Glaring Paradox or Privacy for our Time: Whether Once Public Facts Should Gain Privacy Protection in Law

Kylie Frances Jackson-Cox

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy in Commercial Law, the University of Auckland, 2022

Abstract

The present research asks whether or not once public facts should gain privacy protection in law and concludes that, in appropriate circumstances, they should. The research employs traditional legal research tools like doctrinal research, to articulate and assess the current law regarding privacy, and law reform methodology, to create a package of amendments to New Zealand's privacy laws to ensure that once public facts gain the protection they deserve.

The research has considered the place of once public facts within theoretical concepts of privacy. A literature review of commonly cited theories of privacy and privacy in public has argued that once public facts have been a component of most of the best known concepts of privacy. The research has also considered why society should care about once public facts. The research argues that failure to protect once public facts puts at risk core values at the heart of privacy – liberty, rehabilitation, dignity and autonomy, and can cause substantial harm.

The research then considers whether or not the predominant legal mechanisms for privacy protection in New Zealand can protect once public facts. The analysis considers the statutory protections under the Privacy Act 2020 and the Harmful Digital Communications Act 2015 (HDCA), along with the common law cause of action for public disclosure of private facts. The research determines that appropriate protection for once public facts requires a package of amendments across all of these legal mechanisms, including a new erasure tool in the Privacy Act, refinements to the disclosure tort and amendments to the HDCA. This package of amendments will not only help to protect once public facts in appropriate circumstances, it will bring New Zealand's privacy laws in line with international best practices and contribute to the ongoing development of privacy law in a structured and principled manner for the benefit of all New Zealanders.

It is the present research's linkage between the concepts of privacy and once public facts and its contention that protecting once public facts contributes to supporting the core values of liberty, rehabilitation, dignity and autonomy, as well as the recommended package of law reforms, that make this research an original contribution to New Zealand law.

Dedication

This thesis is dedicated to my children – Nixon and Elspeth. You inspire me every single day.

Acknowledgements

I am grateful to everyone who supported me during the long years of this degree. In particular I wish to acknowledge the people set out below.

My husband Chris, children, family and friends who bore the brunt of the stressful and maddening times when I thought the thesis would never see the light of day, but notwithstanding, supported and inspired me every day.

My supervisors – Associate Professor Gehan Nilendra Gunasekara and Dr Alan Richard Toy – who guided and supported me throughout this journey.

To the anonymous reviewers of my work which has been published. Your thoughtful comments made a real difference to the outcome of that work, and ultimately this thesis.

List of Publishers' Approvals and Third Party Copyright Agreements

The thesis employs parts of the article described below. An email dated 23 September 2020 from Bridget Giblin, Thomson Reuters, advises that copyright is jointly held by Thomson Reuters and the author, and grants permission to include the content in this thesis.

Kylie Jackson-Cox "A 21st Century Right? An Analysis of the Extent to Which New Zealand's Privacy Act 1993 Provides a Right to Be Forgotten" (2019) 28 NZULR 561.

Table of Contents

List of Figures

Glossary

Article 29 Data Protection Working Group Guidelines	Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "*Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales*" C-131/12
BSA	Broadcasting Standards Authority
Canadian Charter	Canadian Charter of Rights and Freedoms 1982
CJEU	Court of Justice of the European Union
Clean Slate Act	Criminal Records (Clean Slate) Act 2004
CP	Communication principle
Disclosure tort	Common law tort action for invasion of privacy by the public disclosure of private facts
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms 1950
ECtHR	European Court of Human Rights
GDPR	Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)
HDCA	Harmful Digital Communications Act 2015
HRA	Human Rights Act 1998 (UK)
IPP	Information privacy principle
NZBORA	New Zealand Bill of Rights Act 1990
NZLC	New Zealand Law Commission
OPC	Office of the Privacy Commissioner (New Zealand)
PIPA	Personal Information Protection Act 2003 (Alberta, Canada)
PIPEDA	Personal Information Protection and Electronic Documents Act 2000 (Canada)
RTBF	Right to be forgotten
Tribunal	Human Rights Review Tribunal
SNS	Social networking site
White Paper	A Bill of Rights for New Zealand: A White Paper
WWW	World Wide Web

1 INTRODUCTION

I Old Problems; New (and Old) Solutions

The issue at the heart of the present research is whether information that has been made public at some point in time (called 'once public facts') – perhaps because the media published an article containing particular information about a person, the information appeared in an official document, or because a person posted the information to a social networking site (SNS) – can obtain protection via the legal mechanisms provided by the law of privacy.

Before the modern information age people commonly relied on the relative obscurity of information to protect it from disclosure. Personal, sensitive or intimate information might be contained in a public document, like a court record, but because that record only existed in hard copy, in a locked file, in an archives room, in the basement of a building, the information was ostensibly protected from disclosure. Only if the information was of vital importance was a person likely to make the effort to find it. Personal information might be published in a national newspaper, but after a day or two the headlines changed and the information eventually faded into people's memories. Personal information might become widely known in a community, but a person who wanted the information forgotten could move away and the chances of the information following them were slight.

Modern information technology has changed this landscape. Old government records have been digitised and put online and new records are commonly generated online. Community gossip is created and distributed on SNSs. Newspaper articles are created and archived online. Information is now considerably easier to find, retrieve and distribute. This information age is to be lauded. It has fundamentally changed so many aspects of our life – the dissemination of information has been democratised,[1] people half a world apart can stay connected, and during a global pandemic, where people have been told to stay away from family and colleagues, a new normal has been enabled .[2] However, like most innovations, modern information technology has created risks. There has been the rise of cyberbullying and trolling, democratic

[1] See David Harvey *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Hart Publishing, Oxford, 2017) at 30.
[2] See Rahui De', Neena Pandey and Abhipsa Pal "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice" (2020) 55 International journal of information management 102171.

processes have been opened up to manipulation[3] and, for the purposes of the present research, it has become difficult for people to leave behind any previous infamy and truly start afresh.

While the issue may appear a thoroughly 21st century one, its genesis in legal discourse was almost 100 years ago, with the case of *Melvin v Reid* in the United States.[4] The fact that the issue has been active for over a century demonstrates a core of concern, a core interest that people wanted to protect in 1930 and still want to protect now.[5] However, what is that core interest? Is the interest still relevant? Is the interest truly related to privacy? Should the interest still be protected by privacy law in the face of the modern information age? What privacy law mechanisms can be used to protect the interests? Are these mechanisms fit-for-purpose? These are the questions ultimately addressed by the present research.

The present research finds that protecting once public facts, in the right circumstances, is squarely within the concept of privacy and privacy law in New Zealand, and at the heart of once public facts are interests worthy of protection – for example, liberty, rehabilitation, dignity and autonomy. However, it is argued that changes to New Zealand's privacy laws are required to provide the right environment for protection and to assist with the development of privacy law in a structured and principled manner.

A considerable amount of legal scholarship exists on privacy and potential solutions to once public facts, like the so-called 'right to be forgotten' (RTBF) and the tort of public disclosure of private information (disclosure tort).[6] However, none of this scholarship has drawn together all the relevant solutions into a unified system or package of amendments to enable appropriate legal protection for the privacy interest in once public facts. The present research does so. The present research provides a ready-made baseline for future law reform that can be adopted by law-makers. It is these factors, along with the theoretical findings regarding privacy, once public facts and core values, that makes the present research, and this thesis, an original and positive contribution to legal literature in New Zealand and internationally.

---

[3] For an example see the Facebook and Cambridge Analytica controversy, which is discussed further in Olivia Solon and Emma Graham-Harrison "The six weeks that brought Cambridge Analytica down" *The Guardian* (online ed, London, 3 May 2018).
[4] *Melvin v Reid* 297 P 91 (Cal App 1931).
[5] A recent example of protecting a similar interest is Case C-131/12 *Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales* ECLI:EU:C:2014:317. This case is discussed significantly throughout the remainder of the thesis.
[6] See discussions in Chapters 5 and 6.

II Once Public Facts

The simplest way to understand once public facts is to consider some well known cases that involve once public facts. The seminal case is *Melvin v Reid*, where the defendant made and distributed a film of the appellant's former life as a prostitute who had been tried and acquitted for murder 10 years previously.[7] The claimant brought an action based on, amongst other things, violation of her right to privacy. The Californian Court of Appeal held that the claimant had a valid cause of action for breach of privacy for the publication of the incidents of her former life coupled with her name. In finding as it did, the Court made a distinction between the publication of the fact of the murder charge and the incidents of her life (which were not actionable because their existence was a matter of public record) and the publication of her true name in conjunction with those incidents, which was actionable.[8]

In *Briscoe v Reader's Digest Association* a former convicted truck hijacker brought an action for invasion of privacy for the publication of an article about him and the hijacking incident which had occurred 11 years ago.[9] The Supreme Court of California found that there was a valid cause of action for invasion of privacy. Similar to *Melvin v Reid,* the Court focused on the fact that "identification of the actor in reports of long past crimes usually serves little independent public purpose",[10] although the facts of past crimes were newsworthy and publication of the facts alone was justified. In *Sidis v F-R Pub Corporation* the plaintiff brought a cause of action for breach of privacy for the publication of a biographical sketch and cartoon of himself in *The New Yorker* magazine.[11] Mr Sidis was a famous child prodigy who had "lectured to distinguished mathematicians on the subject of Four-Dimensional Bodies."[12] At 16, Mr Sidis "graduated from Harvard College, amid considerable public attention."[13] However, since that time he had "cloaked himself in obscurity".[14] The Court held that the history and fate of Mr Sidis were still of public concern 25 years later because they answered the question of whether or not he had fulfilled his early promise. Neither the ruthlessness of the exposé nor the lengths Mr Sidis went to protect his privacy and escape his

---

[7] *Melvin v Reid*, above n 4. While the judgment is not clear as to when the trial occurred it does note that in 1918 Mrs Melvin abandoned her life of shame and in 1925 the film of her life was released.
[8] At 93. Invasions of privacy in the United States are generally protected by four distinct causes of action: (1) public disclosure of private facts; (2) interference with seclusion and solitude; (3) publicity that places a person in false light; and (4) appropriation of another's name or likeness. This classification is discussed further at Chapter 6(IV)(A). *Melvin v Reid*, above n 4, is an example of the public disclosure of private facts cause of action and has been called the "leading case in this area" of United States Law. See *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [69].
[9] *Briscoe v Reader's Digest Association* 483 P 2d 34 (Cal 1971).
[10] At [40].
[11] *Sidis v F-R Pub Corp* 113 F 2d 806 (2d Cir 1940).
[12] At [806].
[13] At [806].
[14] At [809].

past over the intervening years outweighed the public interest in knowing about Mr Sidis and his subsequent history.

In recent times, the most famous case is *Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales* where Mr Gonzales brought an action against Google for the search results that returned when his name was searched on the Google Spain search engine. The most prominent results related to home-foreclosure notices from nine years ago when Mr Gonzales was in temporary financial trouble.[15] The notices had been published originally by a third party newspaper and then made available online. The Court of Justice of the European Union (CJEU) held that under the European Union's Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data,[16] Google had to break the links to the old newspaper information about Mr Gonzales' debt, so that the information was not returned on a search of his name.[17]

What do these cases say about once public facts? First, the facts were generally old facts. In the cases cited above the facts were nine, 10, 11 and 25 years old respectively. Second, the facts were usually true.[18] Third, the facts predominantly relate to people who had rehabilitated or otherwise moved-on from the republished information and who wished to no longer be defined or judged based on those facts. Fourth, the facts were public. The use of the term 'public' can be fraught (the difficulties with the term are discussed in Chapter 3 below), however, at this stage it is sufficient to appreciate that 'public' means the facts are accessible to the general public.

III Research Questions

As set out in the title to the thesis, the overarching research question is whether or not once public facts should gain privacy protection in law? To assist in answering the question, it has

[15] See *Google Spain*, above n 5.
[16] Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data [1995] OJL 281. Directive 95/46/EC is no longer in force. It was repealed on 24 May 2018 by Regulation 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data [2016] OJL 119 [GDPR].
[17] Mr Gonzales had also brought an action against the newspaper publisher of the foreclosure notices. However, the AEPD found that publication by the newspaper was legally justified (see *Google Spain*, above n 5, at [16]). This decision was not appealed to the European Court of Justice [ECJ]. However, the ECJ did note that search engines affect individuals' rights to privacy over and above the original publishers (at [38]).
[18] The law of defamation generally addresses the publication of untrue information. The relationship between defamation and privacy is discussed further in Chapter 4(II)(A)(2).

been broken into five sub-questions that have guided the structure of the present research and its presentation in the thesis. The sub-questions are:

1. Is it appropriate to discuss once public facts under the banner of privacy?

2. What are the core values affected by once public facts? Put another way, what core values are put at risk if a zone of protection for once public facts is not recognised?

3. What existing legal mechanisms can be used to protect once public facts and how effective are those mechanisms?

4. Privacy commonly comes into conflict with freedom of expression. How are these two fundamental rights, values or interests balanced?

5. What amendments are required to existing legal mechanisms to ensure appropriate protection for once public facts in New Zealand?

IV Outline of Chapters and Summary of Conclusions

The overarching conclusion of the research is that it is conceptually and jurisprudentially sound for once public facts to gain protection in privacy law in the right circumstances. However, in order for this protection to be gained, it is recommended that New Zealand's privacy law mechanisms are amended. This conclusion is reached via the arguments set out in the 10 chapters contained in this thesis. The structure and conclusions of each chapter are described below.

The first four chapters provide the scaffolding of the thesis and answer the first two research sub-questions. Chapter 1 – this Chapter – provides an introduction to the thesis, ensures an understanding of the subject matter of the present research (once public facts) and signals the direction of the thesis as a whole. Chapter 2 describes the research's methodology and jurisprudential considerations. The research is a combination of doctrinal research and law reform-oriented research. The research articulates the current law relating to once public facts and assesses its overall effectiveness (the doctrinal component) and then proposes policy and law reforms. Jurisprudentially, the present research considers law as incorporating rules and principles, in line with the theories of Dworkin. Chapter 3 is the literature review, which highlights the scholarly work on which the thesis is built and provides an answer to the first

research sub-question above. The literature review demonstrates that once public facts have been a component of most of the best known concepts of privacy. Furthermore, many notable privacy scholars have argued for a broad view of privacy that includes protection for privacy in public. The research argues that there is theoretical and conceptual support for the protection of once public facts under the banner of privacy. The chapter concludes with a discussion of tikanga Māori concepts of privacy, which are a vital aspect of considering wider concepts of privacy within New Zealand. Chapter 4 asks why society should care about once public facts and ultimately provides an answer to the second research sub-question. The chapter finds that failure to protect once public facts imperils core values at the heart of privacy – liberty, rehabilitation, dignity and autonomy. In addition, failing to protect once public facts can cause substantial harm. Chapter 4 also considers the extent to which these core values should bow to the capacities of modern information technology. Ultimately, the chapter argues that it is for society to determine the interests it wishes to protect and that technology should operate in ways that support not hinder those values.

Chapters 5 – 8 consider the existing privacy law mechanisms for protecting once public facts and asks, variously, whether those mechanisms do protect such facts, whether they should protect such facts, and how effective they are at achieving protection. These chapters address the third and fourth research sub-questions. Chapter 5 considers the Privacy Act 2020, and explores its effectiveness by investigating the extent to which the Act provides a RTBF. The term 'RTBF' is fraught, but also captivating, triggering an inherent sense that many people feel of retreat and mystery.[19] Such a tool, constituted appropriately, can provide a measure of escape from historical information that is persistently available online. The chapter finds, however, that the tools within the Privacy Act are too narrow to provide an effective RTBF. As a result, the chapter recommends changes to the Privacy Act to address the gap.

Chapter 6 considers the second key mechanism for protecting once public facts – the common law disclosure tort. The tort is an important weapon in the arsenal for protecting once public facts because the Privacy Act excludes from its coverage news activities – one of the main activities responsible for inappropriate publication of once public facts. The chapter finds that the current tort test can protect once public facts, but that refinements to the test are recommended to ensure it is fit for purpose. Chapter 7 addresses the fourth research sub-question by considering the conflict between privacy and freedom of expression. The chapter finds that a balancing of privacy and free speech occurs in all legal mechanisms that protect

[19] See the discussion in Chapter 5(II)(A) for a summary of the difficulties in defining the 'right to be forgotten' [RTBF].

privacy, although in different ways. In the disclosure tort, where the most overt balancing occurs, the New Zealand case law demonstrates that what is required is a close assessment of the facts, an identification of the interests at issue and a weighing of those interests. This conclusion means that the operation of the tort does not provide any specific constraints on protecting once public facts, even though the facts are 'public'. However, the chapter also finds that improvements could be made to the way the balancing occurs in the tort to ensure it operates in a structured and principled manner.

Chapter 8 considers the recent development of the HDCA. The HDCA was introduced to address cyberbullying, but due to its framing also covers privacy. The chapter finds that the drafting of the HDCA means that it can be used as a limited form of RTBF, but that hurdles exist, including the level of harm required and lack of clarity over jurisdictional reach. However, the Act cannot be used as a right to delist or delink search results as occurred in the decision in *Google Spain*. Ultimately, the chapter recommends allowing the HDCA to continue in its development, with minor amendments to enhance its efficacy.

Chapter 9 wraps up all the findings in the previous chapters into a package of amendments to enable appropriate protection for once public facts. The package includes amendments to the Privacy Act, the disclosure tort and the HDCA. In regard to the Privacy Act, it is recommended that a new information privacy principle (IPP) is included called 'erasure of personal information', and that amendments are made to IPP 8 to ensure that agencies' use of personal information is appropriate. In regard to the disclosure tort, it is recommended that: (1) the reasonable expectation test is elaborated upon by recognition that the test requires consideration of three particular matters – the specific circumstances of the case, an empirical analysis, and a core values assessment; (2) the 'highly offensive' test is abandoned; and (3) a proportionality framework is utilised for determining whether the defence of legitimate public concern exists. The proportionality framework requires consideration of the particular free speech and privacy interests involved, the relative weight of the interests and ultimately which interest comes out ahead. These refinements are demonstrated graphically in Figure one below. In regard to the HDCA, while the ultimate conclusion is that a watching brief is required on the use of the Act as a limited RTBF, two minor amendments are recommended. These amendments are: (1) the removal of s 12(2)(a), which is the requirement for a serious or repeated breach, and (2) amendment of the jurisdictional reach of the Act to reflect that which exists under the Privacy Act.

