p>Regulators may take confidence in the results of a privacy audit report, and the public may also take confidence from the results if the report is available to them. In addition to Accountability, the principle of Transparency is also served by making a privacy audit report public</p>	<p>There needs to be flexibility in privacy audit standards because of the great variety of companies being audited</p>	<p>A privacy auditor may examine just one area of the organization at a time, as part of a process of continuous audits. However, audits may also be one-off investigations that examine the whole organization</p>	<p>It is important to develop the privacy understanding of executive management because executive management have the greatest influence over whether or not an organization decides to improve its privacy practices, or to have a privacy audit in the first place</p>
	<p>The Big Four audit firms have a global presence which translates into their privacy audit program in their view of what standards are appropriate for a privacy audit</p>	<p>Privacy audits may be limited to particular data flows of classes of data across the organization (such as the data relating to a particular group of consumers) and/or they may examine particular areas of a business or particular systems within an organization</p>	<p>Pressure from lawmakers may lead to more rigorous privacy audits, especially if that pressure is in the form of a legal requirement to conduct a privacy audit</p>

	<p>Privacy as an organizational issue affects how an organization interacts with its stakeholders and how it is designed to allow privacy issues to be properly managed</p>	<p>Privacy audits may be followed by action by the auditee organization to address the recommendations in the privacy audit report, but this is not always the case</p>	
	<p>An implementation of privacy as an organizational issue may assist an auditor to conduct a privacy audit in a more sophisticated way than a mere compliance audit</p>	<p>Privacy audit methodologies by private auditors may require the auditee organization to produce documents that detail its understanding of privacy issues and implementation of these in its privacy management practices</p>	
	<p>If an organization understands privacy as an organizational issue, and takes steps to implement this correctly, then the privacy risks it faces are lower</p>	<p>Privacy auditors may conduct interviews with relevant staff members of the auditee organization</p>	
	<p>An auditor must take into account national laws in the country in which the privacy audit is conducted, and possibly also national laws in other countries in which the auditee does business</p>	<p>Privacy as an organizational issue includes all the staff within the organization having responsibility for the privacy management processes within the organization</p>	
	<p>Privacy maturity assessments involve examination of how mature is an organization's understanding of privacy issues and implementation of appropriate controls</p>	<p>Privacy as an organizational issue reflects the understanding of the organization of a whole as to the privacy issues that are relevant to it and its customers</p>	

	Private organizations that conduct privacy audits may focus the audit on identifying privacy risks and on assessing the controls within the organization that mitigate those risks	Privacy auditing is an iterative process which involves the privacy auditor forming some initial conclusions, then seeking feedback from the organization before refining those conclusions	
		Governance and accountability processes are an important aspect of a privacy audit, as well as the risks to an organization	
		Information may be collected from reviews of files and site inspections as well as interviews	
		Some moves are occurring to improve the training of privacy professionals. Currently there are only a few scattered papers about privacy	
		Private audit firms conduct privacy audits using teams that consist of people who are experienced auditors and people who have privacy expertise	
		Privacy regulators/enforcement bodies are beneficiaries of privacy audits	
		Privacy audit reports may be made public, so that the public can then assess the organization's privacy management practices by reading the report	

		The organization may be considered to be a secondary beneficiary of a privacy audit due to having the ability to implement the suggestions in the audit report to reduce the likelihood of a privacy breach	
		Privacy auditors themselves may also benefit from privacy audits because they may gain increased skills in conducting audits	
		A combination of both internal and external privacy audits may be of greater assistance to an organization than just one type alone	
		The Big Four audit firms do privacy impact assessments, often as part of their advisory activities, but these may also be considered assurance activities. They focus on new policies and business processes and appropriate controls for management of privacy within that	

Appendix 1: Interview questions – research on privacy audits

- 1) Thanks for agreeing to be interviewed
- 2) Refer to Participant Information Sheet and Consent Form information
- 3) This interview is being recorded
- 4) Any questions before we start?
- 5) Please explain the nature of the privacy audit services provided by your organization?
- 6) What is your role in relation to the provision of privacy audit services?
- 7) What standards are used by your organization in conducting a privacy audit?
- 8) What challenges exist to the creation of standards?
- 9) What methodologies are used by your organization in conducting a privacy audit?
- 10) What challenges exist to the creation of methodologies?
- 11) What factors are used by your organization to improve privacy audit quality?
- 12) In your opinion, how effective are the factors used to improve privacy audit quality?
- 13) In your opinion, who are the people most likely to benefit from a privacy audit?
- 14) In your opinion, are privacy audits the most effective way to provide such benefits to those people?
- 15) Have there been any recent changes in information privacy laws in this jurisdiction that may affect the standards and methodologies that your organization will use in privacy audits?
- 16) Are there any other people in your organization that you think it would be useful for us to discuss privacy audit services with?
- 17) Would it be possible to have a follow up interview at some later time?

REFERENCE LIST

- Abdel-Khalik, A. 1993. Why Do Private Companies Demand Auditing? A Case for Organizational Loss of Control. *Journal of Accounting, Auditing & Finance* 8 (1): 31-51.
- Alvesson, M., & Willmott, H. (Eds.). (2003). *Studying management critically*. London, Sage.
- American Institute of Certified Public Accountants (AICPA). 2006. *International Legislative Privacy Developments*. Available at: http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/privacyservices/downloadabledocuments/9568b395_intlprivac.pdf (site accessed 24 August 2013).
- American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA and CICA). 2009. *Generally Accepted Privacy Principles; CPA and CA Practitioner Version*, Available at: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_PRAC_%200909.pdf (site accessed 27 May 2015).
- American Institute of Certified Public Accountants (AICPA). 2012. *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing, Integrity, Confidentiality, or Privacy (SOC 2sm), with conforming changes as of March 1, 2012*. New York, NY: American Institute of Certified Public Accountants, Inc.
- APEC Secretariat (APEC). 2005. *APEC Privacy Framework*. Available at: http://publications.apec.org/publication-detail.php?pub_id=390 (site accessed 3 October 2014).
- Asia-Pacific Economic Cooperation (APEC), 29th Electronic Commerce Steering Group. 2014. *APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System - Draft Endorsement Request*, Available at: http://mddb.apec.org/Documents/2014/ECESG/ECESG1/14_ecsg1_013.pdf (site accessed 3 March 2015).
- Australian Law Reform Commission (ALRC). 2008. *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*. Canberra: Paragon Group.
- Baker, C. R., and M. S. Bettner. 1997. Interpretive and critical research in accounting: A commentary on its absence from mainstream accounting research. *Critical Perspectives on Accounting* 8 (4): 293-310.
- Bean, L., and D. Hott. 2006. An Internal Audit Focus on Privacy Policies. *Internal Auditing* 21 (2): 20-26.
- Bender, D., and L. Ponemon. 2006. Binding Corporate Rules for Cross-Border Data Transfer. *Rutgers Journal of Law & Urban Policy* 3 (2): 154-171.
- Bennett, C., and C. Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot, UK: Ashgate Publishing Limited.
- Boritz, E., and W. No. 2011. E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery. *Journal of Information Systems* 25 (2): 11-45.
- Braun, V., and V. Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3 (2): 77-101.
- Bygrave, L. 2002. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague, The Netherlands: Kluwer Law International.
- Bygrave, L. 2014. *Data Privacy Law: An International Perspective*. Oxford, United Kingdom: Oxford University Press.
- Cavoukian, A., and A. Stoianov. 2014. *Privacy by Design Solutions for Biometric One-to-Many Identification Systems*. Available at: <http://www.ryerson.ca/pbdi/privacy-by-design/resources.html> (site accessed 1 March 2016).