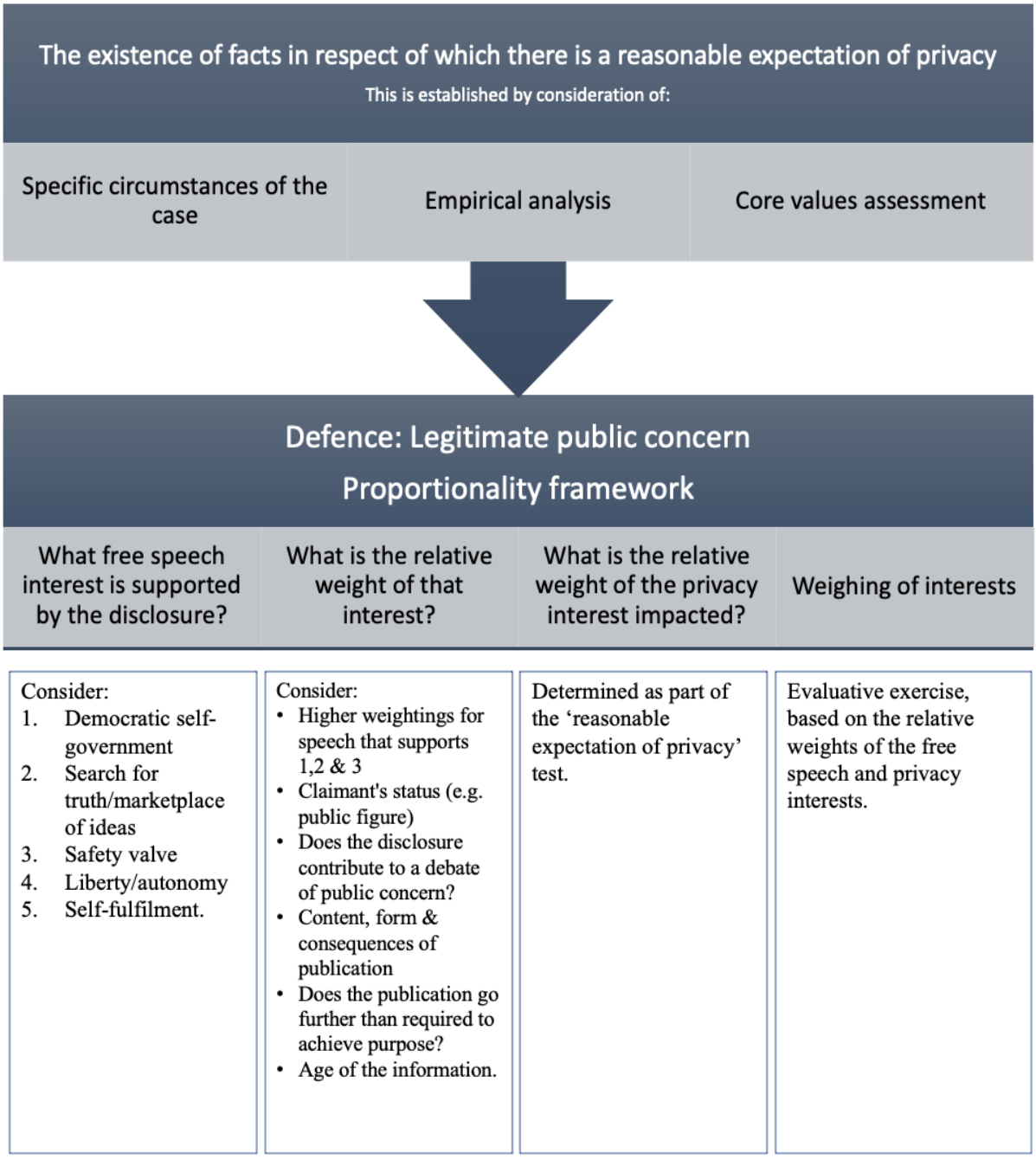
In addition to the above changes, the present research has also identified ancillary changes which may bolster the protection given to once public facts. These changes are not to the direct legal mechanisms that protect privacy and are therefore not included in the package of amendments. These changes are a review of the Criminal Records (Clean Slate) Act 2004 (Clean Slate Act), to ensure an appropriate commitment to the rehabilitation of former offenders, and recognition (either judicially or via the New Zealand Bill of Rights Act 1990 [NZBORA]) that privacy is a right.

Chapter 10 concludes the thesis. The chapter demonstrates how the results of the present research and the thesis have addressed the research questions and led to the conclusion that protecting once public facts *is* privacy for our time, not a glaring paradox. The conclusion also demonstrates how the thesis contributes to the theory and law reform of privacy of New Zealand. Theoretically, the present research has argued that the predominant theories of privacy are broad enough to encompass once public facts and that protecting a zone of privacy around once public facts can uphold the core values of liberty, rehabilitation, dignity and autonomy. The research has also provided a law reform package which can contribute to the future development of privacy law in New Zealand. The research may also prove useful for other common law jurisdictions whose "fledgling"[20] privacy torts might benefit from the learnings in New Zealand.

[20] Samuel Beswick and William Fotherby "The Divergent Paths of Commonwealth Privacy Torts" in Margaret I Hall (ed) *The Canadian Law of Obligations: Private Law for the 21st Century and Beyond* (LexisNexis Canada Inc, Toronto, 2018) 225 at 239.

Figure 1

Disclosure Tort



2 METHODOLOGY AND JURISPRUDENCE

I Introduction

The purpose of this chapter is twofold: (1) to describe the methodology employed in the present research; and (2) to discuss some key jurisprudential considerations that impact on the present research. The research uses traditional doctrinal methodology to identify the law that applies to once public facts and to determine whether or not protecting once public facts is consistent with broader legal protections in New Zealand. The research then pivots to reform-oriented research to propose recommendations about how the law in New Zealand should be structured. The proposed reforms are identified using a range of tools, including comparisons with international jurisdictions, review of wider societal benefits to be gained from recognising the reforms, considering broader regulatory imperatives, and endeavouring to provide a consistent and holistic approach to legal remedies.

The role of once public facts in privacy law is far from settled in New Zealand. The structure of the current legal protections for privacy rely on rules, principles and a balancing of competing interests. As such, it is important to consider jurisprudential issues, like what law is and how is it made. The chapter briefly discusses the two main competing approaches to what law is – the interpretative approach of Dworkin and the positivist approach.[21] At the heart of these two approaches is the role of morality in law, and whether a legal system is comprised solely of rules made by an appropriate authority or whether there is a place for principles driven by the morals of society. It will be seen that the position of this thesis is that the interpretive approach of Dworkin is the most appropriate to explain the current development of privacy law and for its future development as a mechanism for protecting once public facts.

II Methodology

The present research is both descriptive and normative. The research searches for what the law currently comprises and what the law ought to be. The descriptive component employs standard doctrinal methodology to identify the current law regarding once public facts. Doctrinal research is a common tool employed by legal scholars,[22] which has been described

[21] Brian Bix *Jurisprudence: Theory and Context* (7th ed, Sweet & Maxwell, London, 2015) at 94.
[22] Ian Dobinson and Francis Johns "Qualitative Legal Research" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 16 at 18.

as "research which asks what the law is in a particular area."[23] Pendleton has provided a deeper definition of doctrinal research, as "research which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments."[24] Pendleton refers to two other major categories of legal research – reform-oriented research which "intensively evaluates the adequacy of existing rules and which recommends changes to any rules found wanting",[25] and theoretical research which:[26]

> … fosters a more complete understanding of the conceptual bases of legal principles and of the combined effects of a range of rules and procedures that touch on a particular area of activity.

Others view theoretical research as an aspect of doctrinal research and categorise all other legal research – like reform-based and policy research – as non-doctrinal research.[27] The present research takes the latter approach – categorising theoretical legal research as an aspect of doctrinal research. The present research argues that understanding the theoretical basis of a legal concept like 'privacy' is part and parcel of being able to identify what the law is.

Dobinson and Johns analogise doctrinal and theoretical research to a social science literature review, which requires: (1) selecting research questions; (2) selecting bibliographic or article databases; (3) choosing search terms; (4) applying practical screening criteria; (5) applying methodological screening criteria; (6) doing the review; and (7) synthesising the results.[28] Hutchinson, however, disagrees, arguing that the scholarship required for doctrinal research is more extensive than a literature review because the primary sources are the law itself, which requires "the intricate step of locating and then 'reading, analysing and linking' the new

---

[23] At 18–19.
[24] Australian Law Deans "Submission to the CTEC Assessment Committee for the Discipline of Law" in Dennis Pearce, Enid Campbell and Don Harding *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (Australian Government Publishing Service, Canberra, 1987) at 9.15, cited in Michael Pendleton "Non-empirical Discovery in Legal Scholarship – Choosing, Researching and Writing a Traditional Scholarly Article" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 159 at 159.
[25] Pendleton, above n 24, at 159.
[26] At 159.
[27] See Dobinson and Johns, above n 22, at 18–20.
[28] Arlene Fink *Conducting Research Literature Reviews: From the Internet to Paper* (Sage Publications, Los Angeles, 2014) at 3–5, cited in Dobinson and Johns, above n 22, at 22–23.

information to the known body of law."[29] Hutchinson cites with approval the Council of Australian Law Deans Statement on the Nature of Legal Research which argues that:[30]

> Doctrinal research, at its best, involves rigorous analysis and creative synthesis, the making of connections between seemingly disparate doctrinal strands, and the challenge of extracting general principles from an inchoate mass of primary materials. The very notion of 'legal reasoning' is a subtle and sophisticated jurisprudential concept, a unique blend of deduction and induction that has engaged legal scholars for generations.

Hutchinson's view of doctrinal research is preferred here to that referred to by Dobinson and Johns. It recognises the complex and in-depth processes employed when conducting doctrinal research.

To support his view of doctrinal research, Hutchinson puts forward a "simple problem-based doctrinal research methodology" [31] which consists of: (1) assembling the relevant facts; (2) identifying the legal issues; (3) analysing the issues with a view to searching for the law; (4) locating and reading background information; (5) locating and reading primary sources; (6) synthesising all the issues in context; and (7) coming to a tentative conclusion. The present research follows this approach when utilising the doctrinal methodology.

As noted above, the present research is wider than just doctrinal research. The research seeks to determine what the law *ought* to be. It does this through intensively evaluating the adequacy of the existing rules and then proposing law reform.[32] The evaluation of the existing rules involves considering the social environment and values in which the rules operate, the wider regulatory framework within New Zealand,[33] comparing the rules to those which exist in other jurisdictions,[34] and ultimately seeking to establish a unified and consistent approach to the law and outcomes under the law. This process leads to the package of law reforms ultimately presented.

In regard to the methodology employed in the present research, the matters described below must be highlighted.

---

[29] Terry Hutchinson "Doctrinal research: Researching the jury" in Dawn Watkins and Mandy Burton (eds) *Research Methods in Law* (Routledge, London 2013) 7 at 13.
[30] Council of Australian Law Deans "Statement on the Nature of Legal Research" (May-October 2005) CALD <https://cald.asn.au> at 3, cited in Hutchinson, above n 29, at 11.
[31] Hutchinson, above n 29, at 12.
[32] Pendleton, above n 24, at 159.
[33] See the discussion in Chapter 4.
[34] See the discussions in Chapters 5–7, where privacy law in the United States, England, Europe, Canada and Australia is considered.

(1) Questions have been posited for all areas of the research and these have been used to focus the research irrespective of particular legal research method employed. For those parts of the research that are doctrinal, these questions identify the problem that needs to be solved and assist with assembling the facts and identifying and analysing the legal issues.

(2) Locating primary and secondary sources has employed traditional legal research techniques (for example, key word searches, reviewing citations, identifying recently released cases and articles, and reviewing parliamentary resources) and utilised common national and international legal databases (for example, Lexis Advance and Westlaw).

(3) Synthesising the results has employed traditional legal concepts like the doctrine of stare decisis[35] and statutory interpretation rules. These concepts provide in-built guidance to determine what the law is on a particular topic and how the law should be applied.

(4) The present research has considered the law in a number of comparator jurisdictions. This is a common technique because the law from other jurisdictions holds weight in New Zealand cases and other countries have more developed laws on some of the topics discussed, for example, the United States' disclosure tort and Europe's Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (called the 'General Data Protection Regulation' [GDPR]).[36] However, the present research is not comparative law research.[37] The use of the law from other countries is used to benchmark, to compare and ultimately to inform the national law of New Zealand. To the extent possible and practicable within the constraints of the present research, the context of the law in other jurisdictions has been discussed, but in some respects the discussion is more superficial than would be expected if this was a work of comparative legal analysis.

---

[35] "Structure of the court system" Courts of New Zealand <www.courtsofnz.govt.nz> describes stare decisis, or the doctrine of precedent, as follows: "A decision of a higher court is binding on lower courts and decisions of the Supreme Court, the final court of appeal, are binding on all other courts. Cases that are legally similar will generally be decided in the same way, conforming with the decisions of a higher court."

[36] GDPR, above n 16. The United States tort has exerted considerable influence on the development of New Zealand privacy common law. See discussion at Chapter 6(II)(A). For a discussion of the GDPR and its comparison to New Zealand data protection law see Chapter 5.

[37] For a discussion of comparative legal research see Geoffrey Wilson "Comparative Legal Scholarship" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 87.

III Jurisprudential Considerations

Jurisprudence is the philosophy of law and seeks to understand the nature of law and legal systems. Toy has noted that jurisprudence is "very relevant" to the study of information privacy law because privacy law is "a new and unsettled field".[38] Where the law is at a nascent stage there are often questions about the scope of the law, how it should be applied and how it should be balanced against other laws. Jurisprudential considerations help with answering these questions.

Toy has argued that the jurisprudential theories of Dworkin are most appropriate for explaining information privacy law.[39] Dworkin argues that the law contains both rules and principles.[40] Principles are standards that are observed because "it is a requirement of justice or fairness or some other dimension of morality."[41] In Dworkin's analysis, rules "are applicable in an all-or-nothing" fashion;[42] if they apply then they are conclusive. Principles operate differently. Principles only have to be taken into account if they are relevant. This approach means that principles have a "dimension of weight or importance" that rules do not.[43] If there are competing principles involved in a particular situation (and there commonly are), then what has to be considered is the relative weight of each principle.

The opposite school of thought, called positivism, argues that the law is a system of rules alone, the law is identified by its sources, and that questions of law and morality are separate.[44] Central to positivism is the concept of a "rule of recognition" – a rule which stipulates the criteria by which all other rules are judged valid.[45] In regard to the rule of recognition, Bix notes that it:[46]

> … expresses, or symbolises, the basic tenet of legal positivism: that there are conventional criteria, agreed upon by officials, for determining which rules are and which are not part of the legal system.

[38] Alan Toy "Privacy Audits: Expectations and Implementation" (PhD Thesis, University of Auckland, 2016) at 53.
[39] At 54–55.
[40] See Ronald Dworkin *Taking Rights Seriously* (Bloomsbury, London, 2013) at 38 for a discussion of Dworkin's use of the word 'principles'.
[41] At 39.
[42] At 40.
[43] At 43. Dworkin argues that if two rules conflict, then one cannot be valid.
[44] Bix, above n 21, at 35.
[45] H L A Hart *The Concept of Law* (2nd ed, Clarendon Press, Oxford, 2012) at 100. See also Bix, above n 21, at 40–41.
[46] Bix, above n 21, at 41.

In the argument for his theory of rules and principles, Dworkin looked to some "difficult" cases where the decision of the judges seemed to contradict a statute or a previous decision,[47] but appealed to standards like "general, fundamental maxims of the common law" to decide the case.[48] These, Dworkin argued, demonstrated the role played by principles rather than rules. Dworkin noted:[49]

> A Principle like 'No man may profit from his own wrong' does not even purport to set out conditions that make its application necessary. Rather, it states a reason that argues in one direction, but does not necessitate a particular decision…There may be other principles or policies arguing in the other direction… If so, our principle may not prevail, but that does not mean that it is not a principle of our legal system, because in the next case … the principle may be decisive. All that is meant, when we say that a particular principle is a principle of our law, is that the principle is one which officials must take into account, if it is relevant, as a consideration inclining in one direction or another.

Toy argues that Dworkin's theory is to be preferred over legal positivism because much of privacy law involves principles, and balancing principles is a common adjudicative approach in many privacy cases and jurisdictions.[50] The present research argues that Toy's approach is the correct one.[51] The balancing of principles can be seen in the landmark privacy case of *Melvin v Reid*, where the Judge had to weigh the right to pursue and obtain safety and happiness as set out in the Constitution of California with the community's right to open justice.[52]

It is also clear that the Privacy Act is based on principles. Section 22 of the Act sets out information privacy principles which must be complied with. Furthermore, Gunasekara and Toy argue that more fundamental and abstract principles underlie the information privacy principles.[53] Dworkin himself raised the idea that the right to privacy might be based upon the

---

[47] Dworkin, above n 40, at 45. The cases were *Riggs v Palmer* 22 NE 188 (1889) and *Henningsen v Bloomfield Motors Inc* 161 A 2d 69 (1960).
[48] Dworkin, above n 40, at 39.
[49] At 42. See also Bix, above n 21, at 94 who saw support for Dworkin's theory in "landmark" judicial decisions "where the outcome appears to be contrary to the relevant precedents, but the court still held that it was following the 'real meaning' or 'true spirit' of the law".
[50] Toy, above n 38, at 53–55.
[51] See Privacy Act 2020, s 22 and the discussion in Chapter 7 regarding privacy and free speech.
[52] *Melvin v Reid*, above n 4, at 93.
[53] Gehan Gunasekara and Alan Toy "Principles or Rules: The Place of Information Privacy Law" (2011) 24 NZULR 525 at 542. Alan Toy "Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy" (2013) 25 NZULR 938 at 940 argues that the information privacy principles [IPPs] in the Privacy Act are in fact rules (rather than principles) due to the level of specificity. It is arguable that, based upon Dworkin's analysis, Toy is correct. The IPPs are more like rules than principles.

abstract right to liberty.[54] Gunasekara and Toy endorse Dworkin's liberty principle, and also point to the principles of good faith, transparency, fairness, accountability, proportionality and consent.[55] While Gunasekara and Toy's identification of abstract fundamental principles which drive explicit principles in data protection statutes is useful, debate could be had about the extent to which the Privacy Act in New Zealand adequately upholds some of these abstract principles. The present research, for example, argues that accountability may not be as strong in the Act as it could be, especially when compared with other jurisdictions, like the GDPR.[56] Furthermore, the description of the specific principles could also be a point of contention. In 2013, as a result of international developments, Toy argued that good faith and fairness should be replaced with principles relating to legitimacy, privacy by design and respect for context.[57] However, it is not readily evident that legitimacy adds anything not already covered by the good faith principle and, while the inclusion of 'privacy by design' reflects current thinking about privacy,[58] it is arguable that it is too specific to be a true abstract principle. Perhaps the broader principle of protection would better address the matters Toy was concerned about – security and accuracy.[59]

In accepting the role of principles in a legal system, the question becomes which morals underpin the principles. It is clear that many laws do enforce moral standards, for example, it is common for criminal laws to impose sanctions for murder, robbery and rape.[60] However, Bix speaks of a "dividing line" between those moral standards the law should enforce and those the law should not,[61] and most of the argument is where that dividing line should rest.[62]

---

[54] Dworkin, above n 40, at 144.
[55] Gunasekara and Toy, above n 53, at 541–542.
[56] At 542. Gunasekara and Toy argue that accountability is "a very strong theme running through" the Privacy Act. However, the position of the present research is that without stronger erasure rights, organisations have less accountability for how they use personal information than in Europe. The commitment to consent in the Privacy Act is also potentially less when compared to the GDPR. These matters are discussed further in Chapter 5 below.
[57] Toy "Different Planets or Parallel Universes", above n 53, at 947. The principle of 'respect for context' derives from the White House Report "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (7 February 2012). That Report proposed a Consumer Privacy Bill of Rights, which included the right to 'respect for context', which was described as "a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data" (at 97). Toy includes fairness in the proportionality principle.
[58] Toy, above n 53, at 947 states that 'privacy by design' means "that information privacy protections should be baked in to every stage of the development of products and services". GDPR, art 25 sets out a statutory framework for privacy by design.
[59] At 948.
[60] Bix, above n 21, at 171.
[61] At 171–174.
[62] At 173. Bix argues that much of the argument in this space exists in the areas of sexuality, pornography, surrogate motherhood, and sado-masochism.

For Dworkin, the morality that judges uphold in cases is a "community morality", a "political morality presupposed by the laws and institutions of the community."[63] On the issue of community morality, Toy notes that:[64]

> … a judge who also happens to be committed to the Jewish religion would apply the morality of the 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 the society as a whole.