- Chow, C. 1982. The Demand for External Auditing: Size, Debt and Ownership Influences. *The Accounting Review* 57 (2): 272-291.
- Chua, W. F. 1986. Radical developments in accounting thought. *The Accounting Review* 61 (4): 601-632.
- Cohen, J. and R. Simnett. 2015. CSR and Assurance Services: A Research Agenda. *Auditing: A Journal of Practice & Theory* 34 (1): 59-74.
- Clegg, S. 2006. *The Sage Handbook of Organization Studies*. London, Sage.
- Cloud Security Alliance. 2014. *Data Protection Heat Index Survey Report, September 2014*. Available at: <https://cloudsecurityalliance.org/download/data-protection-heat-index-survey-report/> (site accessed 1 December 2014).
- Cortez, P., and D. Hay. 2014. Privacy Disclosure and Auditing: An Exploratory Study. Available at SSRN: <http://ssrn.com/abstract=2271871> or <http://dx.doi.org/10.2139/ssrn.2271871> (site accessed 25 August 2013).
- Davidson, C. 2009. Transcription: Imperatives for Qualitative Research. *International Journal of Qualitative Methods* 8 (2): 35-52.
- Deloitte. 2012. *Ministry of Social Development Independent Review of Information Systems Security*. Available at: <http://www.msd.govt.nz/documents/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-deloitte.pdf> (site accessed 16 April 2013).
- Duncan, P. 2011. Unfriends of Facebook unite. *The Irish Times* 15 Oct: B3.
- Dworkin, R. 1977. *Taking Rights Seriously*. London, Duckworth.
- Dworkin, R. 1978. *Taking Rights Seriously*. London: Duckworth.
- Dworkin, R. 1986. *Law's Empire*. London, Fontana Press.
- Elliott, R. 1997. Assurance Service Opportunities: Implications for Academia. *Accounting Horizons* 11 (4): 61-74.
- European Commission. 2010. *Communication from the Commission to the European Parliament, the Council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union*. Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (site accessed 29 September 2014).
- European Commission. 2012. *Proposal for a Regulation of the European Parliament and of the 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)*. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. (site accessed 2 September 2013).
- Federal Trade Commission (FTC). 2011. *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network*. Available at: <http://www.ftc.gov/opa/2011/03/google.shtm> (site accessed 30 August 2013).
- Federal Trade Commission (FTC). 2012. *Protecting Consumer Privacy in an Era of Rapid Change; Recommendations for Businesses and Policymakers*. Available at: <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> (site accessed 30 August 2013).
- Federal Trade Commission (FTC). 2013. *Mobile Privacy Disclosures: Building Trust Through Transparency*. Available at: <http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf> (site accessed 3 October 2014).

- Federal Trade Commission (FTC). 2014. *Data Brokers: A Call for Transparency and Accountability*. Available at: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> (site accessed 16 June 2015).
- Farrar, J. 2010. *Legal Reasoning*. Sydney, NSW: Thompson Reuters (Professional) Australia Limited.
- Flaherty, D. 1989. *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: University of North Carolina Press.
- Foucault, M. 1983. Afterword: The Subject and Power. In *Michel Foucault: Beyond Structuralism and Hermeneutics*, edited by H. Dreyfus, and P. Rabinow. Chicago, USA: The University of Chicago Press.
- Fraser, N. 2010. A single set of worldwide auditing standards: The road is long.... *International Journal of Disclosure and Governance* 7 (4): 298-309.
- Free, C., S. Salterio, and T. Shearer. 2009. The construction of auditability: MBA rankings and assurance in practice. *Accounting, Organizations and Society* 34 (1): 119-140.
- Freeman, R. 2015. *President Obama Turns His Attention to Privacy*. Available at: <https://privacyassociation.org/news/a/president-obama-turns-his-attention-to-privacy/> (site accessed 16 January 2015).
- Gaffikin, M. 2008. *Accounting Theory: Research, regulation and accounting practice*. Frenchs Forest, NSW, Pearson Education Australia.
- Gelinas, U. 1978. *Privacy Audits and the Certified Public Accountant (PhD Thesis)*. Ann Arbor, MI: University of Massachusetts Amherst.
- Government Chief Information Officer (GCIO). 2014. *Privacy Management in Government*. Available at: <https://www.ict.govt.nz/assets/Guidance-and-Resources/Privacy-Framework-August-online.pdf> (site accessed 10 April 2015).
- Gray, R., and M. Milne. 2015. It's not what you do, it's the way that you do it? Of method and madness. *Critical Perspectives on Accounting* (forthcoming).
- Greenleaf, G. 1994. Private Parts. *Privacy Law and Policy Reporter* 1 (7): 140.
- Greenleaf, G. 1996. Telstra's First Privacy Audit: B-. *Privacy Law and Policy Reporter* 3 (5): 97.
- Gunasekara, G. 2007. The 'final' privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology* 15 (3): 362-394.
- Gunasekara, G., and A. Toy. 2011. Principles or Rules: the Place of Information Privacy Law. *New Zealand Universities Law Review* 24 (4): 525-549.
- Gunasekara, G. 2013. Privacy as a Stakeholder Interest in New Zealand: Transparency in Corporate Governance Practices. *New Zealand Business Law Quarterly* 19 (4): 271-293.
- Haines, J. 1996. Telstra's Privacy Audit. *Privacy Law and Policy Reporter* 3 (4): 64.
- Hart, HLA. 2012. *The Concept of Law* (3rd ed). Oxford: Oxford University Press.
- Hay, D., W. R. Knechel and M. Willekens. 2014. The future of auditing research. In *The Routledge Companion to Auditing*, edited by D. Hay, W. R. Knechel and M. Willekens, 351-357. Abingdon, Oxon: Routledge.
- Hill, K. 2011. So, What Are These Privacy Audits That Google And Facebook Have To Do For The Next 20 Years? *Forbes.com*. Available at: <http://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/> (site accessed 25 August 2013).