For the purposes of this thesis, arguments on what is or is not the morality of current New Zealand society are not required. However, it is important to understand what can shape that morality, and that includes the morality that underpins the laws and institutions of the society. It must also be recognised that law can be slow to change and to adapt to changing community morality, so sometimes officials must look beyond the current law and consider international best practice.[65] Furthermore, in a country like New Zealand, where its constitution includes a founding document like Te Tiriti o Waitangi/Treaty of Waitangi, that founding document and the values that underpin it will also influence the morality of the community.[66]

IV Conclusion

Doctrinal research provides the answer to the question 'what is the law?' Such research is a complex and challenging process to extract rules and principles from an "inchoate mass of primary materials."[67] The present research uses this methodology to determine whether privacy law in New Zealand does and should protect once public facts. However, the research is wider than just doctrinal research. The research uses a range of techniques like international comparisons, consideration of wider social benefits, and broader regulatory imperatives to determine what law reform is needed within New Zealand to provide appropriate protection for once public facts.

[63] Dworkin, above n 40, at 154. To determine this morality, judges will consider laws, decisions and constitutional arrangements.
[64] Toy, above n 38, at 57.
[65] At 59.
[66] See the discussion in Chapter 3(IV) below.
[67] Council of Australian Law Deans, above n 30.

The jurisprudential context of this research is one which views the law as incorporating both rules and principles, in line with the theories of Dworkin. Viewing the legal system as containing both rules and principles not only explains the development of privacy law, it also ensures that the law is flexible enough to recognise and balance important values and interests and take into account when those values and interests may change.

3 LITERATURE REVIEW

I Introduction

The literature review considers some of the best known concepts of privacy and asks if they are broad enough to encompass once public facts. By traversing these concepts of privacy, the literature review also demonstrates how the present research builds upon the scholarship of privacy that has gone before. The intent of the present research, however, is not to revisit all the literature on the concepts of privacy, but rather to consider some of the more influential concepts afresh, with once public facts in mind.[68] Supporting the discussion about the concepts of privacy is also a review of the literature on privacy in public. Once public facts are facts which are or have been in the public domain. Accordingly, if there has been no previous scholarship on the ability for persons to expect some form of privacy regarding public information or in public spaces, then the arguments put forward in this thesis are harder to maintain.

What this research determines is that most of the key concepts of privacy reviewed provide room for once public facts, either explicitly or implicitly, and that there is a growing acceptance that the concept of privacy includes privacy in public. What is public and what is private should be determined not on traditional binary distinctions, but rather on a range of factors, including the nature of the relationship between the affected parties, the accessibility of the information, the context of the information's disclosure and whether that context has adhered to the prevailing norms within that environment, and the consequences of exposure.

The literature review also considers tikanga Māori perspectives on privacy. This cultural perspective is necessary to uphold New Zealand's commitment to Te Tiriti o Waitangi/Treaty of Waitangi and to provide deeper understanding of privacy expectations in New Zealand.[69]

---

[68] The selection of theories has been based on the author's subjective assessment of those works that have been quoted, cited or referenced most frequently in other scholars' work. The research does, however, endeavour to cover the broad spectrum of theories, particularly those that may on the face of it provide insurmountable issues for once public facts.

[69] Te Tiriti o Waitangi/Treaty of Waitangi was signed on 6 February 1840 by Captain William Hobson, several English residents, and between 43 and 46 Māori rangatira (chiefs). After this initial signing, the Māori text, and copies, were circulated around New Zealand. By the end of 1840, over 500 Māori had signed the Treaty. For more information see "Signing of the Treaty" (19 September 2016) Waitangi Tribunal <https://waitangitribunal.govt.nz>. Differences in the Māori and English texts of Tiriti o Waitangi have led to different understandings of what was promised. As a result, the principles of Tiriti o Waitangi and its spirit have become important in understanding how both parties are to ensure Tiriti o Waitangi is upheld. The core principles that underpin Tiriti o Waitangi are good faith, partnership, mutual benefit, informed decisions and consultation, and active protection and redress. For more information see "A Guide to the Principles of the Treaty of Waitangi as Expressed by the Courts & the Waitangi Tribunal" Waitangi Tribunal < https://waitangitribunal.govt.nz>.

Ultimately, what the research finds is that there has been little empirical research into Māori approaches to privacy and none which provides any link between Māori concepts of privacy and once public facts. However, tikanga Māori does demonstrate a commitment to privacy and indicates a Māori view of privacy that is wider and more nuanced than New Zealand's current law recognises. While the present research is not the vehicle to address this issue directly, the recommendations contained in this thesis propose a framework for privacy which will enable consideration of broader cultural perspectives to occur in the future.

II Concepts of Privacy

What privacy is and how it should be defined has been the subject of considerable academic effort. This literature review takes those academic efforts and revisits them with fresh eyes. This review considers some of the best known concepts of privacy and asks if those concepts are broad enough to encompass once public facts. If not, then any argument for protection of once public facts under the banner of 'privacy' is on perilous ground. Many discussions of the concept of privacy devolve it into sub-categories which address the main thrust of the argument, for example, human dignity, personal information, control, secrecy, and intimacy, or complex concepts like Solove's taxonomy of privacy harms. This approach can be fraught, because many scholars' accounts of privacy are rich and complex and not easily categorised into only one bucket. However, a category approach is also useful. Such an approach helps to order the discussion and easily demonstrates the breadth of interests contained under the simple heading of 'privacy'. For that reason, the category approach is employed here. However, what is important is not the title of the category but the substance of the concept, and that the categorisations in this thesis may differ from those of other authors.[70]

A The Right to be Let Alone

Privacy as the right to be let alone derives from Warren and Brandeis' influential article of 1890. In that article, the authors argued that: [71]

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right "to be let alone".

[70] The categories used in this thesis are an amalgamation of those used by Stephen Penk "Thinking About Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 1 at 3–8 and Daniel J Solove "Conceptualizing Privacy" (2002) 90 CLR 1086.
[71] Samuel D Warren and Louis D Brandeis "Right to Privacy" (1890) Harv L Rev 193 at 195. The phrase 'right to be let alone' is a quote from Thomas M A Cooley *Cooley on Torts* (2nd ed, Callaghan, Chicago, 1879) at 29. For the "recent inventions and business methods" see at 195–196.

For the authors, the right to privacy was an aspect of a person's "inviolate personality"[72]and underpinned existing common law protections for intellectual property. Accordingly, protecting personal privacy was not new, merely the next logical step. The authors stated that:[73]

> The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.

Warren and Brandeis did not specify what particular matters were to be protected by the right to privacy; however, their use of phrases like "private life", "private affairs" and "social and domestic relations" point toward a relatively narrow view of the matters that warranted protection and one that would arguably exclude once public facts.[74]

The right to be let alone has, however, been used to support a wide range of matters, including a right to privacy for information posted to SNS[75] and the constitutional privacy in the United States, where certain matters are protected from state intrusion, like the right to make decisions regarding "marriage, procreation, contraception, family relationships, child rearing, and education".[76] Solove, however, argues that the concept is too vague. He states that:[77]

> … formulation of privacy as the right to be let alone merely describes an attribute of privacy. Understanding privacy as being let alone fails to provide much guidance about how privacy should be valued vis-à-vis other interests, such as free speech, effective law enforcement, and other important values.

Furthermore, there are many ways a person could want to be let alone and not all should necessarily be protected by privacy. Parent argues as follows:[78]

---

[72] Warren and Brandeis, above n 71, at 205. The authors also called it the "right to immunity of the person, – the right to one's personality".
[73] At 205 and 207.
[74] At 213–216. The authors did not mention once public facts. They did, however, argue that the right to privacy "ceases upon publication of the facts by the individual, or with his consent" (at 218).
[75] Connie Davis Powell "You Already have Zero Privacy, Get Over It – Would Warren and Brandeis Argue for Privacy for Social Networking" (2011) 31 Pace L Rev 146. This is an unusual argument considering that Warren and Brandeis clearly argue that the right to privacy "ceases upon publication of the facts by the individual, or with his consent" (above n 71, at 218).
[76] Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008) at [2.8]–[2.9] who saw a more sophisticated form of the 'right to be let alone' behind many of the decisions in the constitutional privacy cases.
[77] Solove, above n 70, at 1101–1002.
[78] WA Parent "A New Definition of Privacy for the Law" (1983) 2 L & Phil 305 at 321.

> Think about some of the ways in which *A* can fail to leave *B* alone: by hitting him, interrupting his conversation, shouting at him, repeatedly calling him, joining him for lunch. There is no compelling reason of logic or law to describe any of these actions as an invasion of privacy.

Describing privacy as the right to be let alone also does not provide any rationale for the protections set out in modern data protection statutes. These statutes protect privacy once personal data are provided to a third party, whereas the right to be let alone is directed at seclusion.[79]

B Human Dignity

The concept of privacy as dignity can be seen in the work of Bloustein, where he proposed a unifying general theory of individual privacy based around individual freedom and human dignity.[80] Bloustein saw dignity as central to Warren and Brandeis' concept of 'inviolate personality'. He stated that: [81]

> Thus, I believe that what provoked Warren and Brandeis to write their article was a fear that a rampant press feeding on the stuff of private life would destroy individual dignity and integrity and emasculate individual freedom and independence.

Bloustein also saw dignity as underpinning the privacy torts in the United States. He argued that:[82]

> An intrusion on our privacy threatens our liberty as individuals to do as we will, just as an assault, a battery or imprisonment of our person does. And just as we may regard these latter torts as offenses "to the reasonable sense of personal dignity," as offensive to our concept of individualism and the liberty it entails, so too should we regard privacy as a dignitary tort.

---

[79] Solove, above n 70, at 1102.
[80] Edward J Bloustein "Privacy as an Aspect of Human Dignity" (1964) 39 NYU L Rev 962. See also Edward J Bloustein "Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory" (1978) 12 Ga L Rev 429.
[81] Bloustein "Human Dignity", above n 80, at 971.
[82] At 1002. See Chapter 6(IV)(A) below for a discussion of the United States tort. Bloustein also argued that human dignity was the backbone of early data protection statutes in the United States. He stated that: "The disclosure provisions of the statutes, like the tort disclosure cases, preserve dignity by restricting publicity, by assuring a man that his life is not open and indiscriminate object of all eyes. And … the statutory disclosure provisions complement the statutory intrusion provisions by making a man secure in his person, not only against prying eyes and ears, but against the despair of being the subject of public scrutiny and knowledge" (at 1000).

In regard to the disclosure tort, the affront to dignity is the use of "techniques of publicity to make a public spectacle of an otherwise private life."[83] The use of the phrase 'private life' might speak to a view of privacy that would not encompass once public facts. However, Bloustein referred to both *Melvin v Reid* and *Sidis* in putting forward his concept, where he argued that the wrong being complained of was that:[84]

> … some aspect of their life has been held up to public scrutiny … it is as if 100,000 people were suddenly peering in, as through a window, on one's private life.

While Bloustein did not refer to the once public aspects of those cases, he is obviously aware of the facts of the cases (he provides a summary of both cases) and the fact that the information had been in the public domain previously did not affect his argument.

Closely related to human dignity is Benn's concept of privacy as personhood. For Benn "what is objectionable about invasions of privacy even when there is nothing else objectionable, is their failure to respect personhood."[85] Benn argues that:[86]

> … respect for someone as a person, as a chooser, implied respect for him as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching.

Republishing once public facts, especially where a person has actively dissociated themselves from the facts, arguably shows a lack of respect for the person and could frustrate the person's "self-creative enterprise"[87] of moving on with their life and putting behind them past illegal, wrong or simply different activities or attitudes. Benn was alive to this issue, because, when discussing the dangers of computerised data banks, he referred to the fact that:[88]

---

[83] At 1003.
[84] At 979.
[85] S I Benn "Privacy and Respect for Persons: A Reply" (1980) 58 Australian Journal of Philosophy 54 at 60 (emphasis removed). For Benn interference with privacy might be objectionable because of what he calls 'interest-based' reasons, for example "the interest one has in managing his internal psychic economy and his personal relations, and in the possibility of autonomy" (at 59). He argues that there may be instances where there has been no damage to these interests, yet there could still be wrong as an invasion of privacy. In such circumstances what has been affronted is respect for persons (rather than any damage to interests as discussed above). Solove, above n 70, at 1116 categorises dignity as a subset of personhood.
[86] S I Benn "Privacy, Freedom and Respect for Persons" in J Rolland Pennock and John W Chapman *Privacy: Nomos XIII* (Atherton Press, New York 1971) 1 at 26.
[87] At 26.
[88] At 11.

> … information supplied to and by them … if true, may still put a man in a false light, by drawing attention, say, to delinquencies in his distant past that he has now lived down.

The breadth and vagueness of the human dignity concept, which arguably allows it to support a view of privacy that encompasses once public facts, is also the main reason for its critique.[89] Furthermore, it has been argued that the concept only tells us why we value privacy, not what it "is".[90] To this end, Gavison argues that there are activities which are a serious affront to dignity but involve no loss of privacy.[91] Posner also argues that the concept is not sufficiently distinct. He argues that it is indistinguishable from existing concepts like liberty, autonomy and freedom that describe "the interest in being allowed to do what one wants without interference."[92]

C Limited Access

Privacy as "a limitation of others' access to an individual"[93] is most commonly associated with Gavison. Gavison's 'limited access' concept has three components: lack of information (secrecy); lack of attention (anonymity); and lack of physical access to a person (solitude).[94] To Gavison, a person has perfect privacy when he or she is completely inaccessible to others. However, Gavison recognises that neither perfect privacy nor total lack of privacy is possible, so that what is relevant is "*loss* of privacy."[95] She argues that privacy is lost as "others obtain information about an individual, pay attention to him, or gain access to him."[96]

It is relatively easy to see room for some once public facts in Gavison's concept. If *A* learns about *B*'s past conviction, then *A* has access to *B* by having information about *B*. If *A* does not have information about the conviction, then *B* has more privacy regarding that information. Furthermore, when Gavison discussed the value of privacy,[97] she argued that privacy protection of once public facts was justified in certain circumstances. Relying on *Melvin v Reid* and *Briscoe,* Gavison noted that one way in which privacy is allowed to function is to

---

[89] Solove, above n 70, at 1118.
[90] At 1118.
[91] Ruth Gavison "Privacy and the Limits of Law" 89 Yale L J 421 at 438. Gavison refers to begging or prostitution for this critique.
[92] Richard A Posner *The Economics of Justice* (Harvard University Press, Cambridge (Massachusetts), 1981) at 274–275.
[93] Gavison, above n 91, at 428.
[94] At 428.
[95] At 428.
[96] At 428.
[97] At 424. Gavison put forward a neutral concept of privacy; a concept that was not value laden. However, once she moved to discuss the legal protection of privacy, she argued that "we move beyond the neutral concept of 'loss of privacy' and seek to describe the positive concept that identifies those aspects of privacy that are of value" (at 440).

"promote the liberty of individuals not to disclose some parts of their past, in the interest of rehabilitation or as a necessary protection against prejudice and irrationality."[98] She recognised that there is a strong argument *against* privacy operating in this way because it "perpetuates the very problems it helps to ease".[99] Allowing privacy in these situations masks the underlying societal norms rather than actually challenging those norms. In once public fact situations this means that people hide from pasts that might result in "unpleasant consequences",[100] rather than trying to change society's bias towards people with such pasts. However, countering this argument, she argued that:[101]

> The situation is usually much more complex, however, and then the use of privacy is justified. First, there are important limits on our capacity to change positive morality, and thus to affect social pressures to conform. This may even cause an inability to change institutional norms. When this is the case, the absence of privacy may mean total destruction of the lives of individuals condemned by norms with only questionable benefit to society. If the chance to achieve change in a particular case is small, it seems heartless and naive to argue against the use of privacy.

Moreham provides a derivative version of Gavison's 'limited access' by focusing on the subject's desire, so privacy becomes "desired inaccess" or "freedom from unwanted access".[102] According to Moreham the addition of desire avoids the counter-intuitive issues that arise with pure inaccessibility as the concept of privacy. Under Moreham's concept a person unwittingly stranded on a desert island does not have privacy if they do not desire the lack of access to themselves.[103] Moreham's concept of access focuses on two types of access – physical and informational access. In regard to informational access, Moreham argues that:[104]

> … unwanted access to *any* information about a person can be a breach of privacy and 'private information' is therefore any information which *X* wishes to keep to him- or herself.

While acknowledging that this approach is both broad and subjective, Moreham rejects any attempt to narrow what is private information, saying that past attempts have yielded little in

[98] At 452.
[99] At 452.
[100] At 452.
[101] At 453.
[102] N Moreham "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 LQR 628 at 636.
[103] At 636–637.
[104] At 641.

the way of help in defining just what should be considered 'private' information. Accordingly, she argues that the "only way to define the concept of privacy comprehensively is by reference, not to the type of information in question, but to the *claimant's* wishes in respect of it".[105]

While not addressing once public facts, Moreham's broad concept of informational inaccessibility is wide enough to cover facts that were previously in the public domain, provided that the subject *wishes* to keep the information private.

As with all the theories of privacy, limited access has its detractors. Wacks notes that by focusing on any information, so that a loss of privacy occurs whenever *any* information about a person becomes known to another, the "concept loses its intuitive meaning."[106] Wacks' criticism would also apply to Moreham's concept, which is not much narrower than Gavison's. Solove, however, criticises Gavison's concept as too narrow, because it does not cover decisional privacy.[107] On Moreham's concept, the New Zealand Law Commission (NZLC) has noted that it could be critiqued as too individual and subjective.[108]

D Intimacy

While a number of theorists discuss privacy as intimacy, the NZLC argued that the work of Inness is "the most developed theory of privacy as intimacy, and one that provides a better explanation of the scope of intimacy."[109] Inness' concept of privacy proposes that "privacy offers control over decisions about intimate information, intimate access, and intimate actions."[110] Inness argues that "to claim that an activity or action is intimate is to claim that it draws its meaning and value from the agent's love, care, or liking".[111] However, Innes' concept is broader than this definition implies. Inness herself addressed once public facts by discussing *Melvin v Reid*, where she noted that the case:[112]

---

[105] At 642–643. Moreham notes that this is a theoretical definition of privacy. When turning to suggestions for legal protection of privacy, she adds in three additional factors: (1) an objective check in the nature of a 'reasonable expectation' test; (2) the defendant's knowledge and (3) competing interests. For a discussion of these additional factors see at 643–648.
[106] Raymond Wacks *Privacy Vol 1* (Aldershot, Dartmouth 1993) at xiv.
[107] Solove, above n 70, at 1105.
[108] Law Commission, above n 76, at [2.13].
[109] At [2.27].
[110] Julie C Inness *Privacy, Intimacy, and Isolation* (Oxford University Press, New York, 1992) at 9–10.
[111] At 10.
[112] At 128.

> … involved privacy considerations because the defendant disseminated *intimate*, personal details about the plaintiff's former life as a prostitute, thus allowing others to gain intimate informational access to the plaintiff's life.

Prostitution clearly involves a person's sex life, so the link to intimate information is broadly consistent. It is of note, however, that the fact that the information was normatively public did not stop its classification as 'intimate' information. Furthermore, Inness went beyond focusing on the nature of the information as intimate, she noted that information about a person's past life can be considered intimate:[113]

> … because they are commonly imbued with emotional significance as far as their sharing is concerned; typically, we share secrets about our past with those for whom we feel love, care, or liking.

Under this view, what is important is the value placed on the act of sharing. Inness argued that if "someone intrudes into our past, they fail to acknowledge the emotion-laden value we accord to the sharing of much information about our past."[114]

Fried also saw privacy in terms of intimacy, viewing intimacy, along with "respect, love, friendship and trust",[115] as the ultimate value of privacy. He states that: "Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable."[116] Fried argued that privacy provides a "moral capital which we spend in friendship and love."[117] His argument is that privacy provides us with a sphere of information that we can share with our colleagues, friends and lovers.[118] While Fried acknowledges that there are good reasons to value privacy aside from developing fundamental relationships,[119] he argued that:[120]

> … [not tying privacy to respect, love, friendship and trust] leave privacy with less security than we feel it deserves; they leave it vulnerable to arguments that a particular

---

[113] At 128.
[114] At 130.
[115] Charles Fried "Privacy" (1968) 77 Yale L J 475 at 477. James Rachels "Why Privacy is Important" (1975) 4 Philosophy & Public Affairs 323 at 326 similarly sees privacy as important because it allows us to "maintain the variety of social relationships with other people that we want to have."
[116] Fried, above n 115, at 477.
[117] At 484.
[118] At 477.
[119] At 483. These reasons include control over information and liberty.
[120] At 484.

> invasion of privacy will secure to us other kinds of liberty which more than compensate for what is lost.

Fried defines intimate information as information that is shared with a few people only, so it would presumably exclude once public facts (although, he does not address such facts directly). Gerety, who also sees intimacy as integral to privacy, discusses *Briscoe* and argues that while the plaintiff's claim deserved to be upheld,[121] it was outside the concept of privacy he developed because "no narrowly conceived intimacy was intruded upon and since, moreover, the information was a matter of public record."[122]

The main critique of the intimacy concept is that it is too narrow. These critiques argue that the concept excludes many areas commonly protected by privacy but which do not involve "loving and caring relationships".[123] Solove, for example, noted that there are "many sexual relationships devoid of love, liking, or caring as there are many acts expressive of love, liking, or caring (such as buying gifts) that are not considered intimate."[124]

E Personal Information

One of the strongest proponents of the concept of privacy as related to personal information is Wacks, who argued that the privacy debate had lost its way. He argued that:[125]

> 'Privacy' has grown into a large and unwieldy concept. Synonymous with autonomy, it has colonised traditional liberties, become entangled with confidentiality, secrecy, defamation, property, and the storage of information. It would be unreasonable to expect a notion so complex as 'privacy' not to spill into regions with which it is closely related, but this process has resulted in the dilution of 'privacy' itself, diminishing the prospect of its own protection as well as the protection of the related interests.

Salvation, Wacks argued, comes in focusing on the core of the concept, which was the "protection against the misuse of personal, sensitive information."[126] Central to this concept is

---

[121] Tom Gerety "Redefining Privacy" (1977) Harvard Civil Rights-Civil Liberties Law Review (12) 233 at 236 and 263.
[122] At 294. Gerety notes that both *Briscoe* and *Sidis* are examples of moral wrongs, but which are ultimately "beyond the reach or help of law" (at 296).
[123] Solove, above n 70, at 1124. Solove cites Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, Chapel Hill, 1995) at 213 who he says "notes computer databases pose a significant threat to privacy but 'do not primarily affect … relationships of friendship, love, and trust. Instead, these threats come from private and governmental organizations - the police, welfare agencies, credit agencies, banks, and employers.'"
[124] Solove, above n 70, at 1123–1124.
[125] Raymond Wacks "Poverty of Privacy" (1980) 96 LQR 73 at 88.
[126] Wacks, above n 106, at i and xii.

an understanding of what is personal information. Wacks argued that personal information comprises:[127]

> … those facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold, or at least to restrict their collection, use or circulation.

Discussing once public facts directly, Wacks notes that "it would not be unreasonable … for an individual to wish to prevent the disclosure of facts concerning his trial and conviction for theft."[128] He concludes that such information would pass the personal information test but would not be private due to the "public records" nature of the information.[129] Wacks then notes that: "The passage of time may, however, alter the nature of such events and what was once a public matter may, several years later, be reasonably considered as private."[130] Recognising that the position may be wider than just information on convictions, Wacks argues that: "Similarly, the publication of what was once 'public' information garnered from old newspapers may several years later be considered an offensive disclosure of personal information."[131] Wacks' concept of personal information, therefore, covers once public facts.

Parent also offers a definition of privacy focused on personal information.[132] He proposes that someone has privacy if they do not have "*undocumented* personal information about oneself known by others".[133] Parent's concept of 'personal information' includes "facts about a person which most individuals in a given time do not want widely known about themselves."[134] Parent recognises that information belonging to the public record could be included in this definition of personal information. He notes that:[135]

> … there is nothing odd or misleading about the proposition that public documents contain some very personal information about persons. We might discover, for example, that Jones and Smith were arrested many years ago for engaging in homosexual activities.

---

[127] At xvi. See also Raymond Wacks *Privacy: A Very Short Introduction* (2nd ed, Oxford University Press, Oxford, 2015) at 2 and 46–48.
[128] Wacks, above n 106, at xvii.
[129] At xvii.
[130] At xvii.
[131] At xvii.
[132] Parent, above n 78, at 305.
[133] At 306 (emphasis added).
[134] At 306–307.
[135] At 308.

However, Parent then excludes such personal information from his definition by noting that personal facts belonging to the public record are documented and his definition excludes documented information. His reasoning is that: "What belongs to the public domain cannot without glaring paradox be called private and consequently should not be incorporated within a viable conception of privacy."[136] On the basis of his concept, Parent reasons that the outcome in *Melvin v Reid* was wrong. The facts were documented and "anyone could easily – i.e. without resort to snooping or prying - have found out about the plaintiff's past life."[137] However, he argued that *Sidis* "is a genuine privacy case" which the plaintiff should have won. While Parent provides no rationale for this conclusion, it likely rests on the fact that the publication disclosed *undocumented* information about Mr Sidis (that is, information about his life subsequent to his media exposure, when he was a virtual recluse).[138]

DeCew argues that Parent's concept is too narrow, noting that it does not take account of how the information becomes part of the public record in the first place (so information becoming part of the public record in error makes no difference), nor allows room for questioning what should be on the public record.[139] While not mentioning any once public fact cases, she notes the very real difference between information being "publicly accessible but in obscure documents" and a "widely distributed reprint".[140] DeCew argues that it is hard to see how the latter would not be "a further intrusion on the individual's privacy."[141] Other critiques of the 'personal information' concept note that it ignores important interests normally associated with privacy. The NZLC, for example, highlights that "most people would probably regard surveillance, spying and eavesdropping as invasions of privacy regardless of whether any new information, or any particularly sensitive information, is gained by these means."[142]

F Control

Westin's influential control concept of privacy defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[143] As a part of this definition, Westin identified "four

[136] At 308.
[137] At 324.
[138] At 308.
[139] Judith Wagner DeCew "The Scope of Privacy in Law and Ethics" (1986) 5 L & Phil 145 at 151–152. See also Moreham, above n 102, at 151–152 who had a similar critique.
[140] DeCew, above n 139, at 151.
[141] At 151.
[142] Law Commission, above n 76, at [2.22].
[143] Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967) at 7. Wacks *Privacy: A Very Short Introduction*, above n 127, at 43 states that: "Westin's definition has, however, exerted even greater influence in respect of its description of privacy in terms of the extent to which an individual has *control* over information about him- or herself." Penk, above n 70, at 5 views Westin as a proponent of the concept of limited access.

basic states" of privacy – solitude, intimacy, anonymity and reserve.[144] Solitude and intimacy are about being free from observation by others, with solitude being the person alone and intimacy being when the person is part of a small group.[145] Anonymity is when an individual is in public but is not identified or subject to surveillance.[146] Reserve is the "most subtle state of privacy" and is about not disclosing information about yourself to others, whether in public or as part of an intimate group.[147] Westin argues that: "Even in the most intimate relations, communication of self to others is always incomplete and is based on the need to hold back some part of one's self".[148] Westin's argument is that the right to privacy is the right for persons to decide for themselves their state of privacy and that people are "continually engaged in a personal adjustment process" between their desire for disclosure and participation in society versus withdrawal into a state of privacy.[149]

To find a place for once public facts within Westin's states of privacy, Westin's "reserve" must be considered.[150] If a person has committed an error in their past, but has moved on and changed or rehabilitated, then it could be argued that, in choosing to not disclose that information to new friends or intimates, the person is choosing the state of privacy of reserve. In addition, a person might tell their close intimates a fact about their past, but not want that information known publicly. If the information the person has chosen to keep in a state of privacy is then disclosed by a third party, the person has lost the ability to choose their state of privacy. Westin was also alive to the issues that can arise when old adverse information is remembered. Westin noted that the rise in data collection and processing had created a "record prison" for many people, where:[151]

> … past mistakes, omissions, or misunderstood events become permanent evidence capable of controlling destinies for decades. Out-of-date facts, such as previous political affiliations or nervous disorders, often go unrevised, and these can haunt a person's life.

Fried also takes a control-based view of privacy, where privacy is "the *control* we have over information about ourselves".[152] While this is a very broad concept of privacy which, on the face of it, would support once public facts, Fried's linking of privacy to intimacy, as discussed

[144] Westin, above n 143, at 31.
[145] At 31.
[146] At 31–32.
[147] At 32.
[148] At 32.
[149] At 7.
[150] At 32. Westin himself did not address once public facts. See also Lisa M Austin "Re-reading Westin" (2019) 20 Theoretical Inquiries in Law 53 at 60.
[151] Westin, above n 143, at 160.
[152] Fried, above n 115, at 482.

above, means it is likely he would define the information in the narrow vein of 'intimate' information.[153]

Critiques of the control concept point to a range of difficulties with it. Control is often equated with ownership of information;[154] however, information is not like other property, it "can be easily transmitted, and once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously in the minds of millions."[155] Privacy as control also often leads to contradictory conclusions. Wacks notes that:[156]

> … it fails to account for the fact that if I want you to know a fact about me and I am unable to communicate it to you then, according to the definition of "privacy" in terms of control, I should have *lost* privacy for I have lost control over the circulation of information about myself. Equally, if I succeed in total disclosure of my private life to you I should *not* have lost privacy. Neither of these can be correct.

Austin also argues that Westin's concept, "being so deeply rooted in interpersonal norms", may be "too narrow to account for the kinds of informational contexts we must now navigate."[157]

G Secrecy

Solove has noted that: "One of the most common understandings of privacy is that it constitutes the secrecy of certain matters".[158] Under this concept, he argues:[159]

---

[153] See Solove, above n 70, at 1111 who states that Fried "presumably, would define the scope of information as 'intimate' information (information necessary to form and foster relationships involving respect, love, friendship, and trust)."
[154] See Westin, above n 143, at 324–325 who concluded his discussion with the argument that personal information "thought of as the right of decision over one's private personality, should be defined as a property right".
[155] Solove, above n 70, at 1113. Meg Leta Jones *Ctrl + Z: The Right to be Forgotten* (New York University Press, New York, 2016) at 118 also highlights the differences between information and traditional property, noting that: "Unlike almost all other resources or properties, which have characteristics of divisibility, appropriability, scarcity, and decreasing returns on use, information functions in the opposite way. Information is infinitely shareable – I can possess it while you possess it, and a million others possess it."
[156] Wacks *Privacy: A Very Short Introduction*, above n 127, at 76.
[157] Austin, above n 150, at 80. At 54–55 Austin notes that these information contexts are the "infrastructure of surveillance" where digital platforms and tools are enabling data collection in both our online and physical worlds.
[158] Solove, above n 70, at 1105.
[159] Daniel J Solove "A Taxonomy of Privacy" (2006) 154 U Pa L 477 at 497.

> … privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information.

Posner, who is most frequently aligned to the secrecy concept, describes it as "the withholding or concealment of information, particularly, personal information".[160] However, while Posner describes the concept of privacy, he is also critical of privacy operating in this manner. He argues that the motivation for such secrecy is often to mislead those with whom a person transacts.[161] He argues that society views such false or misleading behaviour as wrong under consumer law, yet privacy law allows people to engage in such behaviour.[162]

In this regard, Posner discusses *Melvin v Reid* and *Briscoe*. He argues that information about past criminal activity is "undeniably material in evaluating an individual's claim to friendship, respect and trust"[163] and that "legal protection of its concealment would be inconsistent with the treatment of false advertising in the market for goods."[164] Posner notes that past criminal activity, while less relevant than recent criminal activity, is still relevant to "people considering whether to enter into or continue social or business relations with the individual."[165] He argues that people "conceal past criminal acts not out of bashfulness but because potential acquaintances quite sensibly regard a criminal past as negative evidence of the value of associating with a person."[166]

While Posner critiques the findings in *Melvin v Reid* and *Briscoe*, the reality is that under a secrecy concept of privacy, the information at issue in those case (and in fact all once public facts) would struggle to find protection because the information has been disclosed previously as part of the public record, and is therefore not secret. The main criticism of the secrecy view of privacy is that it is too narrow. For Solove, the narrow focus on concealed information misses the point that privacy "also involves the individual's ability to ensure that personal information is used for the purposes she desires."[167]

---

[160] Posner, above n 92, at 231. See also Richard A Posner "The Right of Privacy" (1978) 12 Ga L Rev 393. It should be noted that while Posner discusses the concept of privacy as secrecy he does not necessarily agree with it. See, for example, his commentary in *The Economics of Justice* that privacy is also about seclusion and the 'right to be let alone' (at 272–273).
[161] Posner, above n 92, at 235.
[162] At 233–234.
[163] At 260.
[164] At 260.
[165] At 260. Posner notes that if information about recent criminal activity was irrelevant then publishing such information would not injure a person.
[166] At 260–261.
[167] Solove, above n 70, at 1108.

H Pragmatic, Complex or Novel Definitions[168]

Some authors have moved away from trying to find a core of the privacy concept, instead focusing on complex or pragmatic definitions. Gavison's limited access and Westin's states of privacy have been viewed in this vein.[169] However, one of the more comprehensive such definitions has been provided by Solove. Solove saw substantial limitations in attempting to locate a core or essence of privacy,[170] favouring instead a "family resemblances" model,[171] which sought to identify the similarities in the practices and disruptions at the heart of most privacy issues.[172] Under Solove's approach, new privacy problems do not need to be fitted into old concepts. Instead, Solove argues that:[173]

> We should seek to understand the specific circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption?

While Solove does not mention once public facts in his approach, he does note that disclosure of information is a particular type of disruption and that "disclosure of a person's criminal past can interfere with that person's ability to reform herself and build a new life".[174] Solove sees the value of protecting against this type of disruption as depending "in part, upon the social importance of rehabilitation."[175]

In 2006, Solove further developed his view of privacy by proposing a taxonomy to "guide the law toward a more coherent understanding of privacy and to serve as a framework for the future development of the field of privacy law".[176] Following his earlier theme, his intent was to "shift the focus away from the vague term 'privacy' and toward the specific activities that pose privacy problems."[177] Solove's taxonomy proposed 16 different subgroups of "harmful activities",[178] two of which are of particular interest for the purposes of the present research – disclosure and increased accessibility.[179] Disclosure occurs when "certain true information

---

[168] Law Commission, above n 76, at [2.32] refers to "pragmatism" and Penk, above n 70, at 7 refers to: "More complex definitions".
[169] See Penk, above n 70, at 7.
[170] Solove, above n 70, at 1099.
[171] At 1091.
[172] At 1129–1130.
[173] At 1147.
[174] At 1130.
[175] At 1130.
[176] Solove, above n 159, at 478.
[177] At 482.
[178] At 489.
[179] The 16 activities were grouped into four categories: (1) information collection (comprising surveillance and interrogation); (2) information processing (comprising aggregation, identification, insecurity, secondary use, and

about a person is revealed to others".[180] In discussing the harm of disclosure, Solove notes that:[181]

> The risk of disclosure can prevent people from engaging in activities that further their own self-development … Disclosure can inhibit people from associating with others, impinging upon freedom of association, and can also destroy anonymity, which is sometimes critical for the promotion of free expression.

Solove also argued that disclosure can be harmful "because it makes a person a 'prisoner of [his or her] recorded past'".[182] He states that:[183]

> People grow and change, and disclosures of information from their past can inhibit their ability to reform their behaviour, to have a second chance, or to alter their life's direction.

For Solove, therefore, the harm was "not so much the elimination of secrecy as it is the spreading of information beyond expected boundaries."[184]

The harm of increased accessibility, Solove argues, occurs when information that is already available to the public becomes easier to access. This harm, which draws inspiration from the concept of 'practical obscurity',[185] is not negated by previous publication, rather it is focused "on the extent to which the information is made more accessible."[186] Practical obscurity derives from the case of *US Department of Justice v Reporters Committee for Freedom of the Press*, where the United States Supreme Court had to decide whether or not to make a person's rap sheet compiled by the FBI available to a journalist. The Court found that the rap sheet did not have to be disclosed, noting that:[187]

---

exclusion); (3) information dissemination (comprising breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation, and distortion); and (4) invasions (comprising intrusion and decisional interference).

[180] At 531.

[181] At 532.

[182] *Records, Computers and the Rights of Citizens* (United States Department of Health Education & Wealth, xxxii 1973) cited in Solove, above n 159, at 533.

[183] Solove, above n 159, at 533.

[184] At 535.

[185] At 539–540.

[186] At 540.

[187] *US Department of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989). See Patrick C File "A History of Practical Obscurity: Clarifying and Contemplating the Twentieth Century Roots of a Digital Age Concept of Privacy" (2017) 6 U Balt J Media L & Ethics 4 at 7 for a discussion of the case and practical obscurity.

> … although the information in the rap sheet was public and available at its original sources – the records of local police stations and courthouses – the fact that it was not otherwise easily obtained all at once or in one place created a unique expectation of privacy, which it called 'practical obscurity,' that could justify the government's withholding it.

Solove's taxonomy of privacy, therefore, has much room for once public facts which have been published previously and will often inhibit a person from rehabilitating and developing their self.[188] However, Solove's approach has been critiqued as providing "no basis for establishing why some harms are privacy violations and others are not", nor for assisting people to understand "what it means to experience privacy."[189]

In the face of modern technology, Cohen has focused on privacy's role in human flourishing. She argues that:[190]

> Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.

For Cohen, therefore, privacy is "an interest in breathing room to engage in socially situated processes of boundary management".[191] This boundary management refers to the interpersonal boundaries which exist between people in diverse contexts. The concept of 'boundedness' builds upon Westin's "reserve"[192] and is influenced by the privacy vision of Irwin Altman, a social psychologist writing in the 1970s.[193] Altman put forward a view of privacy as a "boundary control process whereby people sometimes make themselves open and accessible to others and sometimes close themselves off from others."[194] Cohen's vision of privacy is about " refusing access, visibility, or interference with particular decisions" and "preventing the seamless imposition of patterns predetermined by others."[195]

---

[188] See discussion in Chapter 4(II)(A)(1).
[189] Law Commission, above n 76, at [2.37]–[2.38].
[190] Julie E Cohen "What Privacy is For" (2013) 126 Harv L Rev 1904 at 1905.
[191] Julie E Cohen *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, New Haven (Conn), 2012) at 149. Cohen argues that people are situated within a culture and context (at 128). Cohen, above n 187, at 1910 argues that: "People are born into networks of relationships, practices and beliefs, and over time they encounter and experiment with others, engaging in a diverse and ad hoc mix of practices".
[192] See Westin, above n 143, at 32.
[193] Cohen *Configuring the Networked Self*, above n 191, at 130–131.
[194] Irwin Altman "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33 Journal of Social Issues 66 at 67.
[195] Cohen Configuring the Networked Self, above n 191, at 130–131.