- Huggins, A., W. Green, and R. Simnett. 2011. The Competitive Market for Assurance Engagements on Greenhouse Gas Statements: Is There a Role for Assurers from the Accounting Profession? *Current Issues in Auditing* 5 (2): A1-A12.
- Hui, K., H. Teo, and S. Lee. 2007. The Value of Privacy Assurance: an Exploratory Field Experiment. *MIS Quarterly* 31 (1): 19-33.
- Humphrey, C., A. Loft and A. Samsonova-Taddei. 2014. Not just a standard story; The rise of international standards on auditing. In *The Routledge Companion to Auditing*, edited by D. Hay, W. R. Knechel and M. Willekens, 161-178. Abingdon, Oxon: Routledge.
- Jamal, K., M. Maier, and S. Sunder. 2003. Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market. *Journal of Accounting Research* 41 (2): 285-309.
- Jamal, K., M. Maier, and S. Sunder. 2005. Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom. *Journal of Accounting Research* 43 (1): 73-96.
- Jerskey, P. et al. 1996. A Privacy Audit Primer. *EDPACS* 23 (9): 1-8.
- Knechel, W., and M. Willekens. 2006. The Role of Risk Management and Governance in Determining Audit Demand. *Journal of Business Finance & Accounting* 33 (9-10): 1344-1367.
- KPMG & Information Integrity Solutions Pty Ltd (KPMG and IIS). 2012. *Independent Review of ACC's Privacy and Security of Information*. Available at: http://www.acc.co.nz/PRD_EXT_CSMP/groups/external_communications/documents/reference_tools/wpc114897.pdf (site accessed 16 April 2013).
- Kuner, C. 2007. *European Data Protection Law: Corporate Compliance and Regulation (Second Edition)*. Oxford: Oxford University Press.
- Kuner, C. 2013. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.
- Kvale, S. 2007. *Doing Interviews*. London: SAGE.
- LaRose, R., and N. Rifon. 2006. Your privacy is assured – of being disturbed: websites with and without privacy seals. *New Media and Society* 8 (6): 1009-1029.
- Lennox, C., and J. Pittman. 2011. Voluntary Audits versus Mandatory Audits. *The Accounting Review* 86 (5): 1655-1678.
- Mayer-Schonberger, V., and K. Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. New York, USA: Houghton Mifflin Harcourt.
- McCain, J. 2011. *Kerry, McCain Introduce Commercial Privacy Bill of Rights*. Available at: <http://www.mccain.senate.gov/public/index.cfm/press-releases?ID=4a92a6f4-daf7-2f4a-84e7-3eb83276af23> (site accessed 9 March 2015).
- Myers, M. 2013. *Qualitative Research in Business & Management Second Edition*. London: SAGE.
- Myers, M., and M. Newman. 2007. The qualitative interview in IS research: Examining the craft. *Information and Organization* 17 (1): 2-26.
- Nanos, N. 2003. Performing a Privacy Audit. *EDPACS* 30 (10): 1-13.
- New Zealand Law Commission (NZLC). 2010. *Issues Paper 17, Review of the Privacy Act 1993; Review of the Law of Privacy Stage 4*. Available at: www.lawcom.govt.nz (site accessed 10 March 2015).
- New Zealand Law Commission (NZLC). 2011. *Report 123, Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*. Available at: www.lawcom.govt.nz (site accessed 10 March 2015).

O'Dwyer, B. 2004. Qualitative Data Analysis: Exposing a process for transforming a 'messy' but 'attractive' 'nuisance'. In *A real life guide to accounting research: A behind the scenes view of using qualitative research methods*, ed. C. Humphrey and B. Lee, 391-407. Amsterdam: Elsevier.

O'Dwyer, B. 2011. The Case of Sustainability Assurance: Constructing a New Assurance Service. *Contemporary Accounting Research* 28 (4): 1230-1266.

Oliver, D., J. Serovich, and T. Mason. 2005. Constraints and Opportunities with Interview Transcription: Towards Reflection in Qualitative Research. *Social Forces* 84 (2): 1273-1289.

OECD Council (OECD). 1980. *OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*. Available at: www.oecd.org/internet/interneteconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm (site accessed 1 October 2014).