For Cohen, privacy focuses not only on the individual interest, "but also collective interests in human flourishing and in the ongoing development of a vibrant culture."[196] Cohen also argued that diminished privacy, and therefore the reduction in the capacity for critical subjectivity, shrinks the practice of citizenship and has a negative effect on democratic self-government. In its place, she argues, is a "modulated democracy", where citizens behaviour is modulated by information technology.[197] She gives the example of search engines that filter and rank search results thereby influencing what information citizens consume.[198] She continues:[199]

> Citizens of a modulated society are not the same citizens that the liberal democratic political tradition assumes, nor do their modulated preferences even approximately resemble the independent decisions, formed through robust and open debate, that liberal democracy requires to sustain and perfect itself. The modulated society is the consummate social and intellectual rheostat, continually adjusting the information environment to each individual's comfort level. Liberal democratic citizenship requires a certain amount of *dis*comfort – enough to motivate citizens to pursue improvements in the realization of political and social ideas. The modulated citizenry lacks the wherewithal and perhaps even the desire to practice this sort of citizenship.

Cohen's concept of privacy has been used by other scholars to support once public facts. Leta-Jones argues that under Cohen's theory: [200]

> … an ongoing record of personal information may create seamlessness. For the dynamic self, creating gaps over time may be as important as creating gaps in any type of informational seamlessness. The right to be forgotten can be understood as the right to retroactively create gaps or boundaries to promote emergent subjectivity and the dynamic self.

Nissenbaum's influential account of privacy as contextual integrity also focuses on individuals' situated actions and expectations. Nissenbaum argues that contextual integrity – and therefore privacy – is only maintained when norms of appropriateness of information about people and norms of flow or distribution of information about people are upheld. Nissenbaum argues that contextual integrity is "maintained when both types of norms are

[196] Cohen, Configuring the Networked Self, above n 191, at 150.
[197] Cohen, above n 190, at 1912.
[198] At 1912–1913.
[199] At 1918.
[200] Leta Jones, above n 155, at 93.

upheld, and it is violated when either of the norms is violated."[201] Underpinning this theory is the view that there are no places "not governed by at least some information norms."[202] These norms set out what sort of information a person should provide in a particular context, so the information given to a doctor is not the same as that given to a hairdresser. Why not? Because norms of behaviour tell us what information should be imparted in which situations. The information flow norms set out how information should move from one person to another in society. An example of such information flow norms are the norms of confidentiality expected in various relationships.[203] Furthermore, Nissenbaum argues that there is a presumption in favour of the status quo of the norms, to protect the norms from challenges from changing behaviour in some sectors of society. That is not to say the norms do not change, just that adequate reasons for change must exist.[204]

While Nissenbaum did not address once public facts in her theory of contextual integrity, her earlier works on a similar theme recognised that invasive public surveillance activities involve not just shifting information across contextual lines but also "temporal lines as information collected in the past – sometimes a very long time past – is injected into a current setting."[205] The implication of this statement is that such temporal movement can also disrupt norms of appropriate information flow.[206] Furthermore, Nissenbaum's argument that there is no place not governed by information norms means that even public information is subject to norms of information flow. For example, a person is unlikely to expect an article published in a local or community newspaper to appear as a headline on a major national media site. That person would also not expect the article to be republished 10 or 20 years later. In regard to appropriateness of information, if the social norm is that old information is forgotten, or if not forgotten at least not used, then the publication or easy accessibility of that information may have disrupted such a norm. However, some argue that the modern information age means that these norms no longer exist.[207] Whether this argument is valid or not will be considered further in the research, but for the purposes of this discussion it can at least be seen how the

[201] Helen Nissenbaum "Privacy as Contextual Integrity" (2004) 79 Wash L Rev 119 at 138.
[202] At 139.
[203] At 140–143. These relationships include, for example, the relationship between lawyer and client, priest and confessor, and doctor and patient.
[204] See generally at 143–146.
[205] Helen Nissenbaum "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998) (17) Law and Philosophy 559 at 585.
[206] At 581.
[207] Harvey, above n 1, at 281–282. Harvey argues that "the development of the Internet and especially the rise of social networking has given rise to the 'look-at-me' Internet users who seem to have no inhibition about diarising their every move with tweets, Facebook entries or the ubiquitous 'selfie'." He then notes that "it may be that social network sites will present a future challenge to expectations of privacy altogether."

existence of these norms means that once public facts could well be a disruption to contextual integrity.[208]

I A Definition of Privacy

For the reasons set out below, the present research argues that the concept of privacy based on limited access provides the most appropriate way to think about privacy. Limited access is broad enough to address the range of harms that are typically considered under the banner of privacy, including access to information, physical access to a person and attention being paid to a person. Other concepts, like secrecy, intimacy and personal information, are too narrow and omit areas that people ordinarily think of as private. The concepts of human dignity, personhood and control are persuasive. The present research argues that privacy is absolutely about dignity and respect for people; however as a functioning definition it is too broad – it provides no guidance on when the label should be applied and when it should not. That said, the present research strongly endorses dignity as a core *value* protected by privacy. The control concept is also immensely attractive. Control is fundamental to privacy and data protection statutes, and many instances of privacy losses are where information is out of the subject's control. However, control is also a slippery definition. If a person hands over sensitive information about themselves, is that a loss of privacy or not? In exercising control to give the information, it is not. However, now that the information is with someone else, it is out of the person's control. Furthermore, a person might have control, but lack meaningful choice, so the outcome is still a lack of protection for privacy.[209] Solove's pragmatic concept is also attractive, as it essentially covers all aspects of all concepts of privacy. This breadth of coverage means it lacks the clarity a definition needs and it provides no ready way to determine whether or not a matter relates to privacy.

The limited access concept focuses on the amount or degree of privacy a person has by reference to the amount of access another person has to them. It recognises that a person losses privacy when others gain access to them. Every time *A* gains a little more access to *B*, whether via having more information or more physical proximity, then *B* loses a little bit of privacy. That may not be unwanted or of concern to *B*, but acknowledging it for what it is might prompt people to think critically about who has access to them and in what ways. Furthermore, when that access becomes concerning, then, with the definition of limited access in mind, it can be easily understood that the issue is a privacy one.

[208] Leta Jones, above n 155, at 90 argues that a RTBF is "potentially even supported by contextual integrity."
[209] Austin, above n 150, at 54–55.

III Privacy in Public

In addition to most of the key concepts of privacy being flexible enough to include once public facts, there is a growing literature questioning the traditional position that there is no privacy in that which is public.[210] This traditional position relies on a dichotomy between the private and the public spheres.[211] The private sphere is mostly associated with the home and personal or intimate information. The public sphere is the outside world, the world of community and free accessibility. Generally, privacy law has protected the former and shunned the latter. The literature challenging the traditional view is of particular importance to once public facts because such facts are those that are or have been in the public domain and a growing acceptance of privacy in public provides additional support for the protection of once public facts under the banner of privacy.

Tverdek describes and critiques four ways that information can be considered 'public'. First, he notes that public information is often simply that which is "left-over" once something has been described as "private".[212] However, this approach does not help determine what makes information public or private. Second, he notes that what is public is often what we do in places where we can expect to be witnessed by others. However, this approach can be strained by persistent, and sometimes surreptitious, surveillance that occurs in public places. Third, he considers the "temporal transformation" of information, so that something becomes public when it is "revealed in a particular way or to particular audiences. Think of this [as] a 'cat-out-of-the-bag' or 'toothpaste-out-of-the-tube' conception of 'public' information."[213] However, this third approach does not address the validity of the disclosure act and creates the unusual situation that additional disclosure becomes a right bundled together with the initial disclosure.[214] Fourth, he considers public information as a relational construct, so public information is "information for which our preferences about disclosing do not rest on the

[210] The American Law Institute *Restatement of the Law of Torts* (2 ed, 1977) § 652D cmt b highlights the traditional position with its declaration that under the public disclosure tort in the United States: "There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public." A leading case to illustrate this point is *Gill v Hearst Publishing Company* 253 P 2d 441 at 442 (Cal 1953) which involved a couple photographed in a park in "an affectionate pose", which was published in an article in Harpers Bazaar magazine.

[211] See, for example, Bert-Jaap Koops and Masa Galic "Conceptualizing space and place: lessons from geography for the debate on privacy in public" in Tjerk Timan, Bryce Clayton Newell, Bert-Jaap Koops (eds) *Privacy in Public Space Conceptual and Regulatory Challenges* (Edward Elgar Pub, Northampton MA, 2017) 19 at 28. The authors note that while this distinction between the privacy and public spheres is not necessarily universally adhered to, it has "proven compelling and enduring."

[212] Edward Tverdek "What Makes Information 'Public'?" (2008) 22 Public Affairs Quarterly 63 at 64.

[213] At 66.

[214] At 67.

'special' nature of the recipient."[215] However, this fourth approach has issues because on occasion people are happy to reveal intimate information to strangers but not to close friends and family.

While finding fault with all four concepts, Tverdek leans towards the fourth approach to public information, but acknowledges "there are two quite distinct privacy interests involved in distinguishing 'private' from 'public' information".[216] There is an "esteem-based interest", which is an interest that reflects how people are judged by others, and a "practical/prudential interest" which relates to the potential consequences of the information becoming public, for example identity theft or fraud.[217] For Tverdek, the interaction of the particular interest and the nature of the relationship between the discloser and the recipient assists in identifying public information. Public information is, therefore, information disclosed within a personal relationship that impacts a practical/prudential interest and information disclosed in an impersonal relationship that impacts the esteem-based interest. So a credit card number disclosed to a spouse is public information but the disclosure of the credit card number to an adult website would make the credit card number private information (as it is an example of information disclosed in an impersonal relationship that impacts a practical/prudential interest).[218]

Tverkek's recognition that what defines public information is more than simply an act of disclosure or the place of occurrence is useful. Furthermore, his recognition that what distinguishes a person's sense of privacy relates to relationships and impacts of disclosure is also a welcome start to a more nuanced understanding of privacy in public.

Hartzog also highlights the complex nature of describing information as public. Hartzog argues that public information has generally been conceptualised in three ways: (1) a descriptive manner; (2) as something that is "not private"[219] and (3) as something designated 'public' by a government authority. Hartzog argues that the descriptive concept of public information usually focuses on the accessibility of the information, how widely the information is known or whether the information is of interest to society. The most common trait of the 'accessibility' description is:[220]

---

[215] At 68.
[216] At 71.
[217] At 71.
[218] At 73. The disclosure of the fact that the credit card holder enjoys watching porn to the adult website would be public information, because while that impacts an esteem-based interest, it is disclosed in an impersonal relationship. That same information disclosed to a group of friends would be private information.
[219] Woodrow Hartzog "The Public Information Fallacy" (2019) 99 B U L Rev 459 at 467.
[220] At 489.

> … that it is not contingent upon how many people have actually accessed or were cognizant of information, but rather either how hypothetically difficult it would be for people or just one person to access information or for others to be geographically close enough to be exposed to a person's acts.

He argues that the hypothetical accessibility is merely conjecture based on a range of assumptions for which there are no rules on how the assumptions are determined. For Hartzog, the 'widely known' description is more defensible than hypothetical accessibility because it is based on what people actually know.[221] The final descriptive account – information which is of interest to society – focuses on the content of the information, rather than the context in which it is disclosed. This descriptive account is generally employed because "in many contexts peoples' privacy interests will be overridden by benefits of a more public disclosure or society's 'right to know'."[222]

Hartzog argues that defining public information as something that is not private is simple and common, but ultimately circular. If it is argued that information is not private because it is public what is being said is that information is not private because it is not private. Hartzog's last concept of public information – that which has been designated so by a relevant governmental authority – is most commonly reflected in public records. This concept, Hartzog argues, is more than "just a description of the information's context or failing to find a privacy interest"; it is value-driven, based on a variety of reasons including "government accountability, research, industry and market support, facilitation of government services, civic participation, and much more."[223]

Ultimately, Hartzog argues that it needs to be acknowledged that labelling information as public "is a value-laden exercise of power"[224] and there is no "objective, value-neutral criterion of 'public' information."[225] Calling information public is a judgement call about what information should be protected and what sort of practices are allowed. It is important to keep this in mind, he argues, when values such as privacy, free speech and security are in conflict. If this value judgement is not recognised, we "disadvantage privacy by creating presumptions of the public nature of information using questionable assumptions about

[221] At 505.
[222] At 506.
[223] At 511–512.
[224] At 512.
[225] At 489.

behavioural norms and societal expectations."[226] Hartzog also argues that to the extent that descriptive factors are important in determining public information, the factors he identifies above – accessibility, how widely-known information is, and the public interest in the information – are wrong. He proposes that obscurity and trust are a better measure of what constitutes public information. In regard to obscurity, he notes that it:[227]

> … is the notion that when our activities or information is unlikely to be found, seen, or remembered, it is, to some degree safe … Every day we make decisions about where we go, what we do, and what we share based upon how obscure we think we are. Most of our information online is obscure as well. For example, just because information is hypothetically available does not mean most (or even a few) people have the knowledge and ability to access information.

Hartzog notes that what makes information obscure is "complex", but includes factors like "searchability; permanence; comprehensibility; identifiability; and the resources, motivation, and pre-existing knowledge of those who seek to surveil or make use of data."[228]

Like Tverdek, Hartzog's nuanced consideration of what makes information public is welcome. His identification that what is public is not an objective criterion, but a value-laden exercise, is also useful. It will be seen that too often worthy privacy interests are dismissed because of the label 'public information' without real analysis of the interest being furthered by labelling the information public.[229]

For Paton-Simpson, what is public can have different meanings. What is 'public' can be viewed in a normative sense, "in that its publication is morally or legally permissible",[230] or a descriptive sense, "in the sense of being widely known or generally available",[231] or in a hybrid sense where "the matter is a 'complex social fact, reflecting both norms and practices conforming to the norms.'"[232] However, using the simplistic label of public discourages

---

[226] At 514.
[227] At 515–516. In regard to trust, Hartzog notes that people feel safe when their actions and information "are disclosed within relationships of trust."
[228] At 518.
[229] See, for example, the case of *Florida Star v BJF* 491 US 524 (1989). This case is further discussed in Chapter 6(IV)(A) below.
[230] Elizabeth Paton-Simpson "Private Circles and Public Squares: Invasion of Privacy by Publication of Private Facts" (1998) 61 Mod L Rev 318 at 321.
[231] At 321.
[232] Ruth Gavison "Feminism and the Public/Private Distinction" (1992) 45 Stan L Rev 1 at 6 cited in Paton-Simpson, above n 230, at 322. Paton-Simpson argues that this 'hybrid' sense of what is public can be seen in the United States test for the disclosure tort. This is discussed further below n 801.

rigorous consideration of what is being meant by the label and whether there is a privacy interest worth protecting.

For Paton-Simpson, private and public are not mutually exclusive categories, "but matters of degree, existing on a continuum. A fact can be public to some extent and also private to some extent."[233] Paton-Simpson points to the enormous difference between "whether a fact is known by a few people or broadcast to thousands."[234] Treating privacy and public as all or nothing concepts is a mistake known as the "fallacy of bifurcation."[235] She highlights that:[236]

> Because our language is full of opposites the tendency to bifurcate is common. We are prone to people the world with the 'haves' and the 'have-nots,' the 'good' and the 'bad,' the 'normal' and the 'abnormal' – forgetting that somewhere between these extremes lie numerous gradations, any of which could serve as further alternatives to an *either/or* polarity.

Nissenbaum argues that there are a number of reasons why theories of privacy have neglected to consider privacy in public. Conceptually, theories of privacy have often simply adopted traditional political and legal theory that demarcates between the private realm and the public realm.[237] This distinction is reinforced by the focus of many theories of privacy on privacy's role as "an important means by which individuals may sustain power, liberty, and autonomy against potentially overwhelming forces of government."[238] Normatively, Nissenbaum argues that privacy in public has been the victim of the commonly held argument that while privacy is important, it must be balanced against competing interests. When this balance occurs, information that is in the public arena is seen as "ostensibly innocuous" or information that people have willingly exposed to public view, therefore it does not take much of the competing interest to outweigh the argument for privacy.[239] Nissenbaum calls this the "'knock down' normative argument."[240]

From an empirical perspective, Nissenbaum argues that threats to public information have arisen only relatively recently with the advent of modern information technologies, and therefore, theories of privacy which arose previously simply had no need to consider privacy

---

[233] Paton-Simpson, above n 230, at 324.
[234] At 324.
[235] At 325.
[236] At 325, citing S Morris Engel *With Good Reason: An Introduction to Informal Fallacies* (New York: St Martin's Press, 2nd ed, 1982) 112.
[237] Nissenbaum, above n 205, at 568.
[238] At 569.
[239] At 571.
[240] At 573.

in public. As an example of such threats, Nissenbaum points to data aggregation, where isolated pieces of public information, which of themselves are not especially revealing, are aggregated into "assemblages [that] are capable of exposing people quite profoundly."[241] These assemblages can "be broad, deep and traverse time" and can be "rich enough to reveal aspects of an individual's character, to ground predictions about their propensities, and even suggest ways of manipulating them."[242] Nissenbaum argues that theories of privacy should be concerned with privacy in public because "even in the public sphere individuals have legitimate privacy interests."[243]

Solove argues that privacy is more complicated than the traditional binary view of privacy that if "a person is in a public place, she cannot expect privacy."[244] Solove argues that modern technology like ubiquitous surveillance, the overwhelming collection of data, and exposure of that data to others (either by parties themselves or third parties) challenges this binary view of privacy. Accordingly, what is important is not "whether something is exposed to others … [but] the nature of the exposure and what is done with the information."[245] Furthermore, Solove argues that people expect anonymity in many of their public interactions – "to be just a face in the crowd, another ant in the colony"[246] – and they have expectations about what is appropriate in a particular context. On this latter point, Solove notes that "there are different social norms for different situations, and broadcasting matters beyond their original context takes away our ability to judge the situation appropriately."[247] Finally, Solove argues that most people operate "in realms that that are neither purely public nor purely private."[248] He posits the following scenario:[249]

> Suppose you're on a train and you have a cell phone conversation with a friend. The person sitting next to you secretly records your conversation and makes the recording available online. Despite the fact you exposed your conversation to people nearby, you didn't expect your conversation to be recorded and made available to the world.

[241] At 589.
[242] At 589–590.
[243] At 591.
[244] Daniel J Solove *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, New Haven, 2007) at 163.
[245] At 164.
[246] At 165.
[247] At 165.
[248] At 165–166.
[249] At 166.

Solove argues that what exists is a "complicated set of norms, expectations, and desires that goes far beyond the simplistic notion that if you're in public, you have no privacy"[250] and that ultimately the law should recognise some level of privacy in public.[251]

McClurg finds support for privacy in public places in the works of other theorists.[252] He argues that Westin's definition of privacy is broad enough to allow privacy in public, pointing to Westin's statement that:[253]

> When people go into stores, hotels, restaurants and other places of public accommodation, they do not expect solitude and total freedom from observation. However, they do not expect to be under secret surveillance, especially in those places times and places for which *social custom has set some norms of privacy, even in 'public' situations*.

He also sees support for privacy in public in Gavison's limited access. He argues that people can gain access to a lot of information about a person by observing them from a public place. Furthermore, Gavison's lack of attention (anonymity) provides powerful support for privacy in public. McClurg notes that: [254]

> When no one is paying attention to us, we are free to go about our business even in public with little concern for relinquishing personal information about ourselves to others.