OECD Council (OECD). 2007. *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*. Available at: <http://www.oecd.org/internet/ieconomy/38770483.pdf> (site accessed 3 October 2014).

OECD Working Party on Information Security and Privacy. 2011. *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*. Available at: <http://www.oecd.org/sti/ieconomy/47683378.pdf> (site accessed 24 August 2013).

Office of the Australian Information Commissioner (OAIC). 2011. *Privacy Performance Assessment Manual*. Available at: <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/privacy-performance-assessment-manual> (site accessed 16 August 2013).

Office of the Australian Information Commissioner (OAIC). 2012. *Passenger Name Records (PNR data) Australian Customs and Border Protection Service Audit Report*. Available at: <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/passenger-name-records-pnr-data-australian-customs-and-border-protection-service-audit-report> (site accessed 27 May 2015).

Office of the Data Protection Commissioner of Ireland. 2008. *Data Protection in the Department of Social & Family Affairs*. Available at: <http://www.dataprotection.ie/viewdoc.asp?m=p&fn=/documents/AUDITS/AuditReports.htm>. (site accessed 2 September 2013).

Office of the Data Protection Commissioner of Ireland. 2009. *Data Protection in the Office of the Revenue Commissioners*. Available at: <http://www.revenue.ie/en/about/data/data-protection-commissioner-report.pdf> (last accessed May 19, 2015).

Office of the Data Protection Commissioner of Ireland. 2011. *Facebook Ireland Ltd; Report of Audit*. Available at: <http://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf> (site accessed 27 May 2015).

Office of the Data Protection Commissioner of Ireland. 2012. *Facebook Ireland Ltd; Report of Re-Audit*. Available at: http://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf (site accessed 27 May 2015).

Office of the Data Protection Commissioner of Ireland. 2014. *Guide to Audit Process*. Available at: <http://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf> (site accessed 3 October 2014).

Office of the Privacy Commissioner of Canada. 2001. *Review of the Personal Information Handling Practices of the Canadian Firearms Program*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2006. *Audit of the Personal Information Management Practices of the Canada Border Services Agency Trans-border Data Flows*. Available at: https://www.priv.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp (site accessed 27 May 2015).

Office of the Privacy Commissioner of Canada. 2007. *Audit Report of the Privacy Commissioner of Canada: Assessing the Privacy Impacts of Programs, Plans, and Policies*. Available at: https://www.priv.gc.ca/information/pub/ar-vr/pia_200710_e.asp (site accessed 27 May 2015).

Office of the Privacy Commissioner of Canada. 2008a. *Privacy Audit of Canadian Passport Operations*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2008b. *Audit Report of the Privacy Commissioner of Canada: Examination of RCMP Exempt Data Banks*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2009a. *Audit of Federal Annual Privacy Reports*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2009b. *Audit of Passenger Protect Program, Transport Canada*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2009c. *Privacy Management Frameworks of Selected Federal Institutions*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2009d. *Financial Transactions and Reports Analysis Centre of Canada*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 20 November 2013).

Office of the Privacy Commissioner of Canada. 2010a. *Personal Information Disposal Practices in Selected Federal Institutions*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2010b. *Audit of Selected Mortgage Brokers*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2010c. *The Protection of Personal Information in Wireless Environments: An Examination of Selected Federal Institutions*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2011a. *Staples Business Depot*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2011b. *Audit of Selected RCMP Operational Databases*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2011c. *Privacy and Aviation Security: An Examination of the Canadian Air Transport Security Authority*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Office of the Privacy Commissioner of Canada. 2012. *Veterans Affairs Canada*. Available at: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp (site accessed 2 September 2013).

Pavlou, P. 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly* 35 (4): 977-988.

Power, M., R. Laughlin, and D. Cooper. 2003. Accounting and Critical Theory. In *Studying Management Critically*. M. Alvesson and H. Willmott, 132-156. London: SAGE.

Prah, P. 2014. Target's data breach highlights state role in privacy. *USA Today* (February 10). Available at: <http://www.usatoday.com/story/news/nation/2014/01/16/target-data-breach-states-privacy/4509749/> (site accessed 8 September 2014).

President's Council of Advisors on Science and Technology. 2014. *Big Data and Privacy: A Technological Perspective*. Available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (site accessed 13 May 2014).

PwC. 2012. *Initial Assessment Report on Google's Privacy Program*. Available at: <http://www.informationweek.com/security/privacy/google-privacy-audit-leaves-lingering-qu/240008622> (site accessed 17 April 2013).