McClurg argues that one of the underlying premises of no privacy in public places is that a person assumes the risk of public inspection when he or she goes into a public space. However, McClurg refutes this premise. He argues that it is based on acknowledged and voluntary consent; however, in reality people have no knowledge of the risk, and voluntariness is mythical at best. He notes that: "Merely to survive in society requires that people spend a considerable amount of their time in places accessible to the public."[255] Socio-economic factors mean that some people spend more time outdoors than others and saying "that homeless people have 'voluntarily' consented to any and all public inspection, no matter how intrusive, would be insensitive and inappropriate."[256] Like a number of the other scholars discussed above, McClurg argues that "privacy is not an all or nothing concept" and that

---

[250] At 166.
[251] At 170.
[252] Andrew J McClurg "Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" 73 (1995) 73 N C L Rev 989 at 991.
[253] Westin, above n 143, at 112, cited in McClurg, above n 252, at 1029 (emphasis added).
[254] McClurg, above n 252, at 1033.
[255] At 1040.
[256] At 1040, citing Westin, above n 143, at 41. See also Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 ITLJ 305 at 343.

while a person surrenders privacy when they go out in public "it does not follow that she forfeits all legitimate expectations of privacy".[257]

Paton-Simpson also takes aim at the idea that a person has no reasonable expectation of privacy in a public place. She argues that just because a location is publicly accessible does not mean that it is not secluded, suggesting that "public access is only loosely connected with public exposure."[258] She considers the difference between a person's expectations of privacy in a quiet bookstore and if they were at a parade on a public street – both 'public' places. There can also be exposure of information to a large group of people who form a linked community (for example, a group of couples having IVF at a local hospital), yet still a sense of privacy in that information vis-à-vis the whole world.[259] Conversely, Paton-Simpson points out that being in a public space does not necessarily ensure exposure, if that space is empty or no one is paying attention. Paton-Simpson also points to the differences between casual observation and systemic surveillance, arguing that the latter "can have a severe impact on privacy, producing a fairly detailed picture of a person's life and allowing inferences to be drawn beyond the facts observed."[260] This impact on privacy can occur despite the systemic surveillance only ever occurring in public places. For Paton-Simpson, anonymity and social rules also protect privacy in public, as does the usually fleeting nature of much of what occurs in public.[261] As a result, she argues that: "Reasonable expectations can be violated by making a permanent record of what is revealed in public only briefly."[262]

Paton-Simpson also rejects what she argues is another underlying assumption of the argument that there is no privacy in public places – that by going out in public an individual consents to the intrusion or waives their right to privacy. She argues that consent or waiver assumption overlooks the fact that consents can be conditional or restricted (that is, people may consent to exposure to a limited group but not to the whole world) and assumes that people have a choice about exposing their affairs in public.[263] Paton-Simpson sees public privacy as an important value, both for the overall level of privacy in society and for its connection to

---

[257] McClurg, above n 252, at 1044.
[258] Paton-Simpson, above n 256, at 322.
[259] See *YG v Jewish Hospital of St Louis* 795 S W 2d 488 (Mo App, 1990).
[260] Paton-Simpson, above n 256, at 324.
[261] At 327. Paton-Simpson uses the examples of the social norms which exist in men's urinals and a person writing in their diary while sitting in an uncrowded park. The latter person "would be surprised and offended if a stranger crept up behind her and read over her shoulder."
[262] At 327.
[263] At 334. Paton-Simpson cites *YG*, above n 256, as an example of conditional consent. In that case the plaintiff's consent to disclose information to a small group was held not to be consent to a wider, public, disclosure. In regard to choice, Paton-Simpson notes that people often do not have a choice to go into public spaces, for example, "people may have to queue in a government building in order to collect social security payments that they need to survive" (at 338).

freedom of association and in "facilitating more equitable access to the benefits of privacy."[264] She notes that much of what people do is done in public, including where a person "borrows a public library book, goes shopping, or goes out on a date", and that these discrete bits of personal information can be aggregated into a "fairly detailed picture of a person's private life".[265] Therefore "to neglect the protection of public privacy is to leave many of the most sensitive details of people's lives vulnerable to unwarranted scrutiny."[266] Furthermore, she argues that if privacy only protects private spaces then it risks becoming a right "enjoyed only by the affluent."[267]

Ultimately, Paton-Simpson believes that the interest in privacy in public and the competing interests like freedom of expression can be balanced "without resorting to a blanket exemption for public places."[268] What is required is a contextual analysis and an appropriate weighing of the competing interests.

Moreham also argues that it is possible to have a reasonable expectation of privacy in public places. She reasons that when people go into public they can "choose how much or how little of themselves they reveal to others".[269] People do this a number of ways, including clothing choice, choosing not to talk about personal matters, and not conducting actions usually reserved for private spaces (for example, undressing or receiving medical treatment). Furthermore, it is a breach of privacy if the images or information obtained from a public space is disseminated to a much wider audience than at the public space from which the images or information came. She argues that this wider dissemination is important because people tailor their actions dependent on the environment that they are in. A person who sunbathes topless on a secluded public beach makes an assessment based on who is present on the beach at the time. That person "might well have conducted herself differently; in particular she might have decided to cover herself up or move to some other location" if she knew that a photo or video of her sunbathing topless was going to be posted on the internet.[270] For Moreham, multiple factors are relevant for determining whether there is a reasonable expectation of privacy in public. These factors comprise the claimant's location, including the number of people present when the information was obtained; the nature of the claimant's activity, including whether the event was involuntary or particularly "intimate, humiliating or

[264] At 340.
[265] At 341.
[266] At 341.
[267] At 343. See also Westin, above n 143, at 41. This risk was also discussed by McClurg, above n 252.
[268] Paton-Simpson, above n 256, at 344–346.
[269] Nicole Moreham "Privacy in Public Places" (2006) 65 CLJ 606 at 617. Moreham also argues that privacy in public is consistent with her theory of privacy as "desired inaccess", which is discussed at above n 102.
[270] At 619.

traumatic";[271] the way in which the image or information was obtained (with surreptitious acquisition, the use of technology to break through "self-presentation barriers",[272] and harassing conduct all making the claim for privacy in public stronger);[273] and the extent to which the publication focuses on the claimant.[274]

It is not just legal scholars who have argued for public information to have a place within privacy. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR) states that: "Everyone has the right to respect for his private and family life, his home and his correspondence."[275] The European Court of Human Rights (ECtHR) has determined that the private life protected by this article is broad enough to include public information. In *Case of LB v Hungary*, the Court held that publication of a person's name, home address and tax identification number on a list of major tax evaders engaged the person's private life despite the fact that the information could "arguably be considered conduct that may be recorded or reported in a public manner".[276] In *NŠ v Croatia* the Court noted that the fact that information is already known to the public might "not necessarily remove the protection of Article 8 of the Convention, especially if information was neither revealed by a person concerned nor that person has consented to its disclosure".[277]

While the above discussion shows that many have rejected the traditional view of privacy in public, not all do. Anderson argues that calls for privacy in public overstate the privacy harm *and* understate the benefits of "exposing truthful information shared in public."[278] Focusing on what she calls "the obscurity problem",[279] when a private person collects and discloses information that someone else shared in public, thereby consigning the exposed person to a loss of obscurity, Anderson argues that the harm is not as permanent as advocates claim, can be readily mitigated by the "right of reply" which exists in most modern technology, and cannot be easily quantified.[280] Furthermore, Anderson believes that the benefits from exposure will in most instances outweigh any overstated harms. Exposure ensures that government officials are accountable and it can deter criminal and "objectively-undesirable

[271] At 623. Where the event was involuntary or traumatic then only a strong public interest should outweigh the privacy interest. Simply adding colour or human interest to a story does not provide enough public interest.
[272] At 630.
[273] At 631.
[274] See generally at 620–635.
[275] European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (opened for signature 4 November 1950, entered into force 3 September 1953) [ECHR].
[276] *Case of LB v Hungary* ECHR 36345/16, 12 January 2021, at [23].
[277] *NŠ v Croatia* ECHR 36908/13, 10 September 2020, at [100].
[278] Heidi Reamer Anderson "The Mythical Right to Obscurity: Pragmatic Defense of No Privacy in Public" (2012) 7 ISJLP 543 at 549.
[279] At 550.
[280] At 578–581.

behaviour".[281] There can also be emotional and therapeutic benefits from exposure – an alcoholic being profiled in public can lead to other alcoholics feeling "connected and no longer alone";[282] celebrities exposed as gay can empower others to come out and thus lead to changed social norms.[283] However, Anderson does not completely reject the privacy in public argument; rather, she limits it to special cases where the exposure involves "a body part or bodily activity that society generally regards as 'private' even when the person ventures into 'public'."[284] In these cases Anderson argues the balance falls in favour of the harms rather than the exposure. She cites Posner, who stated that: [285]

> … because the individual's desire to suppress the photograph [of a body part] is not related to misrepresentation in any business or social market place, there is no basis for a presumption that the social value of disclosure exceeds that of concealment.

However, it is unclear why exposure of genitals is more private than exposure of sexual preferences or exposure of medical conditions, or why hiding body parts is not a misrepresentation, but it is to hide sexual preferences or medical conditions.

The increasingly nuanced view of what is public outlined by most of the scholars reviewed above is welcomed. It recognises that describing information or places as public can have diverse interpretations and without understanding what it actually means to label information or a place 'public', then any argument for no privacy for that information or in that place is fraught. Hartzog has argued that labelling matters 'public' has become a "permission slip for surveillance and personal data practices".[286] He further points out that privacy has had to clarify its meaning in order to be "useful in law or policy", but that "the concept of public information has been given a free pass."[287] However, the articles and scholarship referred to above are a step towards ensuring that the free pass becomes an earned pass. The articles and scholarship recognise that what is public is a complex question based on a range of factors including social expectations, context, the obscurity of the information, the extent of the exposure and the consequences of exposure. Furthermore, the technological developments over the last 20 years have meant that people live their lives in increasingly public spaces and forums, and excluding such spaces and forums from privacy protection will exclude a large

[281] At 589. The undesirable behaviour Anderson refers to includes reckless driving, poor tippers and unruly customers.
[282] At 594.
[283] At 595.
[284] At 598.
[285] At 599.
[286] Hartzog, above n 219, at 459.
[287] At 466.

range of people from privacy protections, leaving their information unprotected and at the mercy of anyone who wishes to use it.

IV A Tikanga Concept of Privacy[288]

A Introduction

The present research considers in-depth privacy law in New Zealand. One of the predominant ways privacy is protected in New Zealand is via the disclosure tort. The disclosure tort hinges on reasonable expectations of privacy, which themselves depend on the values that exist in society.[289] In many instances, these values will be underpinned by tikanga Māori, Māori customary law. Custom and values have always influenced the common law and there is growing recognition that tikanga Māori is therefore an aspect of the common law.[290] In *Takamore v Clarke,* Elias CJ stated that:[291]

> Values and cultural precepts important in New Zealand society must be weighed in the common law method used by the Court in exercising its inherent jurisdiction, according to their materiality in the particular case. … Māori custom according to tikanga is therefore part of the values of the New Zealand common law.

Understanding broader Māori cultural approaches to privacy could also inform other mechanisms for regulating privacy in New Zealand, including statute law. The NZLC considered Māori perspectives in its review of the Privacy Act 1993, although it ultimately recommended that "privacy issues of particular concern to Māori are probably not matters that can be resolved through amendments to the Act."[292] The intent of the present research is not to challenge that conclusion of the NZLC – that is perhaps an argument for another day – nor to add to the academic literature on what privacy means to Māori. The intent here is to survey what literature does exist to understand the current position with regard to Māori and privacy. Ultimately, what the present research finds is that there has been little empirical research into Māori approaches to privacy and none which provides any link between Māori concepts of privacy and once public facts. However, tikanga Māori does demonstrate a commitment to

---

[288] Khylee Quince "Māori Concepts and Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 29 at 30.
[289] See the decision of Tipping J in *Hosking v Runting*, above n 8.
[290] See generally Christian Whata "Biculturalism in the Law: The 'I', the 'Kua' and the 'Ka'" (2018) 26 Waikato L Rev 24 and Natalie Coates "The Recognition of Tikanga in the Common Law of New Zealand" (2015) NZ L Rev 1.
[291] *Takamore v Clarke* [2012] NZSC 116; [2013] 2 NZLR 733 at [94].
[292] Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2008) at [18.13].

privacy, and a view of privacy that is potentially wider and more nuanced than New Zealand's current law recognises.

B A Tikanga Concept of Privacy

Mead described tikanga as follows:[293]

> Tikanga embodies a set of beliefs and practices associated with procedures to be followed in conducting the affairs of a group or an individual. These procedures are established by precedents through time, are held to be ritually correct, are validated by usually more than one generation and are always subject to what a group or an individual is able to do … .
>
> Tikanga are tools of thought and understanding. They are packages of ideas which help to organise behaviour and provide some predictability in how certain activities are carried out … They help us to differentiate between right and wrong and in this sense have built-in ethical rules that must be observed. Sometimes tikanga help us survive.

Quince describes tikanga as a "collection of values that regulate Māori life and reflect our collective customs, beliefs and values."[294] Helpfully, for a Pākehā author, she notes that: "From a pāhekā view, tikanga is law, custom and religion rolled into one."[295] While tikanga Māori is not a rule book, nor is it backed by formal enforcement mechanisms, Quince notes that it has "normative force".[296]

Quince argues that the aspect of tikanga which best approximates the Pākehā concept of privacy is tapu. Tapu "defines things that are special or restricted, including the human person, information places and objects."[297] Tomas similarly sees the link between tapu and privacy, noting that tapu is "circumscribed by ideas of privacy and exclusiveness."[298] Tomas identifies two ways in which 'tapu' was used by pre-contact Māori. The first she described as 'inherent' tapu, "the divine quality attaching to all things by virtue of their whakapapa

---

[293] Hirini Moko Mead "The Nature of Tikanga" (paper presented to Mai i te Ata Hāpara Conference, Te Wānanga o Raukawa, Ōtaki, 11–13 August 2000) at 3–4 as cited in Law Commission *Māori Custom and Values in New Zealand Law* (NZLC SP9, 2001) at [72]. See Joseph Williams "Lex Aotearoa: An Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law" (2013) 21 Waikato L Rev 1 at 3.
[294] Quince, above n 288, at 32.
[295] At 32. The term 'Pākehā' was used by Joan Metge *New Growth From Old: The Whānau in the Modern World* (Victoria University Press, Wellington, 1995) at 20 to describe "immigrants or descendants of immigrants from Europe (including Great Britain) who have put down roots and feel that they belong in Aotearoa New Zealand."
[296] Quince, above n 288, at 32.
[297] At 33.
[298] Nin Tomas "Key Concepts of Tikanga Māori (Māori Custom Law) and Their Use as Regulators of Human Relationships to Natural Resources in Tai Tokerau, Past and Present" (PhD thesis, University of Auckland, 2006) at 97.

relationship to the atua [gods].”[299] Quince describes whakapapa as the “overarching framework of genealogy – that demonstrates the relatedness between people, the natural world and the gods”.[300] Quince notes that inherent or “intrinsic” tapu relates, in a legal sense “to the inviolability of the human person – to be free from physical assault and interference”.[301] Talking about tapu of the person, Quince notes that:[302]

> Human beings possess intrinsic tapu by virtue of their descent from, and connection to, the atua or gods. Pre-contact Māori society was hierarchical and high-born people were viewed as being more closely related to the atua, and therefore to possess more intrinsic tapu as their kaihau-waiu or birthright. The notion of intrinsic tapu relates to a person’s self-worth, dignity and essential humanity, and it is fully realised upon an individual coming into existence.

For Tomas, inherent tapu “enabled value to be given to privacy of the person” in a society where “group welfare often overrode individual concerns”.[303] These rules protected “personal integrity”.[304]

The second use of tapu was “to describe a condition or state of restrictedness imposed on a person, place or object by someone else.”[305] That someone else needed sufficient mana (power and authority) to be able to declare the person, place or object tapu. Marsden describes this type of tapu as follows:[306]

> A person, place or thing is dedicated to a deity and by that act it is set aside or reserved for the sole use of the deity. The person or object is thus removed from the sphere of the profane and put into the sphere of the sacred. It is untouchable, no longer to be put to common use.

This type of tapu – where things are “off-limits”[307] – is more in line with spatial concepts of privacy and the ideas of separateness or seclusion.

Both Quince and Tomas also discuss the tapu of knowledge. Tapu knowledge could include “whakapapa, as well as tribal history and information relating to wāhi tapu, and resources

---

[299] At 97.
[300] Quince, above n 288, at 32.
[301] At 33.
[302] At 35.
[303] Tomas, above n 298, at 97.
[304] At 97.
[305] At 97.
[306] Māori Marsden “God Man and Universe: A Māori View” in Michael King (ed) *Te Ao Hurihuri: The World Moves On – Aspects of Māoritanga* (Hick Smith & Sons Ltd, Wellington, 1975) 191 at 194–195.
[307] Tomas, above n 298, at 98.

necessary for collective wellbeing for health, housing and subsistence."[308] The knowledge itself, as well as its means of transmission, are considered tapu. Thomas describes this type of tapu as:[309]

> … upholding the secrecy and privacy of knowledge considered important to the group's survival, as well as ensuring that those who held it were worthy recipients.

The complementary principle to tapu is noa. Noa "is the state of being unrestricted, or safe for use."[310] Quince describes the relationship between the two as follows:[311]

> I am wary of tapu – whether permanent or temporary – it serves to warn us to be careful and deliberate in our actions so as not to encroach on other people or territories. By contrast, for me, noa conveys a sense of safety and openness.

The NZLC called the concepts of tapu and noa as "structuring principles of traditional Māori society, much as public and private are in contemporary Western societies."[312] However, the tapu/noa distinction is fundamentally different. This is evidenced by Quince, who notes that "the state of noa conveys the sense of freedom and relaxation that is associated with being in private."[313]

In addition to tapu providing a means of individual or personal privacy, tapu can also operate to provide a sense of collective privacy. Quince notes that tapu places are "connected to the mana of the local people, or tangata whenua," who have a "duty of care and protection – kaitiakitanga – towards those places."[314] Viewing tapu places through a privacy lens, Quince states:[315]

> … the collective group has a territorial status that derives from whakapapa, and this connects them in a sense that is collectively private vis-à-vis others. Members of a local entity may communally share or have access to places, or things are that out of bounds to outsiders.

---

[308] Quince, above n 288, at 37. The Māori Dictionary "Definition of Wahi Tapu" (17 November 2020) The Māori Dictionary <https://maoridictionary.co.nz> defines wāhi tapu as a "sacred place, sacred site - a place subject to long-term ritual restrictions on access or use, e.g. a burial ground, a battle site or a place where tapu objects were placed."
[309] Tomas, above n 298, at 100.
[310] Quince, above n 288, at 33.
[311] At 33.
[312] Law Commission, above n 76, at [5.22].
[313] Quince, above n 288, at 34. See also Law Commission, above n 293, at [151].
[314] Quince, above n 288, at 35.
[315] At 35.

This view of collective privacy is not unknown to western liberal democracies. Westin, in particular, argued for a view of privacy which encompassed (small) group claims to privacy.[316] However, what distinguishes the Māori concept of privacy is not just a focus on the collective but a fundamentally different perspective of the self. Quince notes that the "individual in Māori thought is really only validated with reference to their membership of broader collectives of whānau [family], hapū [sub-tribe] and iwi [tribe]."[317]

Quince argues that this Māori world view has significant implications for traditional privacy concepts like the public/private dichotomy. One such implication is that the collective identity at the heart of the Māori world view means that some public places should be considered as having "collective local privacy".[318] A marae is one such public place.[319] If a marae is viewed as having collective local privacy, the norms associated with its use are different for the different people who use the marae. Quince notes that:[320]

> … the marae is a public place for those who have whakapapa and community links to it, and a private place in relation to all others. Public business is conducted on the marae, but that business is only public to those who have an expectation of access – usually the local people.