Radcliffe, V. 1999. Knowing efficiency: the enactment of efficiency in efficiency auditing. *Accounting, Organizations and Society* 24 (4): 333-362.

Raz, J. 2009. *Between Authority and Interpretation*. Oxford: Oxford University Press.

Ross, L., and M. Friedman. 2006. HIPAA privacy audit tool. *Healthcare Financial Management* 60 (2): 133-136.

Roth, P. 2010. Data Protection Meets Web 2.0: Two Ships Passing in the Night? *University of New South Wales Law Journal* 33 (2): 532-561.

Rubinfeld, J. 2008. The End of Privacy. *Stanford Law Review* 61 (1): 101-162.

Schmidt, S. 2010. Watchdog to look at "naked scanners"; Privacy of air travelers under scrutiny. Reappointed privacy commissioner launches audit of agency in charge of air-passenger screening. *The Gazette* 2010 (9 Dec): A12.

Schwartz, P., and D. Solove. 2011. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review* 86 (6): 1814-1894.

Shelton, S. 2010. The Case for Privacy Audits. *Internal Auditor* 67 (4): 23-25.

Simnett, R. 2014. Assurance of environmental, social and sustainability information. In *The Routledge Companion to Auditing*, edited by D. Hay, W. R. Knechel and M. Willekens, 325-337. Abingdon, Oxon: Routledge.

Singer, N. 2014. College Applicants Sanitizing Social Media Profiles as More Schools Pry. *The New York Times*. Available at: <http://www.nytimes.com/2014/11/20/technology/college-applicants-sanitize-online-profiles-as-college-pry.html?hp&action=click&pgtype=Homepage&module=mini-moth®ion=top-stories-below&WT.nav=top-stories-below> (site accessed 20 November 2014).

Singleton, T. 2009. IT and Privacy Audits. *ISACA Journal* 5: 1-4. Available at: <http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit/IT-Audit-Basics/Pages/IT-and-Privacy-Audits.aspx> (site accessed 27 May 2015).

Smith, H. J., T. Dinev, and H. Xu. 2011. Information Privacy Research: An Interdisciplinary Review *MIS Quarterly* 35 (4): 989-1015.

Solove, D. 2008. *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press.

Solove, D. and W. Hartzog. 2014. The FTC and the New Common Law of Privacy. *Columbia Law Review* 114 (4): 583-676.

The Centre for Information Policy Leadership; Hunton & Williams. 2011. *Accountability: A Compendium for Stakeholders*. Available at: <http://informationaccountability.org/wp-content/uploads/Centre-Accountability-Compendium.pdf> (site accessed 16 February 2016).

The President's Review Group on Intelligence and Communication Technologies. 2013. *Liberty and Security in a Changing World*. Available at: <http://www.whitehouse.gov/blog/2013/12/18/liberty-and-security-changing-world> (site accessed 5 January 2015).

The White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Available at: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (site accessed 2 September 2013).

The White House. 2015. *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*. Available at: <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpr-act-of-2015-discussion-draft.pdf> (site accessed 3 March 2015).

Toy, A. 2009. Consent to Online Privacy Policies. *New Zealand Business Law Quarterly* 15 (4): 236-249.

Toy, A. 2010. Cross-border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity. *New Zealand Universities Law Review* 24 (2): 222-238.

Toy, A. 2013. Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy. *New Zealand Universities Law Review* 25 (5): 938-959.

Toy, A. and D. Hay. 2015. Privacy Auditing Standards. *Auditing: A Journal of Practice & Theory* 34 (3): 181-199.

Turner, Bryan S. (Ed). 2006. *Critical Theory*. Cambridge Dictionary of Sociology. Cambridge: Cambridge University Press. Available from: http://search.credoreference.com.ezproxy.auckland.ac.nz/content/entry/cupsoc/critical_theory/0 (site accessed 12 September 2014).

Wright, D., and P. De Hert. (eds). 2012. *Privacy Impact Assessment*. London: Springer.

Wustemann, J., and S. Wustemann. 2010. Why Consistency of Accounting Standards Matters: A Contribution to the Rules-Versus-Principles Debate in Financial Reporting. *ABACUS* 46 (1): 1-27.

Young M., F. Kuo, and M. Myers. 2012. To share or not to share: a critical research perspective on knowledge management systems. *European Journal of Information Systems* 21 (5): 496-511.