Health data are one area where there appears to be increased scholarship on Māori perspectives. When the Privacy Act 1993 was first passed, Te Puni Kōkari (Ministry of Māori Development) hosted a hui [meeting] to discuss the proposed Code of Practice for Health Information.[321] The document that resulted from the hui – *He Taonga te Mātauranga: A Draft Discussion Document – Māori Issues Concerning the Code of Practice for Health Information* – set out a range of matters of concern to Māori in regard to the Code of Practice.[322] The document noted that health information is taonga to Māori (a treasure, or prized possession).[323] The document recognised that personal information belongs to a

---

[316] Westin, above n 143, at 31.
[317] Quince, above n 288, at 42.
[318] At 42–45.
[319] The Māori Dictionary, above n 348, defines "marae" as a "courtyard – the open area in front of the wharenui [meeting house], where formal greetings and discussions take place. Often also used to include the complex of buildings around the marae."
[320] Quince, above n 288, at 44.
[321] *He Taonga te Mātauranga: A Draft Discussion Document–Māori Issues Concerning the Code of Practice for Health Information* (Te Puni Kōkiri, May 1993) at 7.
[322] At 10.
[323] Taonga are protected by Article 2 of Te Tiriti o Waitangi/The Treaty of Waitangi, which states that: "The Queen of England agrees to protect the chiefs, the subtribes and all the people of New Zealand in the unqualified exercise of their chieftainship over their lands, villages and all their treasures." This is an English translation of the Māori version of Te Tiriti o Waitangi. The Waitangi Tribunal "Translation of the te reo Māori text" (19 September 2016) <www. waitangitribunal.govt.nz> views taonga as "all dimensions of a tribal group's estate, material and non-material — heirlooms and wāhi tapu (sacred places), ancestral lore and whakapapa (genealogies)".

person, but that the person is situated within a whānau, hapū and iwi. It further stated that personal information "is looked after and cared for as is whakapapa. Māori therefore still maintain a connection to all information, including that organised into statistics."[324] This broad view of personal information challenges the fundamental basis of the Privacy Act, which applies to information about an identifiable individual and therefore excludes statistical or aggregated information from the definition of 'personal information'. *He Taonga te Mātauranga* also notes that due to the taonga nature of health information, there must be "agreed ways to dispose of the information when the subject dies or the need to hold it has passed."[325]

Recently, in a study on the different perspectives of access to health information between Māori and Pākehā, Menkes et al, noted that Pākehā:[326]

> … tended to define the patient as an autonomous individual in his or her own right, distinct from community, and invoked the priority of society over the individual only under certain circumstances.

In contrast, while the Māori groups also valued autonomy, they described it "with reference to genetic ancestry".[327] Māori participants noted that "individuals and even gametes were consistently described as embedded within whānau and community."[328] These differences resulted in a more cultural-situated view of when information should be disclosed. For Pākehā, health information should be kept confidential unless competence or community safety was an issue. In contrast, Māori:[329]

> … explicitly valued the individual as part of the whānau, and so expected whānau to have access to such information in order to provide care and support. If the whānau were unavailable or unable to provide necessary care or support, information would then flow to more distant elements of hapū and iwi.

The NZLC also noted that the Privacy Act does not easily fit within a tikanga Māori view of privacy. They noted that the Act does not protect against disclosure of information about groups, deceased persons or non-identifiable information. The NZLC recognised that some

---

[324] *He Taonga te Mātauranga*, above n 321, at 10.
[325] At 15.
[326] David B Menkes and others "Perspectives on Access to Personal Health Information in New Zealand/Aotearoa" (2008) 15 Anthropology & Medicine 199 at 205.
[327] At 205.
[328] At 205.
[329] At 208.

Māori considered that, due to a deceased person's place within their whakapapa, that "their privacy might be breached, and by extension, the privacy or his or her whānau, hapū and iwi."[330] Furthermore, Māori information is not necessarily individually owned, so whakapapa information is held by custodians on behalf of the collective – the whānau, hapū or iwi.

A growing area of intersection between Māori and privacy appears to be the issue of data sovereignty. Data sovereignty is "managing information in a way that is consistent with the laws, practices and customs of the nation-state in which it is located."[331] In New Zealand, this translates to Māori data sovereignty, which:[332]

> … recognises that Māori data should be subject to Māori governance and that Māori organisations should be able to access Māori data to support their aspirations.

The conversation on indigenous data sovereignty from a New Zealand perspective stems from a workshop held in Australia in 2015 which brought together representatives of Canada, Australia, New Zealand and the United States to discuss the issue of data sovereignty for indigenous peoples.[333] This workshop was followed in New Zealand by the establishment in 2016 of Te Mana Raraunga – the Māori Data Sovereignty Network. Te Mana Raraunga's stated purpose is to:[334]

> … enable Māori Data Sovereignty and to advance Māori aspirations for collective and individual wellbeing by:
>
> 1. Asserting Māori rights and interests in relation to data
> 2. Ensuring data for and about Māori can be safeguarded and protected
> 3. Requiring the quality and integrity of Māori data and its collection
> 4. Advocating for Māori involvement in the governance of data repositories
> 5. Supporting the development of Māori data infrastructure and security systems
> 6. Supporting the development of sustainable Māori digital businesses and innovations.

---

[330] Law Commission, above n 76, at [5.26]–[5.31].
[331] C Matthew Snipp "What does data sovereignty imply: what does it look like?" in Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Toward an Agenda* (ANU Press, Acton ACT, 2016) 39 at 39.
[332] Māui Hudson and others "He Matapihi ki te Mana Raraunga" – Conceptualising Big Data through a Māori lens in Hēmi Whaanga, Te Taka Keegan & Mark Apperley (eds) *He Whare Hangarau Māori – Language, Culture & Technology* (Te Pua Wānanga ki te Ao/Faculty of Māori and Indigenous Studies, University of Waikato, Hamilton, 2017) 64 at 65.
[333] Tahu Kukutai and John Taylor "Data Sovereignty for Indigenous Peoples: Current Practice and Future Needs" in Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Toward an Agenda* (ANU Press, Acton ACT, 2016) 1 at 1–8.
[334] "Purpose" (17 November 2020) Te Mana Raraunga – the Māori Data Sovereignty Network <www.temanararaunga.maori.nz>.

In its Charter, Te Mana Raraunga asserts that: (1) data are a living taonga and of strategic value to Māori; (2) Māori data are "data produced by Māori or that is about Māori and the environments we have relationships with";[335] and (3) Māori data are subject to the rights articulated in the Te Tiriti o Waitangi/Treaty of Waitangi and the United Nation's Declaration on the Rights of Indigenous Peoples.[336] However, to date it appears that Māori data sovereignty is predominantly focused on the practical uses of data and ensuring that these uses are culturally appropriate and take account of Māori values, rather than the role of the Māori world view in the legal systems which enable or constrain that use.

C Conclusion

While the discussion on tikanga Māori and privacy is brief, some conclusions can be made. First, privacy has a role in tikanga Māori and some of its important concepts, like tapu. There are also similarities in the underlying values, like protection of people, reputation and human dignity.[337] Second, it is clear there are differences between the Pākehā and Māori views of privacy, the most important of which is the collective view of privacy. These differences are evident not only in the concept of collective local privacy applied to places, but also in the view of the individual as part of a collective. Third, it appears that the Māori view of personal information is akin to a life-cycle view of information, with Māori interests remaining at all points along that life-cycle, including when the information is aggregated with other information and when it is deleted or destroyed. Finally, there is a lack of scholarship on the topic of privacy and Māori. There is a risk that this lack of scholarship may hamper tikanga Māori from assuming a greater role within the law of privacy. The present research is not the platform to close this gap, but it does support the need for more research and scholarship in this area, and endeavours to recommend a broad and principled framework for privacy law that provides room for nuanced cultural perspectives to flourish in the future.

V Conclusion

This literature review argues that most of the prior scholarship on the concept of privacy provides room for once public facts. The literature on privacy in public demonstrates that public information should not necessarily be excluded from the application of privacy law. What is required is a recognition that a range of factors influence whether information is

[335] "Charter" Te Mana Raraunga – the Māori Data Sovereignty Network <www.temanararaunga.maori.nz>.
[336] United Nation's Declaration on the Rights of Indigenous Peoples, GA RES 61/295 (2007).
[337] Quince, above n 288, at 29–30.

public or private, including context and expectations, obscurity of information, the extent of exposure and consequences of exposure. Acceptance of this position means that regardless of whether once public facts are viewed as facts that 're-grow' their private nature, or as public facts that remain public, they can still theoretically be protected in appropriate circumstances.[338] While this chapter argues that protection is possible under the banner of privacy, the remainder of this thesis will detail how such protection can be effected in practice. First, however, the thesis discusses why disclosure of once public facts is a loss of privacy that deserves protection in law. Aspects of this discussion were considered in the literature review above; however, the next chapter considers in detail the reasons why once public facts should be protected.

The literature review has also highlighted that tikanga Māori concepts of privacy need to become a greater part of the privacy discussion in New Zealand. Research and scholarship is limited to date; however, what has been considered in this chapter demonstrates that privacy is a valuable concept to Māori, but differences exist in how that concept is understood and pursued. The focused nature of the present research means those differences cannot be pursued here. However, more research is required on Māori perspectives of privacy, so that New Zealand's privacy law can take account of its commitment to the Te Tiriti o Waitangi/Treaty of Waitangi.

[338] See, for example, Stephen Penk "Future Directions and Issues" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 429 at 432 who notes that there is a live issue regarding "whether facts once public may, through the passage of time, become private." This speaks to privacy re-growing; rather than protection for 'public' information.

4 THE BENEFITS OF A ZONE OF PRIVACY FOR ONCE PUBLIC FACTS

I Introduction

The preceding chapter considered some of the common and respected notions of what constitutes privacy, ultimately favouring, at least from a descriptive perspective, a view of privacy that centres on the limited access concept put forward by Gavison. However, as Gavison recognised, a descriptive view of privacy needs to be moulded into a concept which the law can protect.[339] Not all losses of privacy can or should result in a legal response. What must be determined, therefore, is which losses of privacy deserve legal protection. In the context of the present research, the question can be narrowed even further – why do once public facts deserve legal protection?

To answer this question, the research posits that there are core privacy values at the heart of once public facts and failure to protect such facts can put those core values at risk. Furthermore, once public facts can cause genuine harm. It is the link between once public facts and core values, along with the potential for harm, which means once public facts deserve legal protection in appropriate circumstances. To test this hypothesis, the present research proceeds in the following manner. First, the research discusses the core privacy values it argues are at the heart of once public facts. These include the values of liberty, rehabilitation, self-development, dignity and autonomy. Second, the research tests and evaluates the relationship between once public facts and the core values by considering once public facts in an empirical manner using a tool called "anchoring vignettes".[340] The discussion on the anchoring vignettes argues that there is a strong link between once public facts and the core values posited and that, therefore, failure to protect such facts can put those values at risk.

The vignettes also highlight the significant impact of modern technology. Ultimately, the seismic shift from an analogue to a digital world has raised the question whether technology requires a fundamental re-think of the core privacy values. This issue provides the third topic of the chapter, which is a brief overview of the technological challenges to once public facts

[339] Gavison, above n 91, at 440.

[340] James Waldo, Herbert Lin and Lynette I Millett *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washing DC, 2007) at 86, citing the work of Gary King "Enhancing the Validity and Cross-cultural Comparability of Measurement in Survey Research" (2004) 98 American Political Science Review 191.

and whether or not these challenges mean privacy must bend to the technological capability or whether there is room for a normative view of privacy that reflects society and its core values. This research concludes that technological developments are not part of an inevitable tide to which privacy must give. Technology is developed by people, for people and it must reflect the values to which society is committed. The final discussion in the chapter considers the potential harms resulting from the misuse of once public facts, and demonstrates that failure to protect such facts can cause substantial harm.[341]

II Core Values

The core values of privacy that are most at risk from once public facts are liberty, rehabilitation, self-development, dignity and autonomy. At its simplest, liberty is the ability to act free from interference by others.[342] As Mill stated:[343]

> … framing the plan of our life to suit our own character, of doing as we like, subject to such consequences as may follow, without impediment from our fellow creatures, so long as what we do does not harm them, even though they should think our conduct foolish, perverse, or wrong.

For Gavison, privacy promotes this liberty to do as we like by severing "the individual's conduct from knowledge of that conduct by others",[344] thereby "removing the unpleasant consequences of certain actions thus increasing the liberty to perform them".[345] A narrower form of liberty – liberty from state interference – is commonly put forward as a driver of privacy. Whitman argues that privacy in the United States "is the right to freedom from intrusions by the state, especially in one's home."[346] This narrower driver of privacy is most evidenced by the Fourth Amendment of the United States Constitution, which states that the:[347]

---

[341] The focus on core values and harm has been inspired by the work of Anne Cheung "Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd" (2009) 1 JML 191 at 206 who argued that a wider view of privacy was required in the internet era to protect the values of autonomy and dignity, and to prevent harm.
[342] See Helen Winkelmann, Chief Justice of New Zealand "Sir Bruce Slane Memorial Lecture" (Auckland, November 2018). See also David Matheson "A Distributive Reductionism About the Right to Privacy" (2008) 91 The Monist 108 at 195 who stated that privacy is "the right to act free of the influence of illegitimate forces that operate outside our awareness to influence, modify, and condition our behaviour."
[343] John Stuart Mill *On Liberty* (Penguin Books Ltd, London, 1974) at 71.
[344] Gavison, above n 91, at 448.
[345] At 448.
[346] James Q Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) 113 Yale LJ 1151 at 1161.
[347] United States Constitution, amend IV.

> … right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause.

While this narrow view of liberty has little to offer instances where once public facts are at issue – predominantly because once public fact situations involve disclosure of private information rather than intrusion into private matters – Gavison's broader view of liberty is more fruitful.[348]

As noted in the previous chapter, Gavison recognised that privacy can operate as a shield to promote "the liberty of individuals not to disclose some parts of their past, in the interest of rehabilitation".[349] This linkage between privacy and rehabilitation was also discussed by Solove, who argued that privacy should be understood in terms of various disruptions to practices and one such disruption is that disclosure of a criminal past "can interfere with that person's ability to reform herself"[350].

Gavison also saw privacy as having a role in identity development. She stated that:[351]

> Privacy enables individuals to establish a plurality of roles and presentations to the world. This control over "editing" one's self is crucial, for it is through the images of others that human relations are created and maintained.

Solove similarly recognised privacy's role in self-development, arguing that the privacy harm from disclosure "can prevent people from engaging in activities that further their self-development".[352] Westin argued that privacy supported people to "seek self-realization in an open environment."[353]

Another value that is deeply connected to privacy is dignity. In *Brooker v Police*, Thomas J noted that few rights were more basic to human dignity than privacy. He stated:[354]

---

[348] In New Zealand there is a separate privacy tort that deals with intrusion. See below n 1081.
[349] Above n 95.
[350] See discussion, above n 169.
[351] Gavison, above n 91, at 450.
[352] Solove, above n 159, at 532.
[353] Westin, above n 143, at 323.
[354] *Brooker v Police* [2007] NZSC 30, [2007] 3 NZLR 91 at [182].

> It is within a person's sphere of privacy that the person nurtures his or her autonomy and shapes his or her individual identity. The nexus between human dignity and privacy is particularly close.

Winkelmann CJ similarly saw privacy as essential to dignity, and its "related value" autonomy.[355] She noted that privacy supports "true autonomy of the individual and in so doing ensures each human is afforded dignity."[356] She stated that:[357]

> If the individual is unknown and unknowable, then that naturally engenders respect. But where the individual is known and thus predictable, then they are vulnerable to control and manipulation; they are vulnerable to being treated as a mere instrumentality, a means to an end, rather than an end in themselves.

Dignity and respect for personhood were also central to many of the concepts discussed previously. Bloustein argued that making a public spectacle of aspects of another person's private life was an affront to that person's dignity.[358] For Benn, privacy was about respect for personhood, as part of the self-creative enterprise.[359]

To determine if these core privacy values are truly central considerations in situations involving once public facts, the research employs a tool called "anchoring vignettes", which utilises brief privacy scenarios as a way to "collect, articulate, and organize intuitions about privacy in a more precise and empirical fashion".[360] Each vignette sets out a scenario involving disclosure of once public facts and is followed by a discussion about how the disclosure might affect core values and interests.

---

[355] Winkelmann CJ above n 342, at 3. Winkelmann CJ argues that the dignity framework "derives from the German philosophical school, drawing upon the work of Immanuel Kant". Winkelmann CJ argues that "a loss of privacy for one's thoughts and beliefs impinges upon freedom of thought, creativity and freedom of expression. Exposure of thinking to public scrutiny changes that thinking. It may kill its development if it is a thought which is unpopular. It encourages conformity in thought" (at 4). See also Lord Hoffmann in *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457 at [51], who noted that the inclusion of privacy within human rights conventions like the ECHR has identified private information as "something worth protecting as an aspect of human autonomy and dignity."

[356] Winkelmann CJ, above n 342, at 4.

[357] At 4. This link between dignity and autonomy was also highlighted by Thomas J in *Brooker*, above n 354, at [178] who cited Aharon Barak *The Judge in Democracy* (Princeton University Press, Princeton, 2006) at 87, where Barak argues that human dignity "regards a human being as an end, not as a means to achieve the ends of others".

[358] See discussion, above n 80.

[359] Benn, above n 87.

[360] Waldo, Lin and Millett, above n 340, at 86.

A Liberty

1 Liberty to not disclose information in the interest of rehabilitation

(a) Vignette

Twelve years ago, Robb was a senior executive in a company which hired a private investigator to investigate threats made against the company and Robb. The investigator proposed, and Robb agreed, to conduct (illegal) phone tapping. When the phone tapping was discovered, Robb was prosecuted and sentenced to imprisonment for six months. Robb served his sentence, was released and has not committed any other criminal offences. Information about Robb's conviction and sentencing is still widely available online, with the information forming the most prominent results when his name is searched via a search engine.[361]

(b) Discussion

Rehabilitation has repeatedly been viewed as a primary driver for protection of once public fact cases. In *Melvin v Reid* the Court noted:[362]

> One of the major objectives of society as it is now constituted, and of the administration of our penal system, is the rehabilitation of the fallen and the reformation of the criminal. Under these theories of sociology it is our object to lift up and sustain the unfortunate rather than tear him down. Where a person has by his own efforts rehabilitated himself, we, as right-thinking members of society, should permit him to continue in the path of rectitude rather than throw him back into a life of shame or crime.

Similarly, the Judge in *Briscoe* stated:[363]

> One of the premises of the rehabilitative process is that the rehabilitated offender can rejoin that great bulk of the community from which he has been ostracized for his anti-social acts. In return for becoming a "new man", he is allowed to melt into the shadows of obscurity.

---

[361] This fact scenario derives from the English case *NT 1 & NT 2 v Google LLC* [2018] EWHC 799 (QB), [2019] QB 344 and is the fact scenario for the plaintiff NT 2. For a discussion of the case see Chapter 6(IV)(D) and Chapter 7(VI). The names of individuals in these vignettes have been taken from George R R Martin *A Game of Thrones* (Harper Voyager, London, 1996) because in many instances the names of the individuals concerned are not available from the case information.

[362] *Melvin v Reid*, above n 4, at 93.

[363] *Briscoe*, above n 9, at 41.

In Europe many jurisdictions have recognised a privacy concept called the "right to oblivion" (*droit à l'oubli* in France and *dirrito all'oblio* in Italy),[364] which has been described as "a right that allows a criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration".[365] In English jurisprudence, the "right to rehabilitation" has also been held to be a part of privacy law.[366] In *NT 1 & NT 2 v Google LLC* Justice Warby stated that:[367]

> The right to rehabilitation is an aspect of the law of personal privacy. The rights and interests protected include the right to reputation, and the right to respect for family life and private life, including unhindered social interaction with others. Upholding the right also tends to support a public or societal interest in the rehabilitation of offenders.

That privacy is needed to support rehabilitation is reinforced by the existence of 'spent conviction' or 'clean slate' legislation in many western democracies. Spent conviction legislation allows rehabilitated offenders to not disclose information about their past convictions and sentences in certain circumstances. The legislation recognises that without the ability to effectively draw a veil over the past, offenders may not be able to move on from their historical convictions. The issues with being tied to a past conviction are well known. In a recent empirical study of the effect of spent conviction legislation in the United States, the authors noted the consequences of criminal sanction may be "swamped in importance by what comes next: exclusion from employment; obstacles to social integration; and a vast array of collateral legal consequences that often last a lifetime."[368]

In New Zealand, the spent conviction legislation is the Clean Slate Act. In order for a conviction to be classed as spent under the Act, the person must not have had a custodial sentence imposed on him or her and the offence must not be a sexual one involving children, rape or incest.[369] If the person meets the criteria, and once they have completed the rehabilitation period of seven years, they are deemed to have no criminal record for the

---

[364] Paul A Bernal "A Right to Delete?" (2011) 2(2) EJLT at 2. See also David Lindsay "The 'Right to Be Forgotten' in European Data Protection Law" in Norman Witzleb and others (eds) *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, New York, 2014) 290 at 302. Meg Leta Jones, above n 155, at 96 notes that this right to oblivion finds its rationale in privacy as a human right.
[365] Jeffrey Rosen "The Right to Be Forgotten" (2012) 64 Stan L Rev 88 at 88. See also Lindsay, above n 364, at 302 who cites Rosen's definition.
[366] *NT 1 & NT 2,* above n 361, at [166(1)].
[367] At [166(1)].
[368] J J Prescott and Sonja B Starr "Expungement of Criminal Convictions: An Empirical Study" (2020) 133 Harv L Rev 2460 at 2468.
[369] Criminal Records (Clean Slate) Act 2004, s 7 [Clean Slate Act].

purposes of any question asked about their criminal record (for example, as part of an employment process) and have the right to have their criminal record concealed by government departments and law enforcement agencies that have access to the record.[370]

In the United Kingdom, the Rehabilitation of Offenders Act 1974 takes a different approach. The Act uses a graduated system, whereby different sentences become eligible for rehabilitation after different time periods. In England and Wales, for example, a sentence of imprisonment of up to six months becomes rehabilitated after 24 months, imprisonment of between seven and 30 months after 48 months and for custodial sentences between 31 and 48 months, after seven years. A fine requires 12 months to be rehabilitated.[371] Where a custodial sentence of more than 48 months has been imposed, then the Act does not apply at all.[372] In Scotland, the time limits are not as generous, with custodial sentences of between six months and 30 months being rehabilitated after 10 years. Custodial sentences up to six months require seven years, and fines or lesser sentences, five years.[373] For those who are rehabilitated under the Act, they are treated for all purposes in law as someone who has not committed a crime and the person does not have to refer to the spent conviction when asked questions about previous convictions.[374] In Australia, different requirements exist for each state and at a federal level. In some respects, some of these statutes provide less protection for prior convictions than in New Zealand, because the rehabilitation period is routinely 10 years.[375] However, in terms of the coverage of convictions, they are all more lenient because they apply to custodial sentences between no more than six months (New South Wales and Australian Capital Territory)[376] and 30 months (Queensland and the Commonwealth).[377]

While spent conviction legislation reinforces the need to have privacy in order to support the goal of rehabilitation, the reach of such legislation is limited. The freedom to not disclose past convictions only operates when a question about convictions is put to the person or a government official. Publication of the spent conviction which is not connected to the official record is not a criminal offence or civilly actionable.[378] Gollogly argues that spent legislation

[370] Sections 4 and 14.
[371] Rehabilitation of Offenders Act 1974 (UK), s 5(2) (England and Wales). Lesser periods apply for minors.
[372] Section 5(1)(b) (England and Wales).
[373] Section 5(2) (Scotland).
[374] Section 4(1).
[375] See, for example, Crimes Act 1914 (Cth), s 85ZL; Criminal Records Act 1991 (NSW) s 9; Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld) s 3(1); and Spent Convictions Act 2000 (ACT), ss 12–13.
[376] Criminal Records Act 1991 (NSW) s 7 and Spent Convictions Act 2000 (ACT), s 11.
[377] See Crimes Act 1914 (Cth), s 85ZM(2)(b) and Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld) s 3(2).
[378] The offences under the Clean Slate Act are set out in ss 17–18. Section 17 makes it an offence for a person who is an officer, employee, or contractor of a public office, government department, or law enforcement agency, and who has access to criminal records, to knowingly or recklessly not comply with the Act. Section 18

is "premised on an outdated understanding of how people access information."[379] He says that before the advent of the internet, criminal convictions were "practically and partially obscure".[380] Newspapers only detailed convictions that were of interest to the public and then those newspapers passed into archive at local libraries. Information of the conviction would then "fade from memory of all but those closest to the event."[381] Now, however, with search engines and newspapers online, the information is easily available. The information may also have more prominence that it deserves. Gollogly argues that most people do very little that is newsworthy within their lifetime, so that a reported minor criminal conviction will be the prominent search engine result.[382] Considering the limits of spent conviction legislation, it is understandable why people have turned to data protection legislation and the decision in *Google Spain* – and its remedy of delisting or delinking search results – to obtain the privacy they desire.

While there is a clear link between spent convictions and privacy, less clear is whether convictions that have not yet, or never will, become spent may still warrant protection. In *NT 1 & NT 2*, Justice Warby noted that people do not enjoy a reasonable expectation of privacy in "information disclosed in legal proceedings held in public".[383] However, at some point in time this position can change, and that point is when Parliament has determined the conviction spent. The implication of Justice Warby's words is that if the conviction is not spent, there is no expectation of privacy.[384] In contrast, one of New Zealand's few cases to discuss once public facts – *Tucker v News Media Ownership Ltd* – found that having a previous conviction for indecent assault (which had allegedly resulted in imprisonment for nine months) was not a barrier to determining that the publication of that information might be a breach of privacy.[385] While the case was decided before the Clean Slate Act came into effect, Tobin has argued that the decision might still be good law.[386] However, there are limits to Tobin's argument. Tobin argues that where the conviction is for a serious offence not covered by the Clean Slate Act, "it is unlikely that a court will find an expectation of privacy

---

establishes an offence for persons who require an individual to disregard the Act when answering or providing disclosure on criminal records. For the position in the United Kingdom, see Iain Christie and Adam Wolanski "Context and Background" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 3 at 19.

[379] Fraser Gollogly "The Blemish on the Clean Slate Act: Is There a Right to Be Forgotten in New Zealand?" (2019) 25 Auckland U L Rev 129 at 131.

[380] At 131.

[381] At 131.

[382] At 132.

[383] *NT 1 & NT 2*, above n 361, at [166(2)].

[384] At [166(2)].

[385] *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716 (HC). This case is discussed further in Chapter 6(II).

[386] Rosemary Tobin "The Common Law Tort of Invasion of Privacy in New Zealand" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 89 at 104.

in that conviction until some considerable time has passed."[387] Whether a reasonable expectation of privacy will arise is likely to depend upon "all matters surrounding the conviction",[388] as well as the potential consequences of publication.[389]

There is also a question about the impact of repeat offending on expectations of privacy. Repeat offending may militate against any argument for rehabilitation. A person may not appear committed to rehabilitation if they have continued to offend. Furthermore, prior offending may make current offending more relevant and vice versa.[390] However, the relationship of privacy to the core values of liberty and rehabilitation must not be substituted for a simple numbers game. It must always depend on the circumstances in the case. In *Brown v Attorney General*, for example, the plaintiff had a history of sexual offences dating back almost 20 years, however, the Court still found an invasion of privacy when the Police disclosed information about the plaintiff in a manner in which the plaintiff did not consent.[391]

Difficult issues also arise where the person claiming the rehabilitation benefit is not an offender, but a person accused of a crime and acquitted, or not accused of a crime but accused of transgressing moral or ethical standards. While the quote from *Melvin v Reid* above relates to criminals, it must be remembered that the plaintiff in that case was actually acquitted of murder. So it is arguable that the plea to the rehabilitative interest was being more broadly applied – to those accused of a crime and acquitted, or even those accused of transgressing moral codes, since part of the infamy of the case was that Mrs Melvin had been a prostitute. It certainly seems right that, if those who have been convicted of certain offences can have a reasonable expectation of privacy in relation to that offending after a period of time, then those who have been accused but *not* convicted, should similarly have a reasonable expectation of privacy, and possibly after a shorter period of time, because there is no actual rehabilitation to occur and no competing interest of open justice.[392]

---

[387] At 100. However, Tobin notes that where the offending is particularly serious, like murder, it is unlikely that the conviction will ever support a reasonable expectation of privacy.
[388] At 100.
[389] At 100. In *Tucker* the consequences of publication were potentially life threatening.
[390] See *Reekie v Television New Zealand Ltd* 6/7/10, BSA Decision No 2009-111 at [24].
[391] *Brown v Attorney General* [2006] NZAR 552 (DC) at [17]. An interesting issue also arises regarding the impact that registration of a sex offender on a register would have on reasonable expectations of privacy. While the topic of sex offender registers is outside the scope of the current research, the impact on expectations of privacy is likely to depend on the type of regime a country has. In New Zealand, for example, the Child Protection (Child Sex Offender Government Agency Registration) Act 2016 sets up a registration regime, whereas some jurisdictions in the United States operate registration and notification regimes. See Jordan Anderson "Dangerous Neighbours: Risk Control, Community Notification and Sex Offender Release" in J Pratt and J Anderson (eds) *Criminal Justice, Risk and Revolt against Uncertainty* (Palgrave Macmillan, Cham, 2020) 93 at 94.
[392] In New Zealand the interest in open justice finds expression in the Criminal Procedure Act 2011. Section 196 states that court hearings must be open to the public. This requirement reflects that it has "long been the general rule" that civil and criminal hearings must take place in public (see Ursula Cheer *Burrows and Cheer Media Law*

A broader view of the rehabilitative interest was also seen in a decision of the AEPD following the *Google Spain* case. In that decision, the complainant had requested Google remove URLs referring to the complainant's murder trial and acquittal by reason of insanity. The AEPD found in favour of the complainant and required the search results to be delisted. One of the key factors in AEPD's decision was that the medical evidence stated that memory of the events would undermine the complainant's recovery from the paranoid schizophrenia which had been a rationale for his acquittal.[393]

A similar logic to that applied to those who are accused but not convicted of a crime should apply to those accused of something less than a crime. Why should those convicted of a crime be able to put the past behind them, but those not convicted of a crime, but judged in the court of public opinion, not be given the same opportunity? The Article 29 Data Protection Working Group tasked with establishing guidelines for complying with the decision in *Google Spain* recognised the long-term impact of foolish but non-criminal acts on people, and included it as a factor to be considered in any delisting decision. The "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales*' C-131/12" (the Article 29 Data Protection Working Group Guidelines) note that:[394]

> The data might have a disproportionately negative impact on the data subject where a search result relates to a trivial or foolish misdemeanour which is no longer – or may never have been – the subject of public debate and where there is no wider public interest in the availability of the information.

Similarly, Solove has argued for a wider perspective on the rehabilitation interest and recognised the value of such a perspective. He stated that:[395]

---

in New Zealand (7th ed, LexisNexis NZ Limited, Wellington, 2015) at 467). However, open justice is not an absolute. There are common law and statutory exceptions to the principle, which include judges' right to clear the court in limited circumstances and the right to prohibit publication of proceedings in court. One of the more well known exceptions is name suppression. See generally Cheer *Media Law in New Zealand* at [8.4.2].

[393] Artemi Rallo Lombarte "The Origins and Importance of the Right to be Forgotten: The Spanish Experience" (presentation at the University of Oxford, Centre for Socio-Legal Studies, 2012) <http://slideplayer.com/slide/6276508/> at slide 14. See also Lindsay, above n 364, at 300–301.

[394] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/12* (European Commission, 14/EN WP 225, 26 November 2014) at 18. This statement was made regarding criteria 8, entitled: "Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?"

[395] Daniel J Solove "The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure" (2003) 53 Duke L J 967 at 1054.

> Most people have embarrassing moments in their past. Everyone has done things and regretted them later. In childhood, they may have acted with great immaturity, done cruel things to others, or done things to make them ashamed. There is a great value in allowing individuals the opportunity to wipe the slate clean … Society has a tendency to tie people too tightly to the past and to typecast people in particular roles. The human personality is dynamic, yet it is frequently difficult to accept the complete implications of this fact.

While the rehabilitation interest has found much support, not all are convinced by it. Posner argues that the interest: [396]

> … rests on the popular though implausible and, to my knowledge at least, unsubstantiated assumption that people do not evaluate past criminal acts rationally, for only if they irrationally refused to accept evidence of rehabilitation could one argue that society had unfairly denied the former miscreant a fresh start.

He argues that information on past criminal activities is not irrelevant to those entering into social or business relations with the offender. If it were irrelevant, then there would be no harm to the individual concerned in publicising the information. He argues that people want to conceal such information because others "quite sensibly regard a criminal past as negative evidence of the value of cultivating an acquaintance with a person."[397] Posner also takes issue with the societal or social policy behind rehabilitation, noting that "whether there is more or less crime in a system that emphasizes rehabilitation is unclear."[398] He also queries whether concealment is a "'fair' method of rehabilitation, since it places potentially significant costs on those who deal in ignorance with the former criminal." [399] However, there is only a cost on the third parties if it is assumed that rehabilitation does not occur. If a person has truly rehabilitated then there is no cost and the concealment merely eliminates any prejudice that the person dealing with the ex-convict might have.[400]

However, what if the person has not really rehabilitated. Friedman provides an alternative version of the *Melvin v Reid* story, where he argues that the plaintiff won her case based on

---

[396] Posner "The Right of Privacy", above n 160, at 409. Posner further argued that: "To attach adverse significance to past criminal acts without conducting the kind of thorough investigation that would, in a few cases, dispel their significance, is not irrational or malevolent; it is a method of economizing on information costs" (at 415).
[397] At 415–416.
[398] At 415.
[399] At 415.
[400] See Gavison, above n 91, at 454, who argues that Posner's position is "an extremely harsh one".

lies and falsehoods.[401] He argues that at the time of the privacy case she had not rehabilitated and in fact was "still working a a prostitute and a madam … [and that] [d]uring her lifetime she had several husbands, but they had the distressing habit of turning up dead".[402] In light of the potential for persons to bend the truth to suit their purposes, it raises the question of whether it can be justified to dislose once public facts to correct false or misleading information. Harvey would argue "yes" and that concealment is "an attempt to alter the truth".[403] Certainly, if a person is relying on the pursuit of an interest in rehabilitation and second chances, then if that interest is not valid there is an argument for the publication of the additional information to establish the truth of the matter. However, more information will not necessarily lead to the truth of a matter,[404] and what must be avoided is what Cohen calls the "information processing imperative" – the "culturally determined urge to collect more and more information."[405] Cohen argues that this imperatives is:[406]

> …grounded in a view of information gathering as knowledge discovery along a single, inevitable trajectory of forward progress. Within that philosophical framework, the interest in getting and using more complete information is presumptively rational and entitled to deference. The truth-value of "more information" is assumed and elevated to a level beyond ideology…

However, Cohen argues that this adherence to the information processing imperative has not heralded "universal enlightenment",[407] and that "a wealth of historical evidence undercuts the rationalist faith in the inevitable link between information processing and truth."[408] Furthermore, Cohen notes that sometimes information truth seeking has resulted in political repression and even genocide.[409] The key, therefore, is not to assume that more information results in truth or more rational decision making, rather the circumstances and the need for more information need to be carefully interrogated.[410]

Bringing the discussion back to the vignette, and assuming that Robb is based in a jurisdiction where his conviction is spent, then the fact the conviction is widely available via search

---

[401] Lawrence M Friedman *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy* (2007, Standord University Press, California) at 218–219.
[402] At 218.
[403] Harvey, above n 1, at 294.
[404] See also below n 1009.
[405] Cohen *Configuring the Networked Self*, above n 202*,* at 127.
[406] At 118.
[407] At 147.
[408] At 251.
[409] At 251.
[410] At 148.

engine results usurps his ability to move on from information the state has deemed he should be able to move on from. He has a legally protected interest to move on, but practically he cannot. Ultimately, not allowing privacy to protect the previous conviction frustrates Robb's liberty of action to conceal information in the interests of rehabilitation. However, as noted above, if Robb was in a jurisdiction where his conviction is not spent, then the issues are less clear because there is no governmental policy to guide the analysis. In such a situation the analysis needs to return to fundamentals. Here, Robb has served his sentence and demonstrated his commitment to rehabilitation over a considerable period of time. His conviction appears to not be connected to, nor in fact has ever been, a topic of public debate. The custodial sentence was a relatively short one and the nature of the conviction was highly fact-specific, which does not point to any ongoing threat to public safety or welfare. In the vignette the information is readily available because technology enables such a situation, not because the information itself has any objective value. In light of these factors, and of Robb's clear wish to keep the information private, it may be that this vignette is one where the rehabilitative interest is sufficient to uphold a privacy interest in the information.

2 Liberty to not disclose the past in the interest of self-development

(a) Vignette

Twenty years ago, Catelyn was a member of a high profile youth organisation well known for being involved in anti-social activities. As a member of that organisation she once spoke about the organisation on a television show. Since that time, she has no longer associated with the organisation, does not proactively tell people she once belong to that organisation and has led a life outside of the public gaze. However, when Catelyn's name is searched on search engines the top results show her public association with the organisation.[411]

(b) Discussion

The ability to move on and develop one's identity is closely related to the interest in rehabilitation. Both are about an individual's freedom to grow and develop free from the past – whether it is a previous legal or moral transgression or a former identity, belief or

[411] This vignette is based off a Japanese case discussed in Yuriko Haga "Right to Be Forgotten: A New Privacy Right in the Era of Internet" in Marcelo Corrales, Mark Fenwick, Nikolaus Forgó (eds) *New Technology, Big Data and the Law* (Springer Nature Singapore Pte Ltd, Singapore, 2017) 97 at 112. While this example might seem unlikely, Jon Ronson *So You've Been Publicly Shamed* (Pan MacMillan, London, 2015) at 211 discusses one situation of a person who wanted to obtain digital redemption. This person stated: "When I was seventeen I was a Nazi … Now I'm in my forties I'm trying to move on but the Internet still thinks that I am a Nazi."

affiliation. Privacy's role in the development of self has a long history. Benn talked about the "self-creative enterprise" which would be frustrated by activities invasive of privacy.[412] Westin noted that: "Part of the value of privacy … was that it limited the circulation of recorded judgments about individuals, leaving them free to seek self-realization in an open environment."[413] Murchison defined privacy as an aspect of self-development and argued that self-development "crucially depends on articulating a narrative of one's past."[414] This narrative process is dialogic, "a conversational engagement with one's past and with others."[415] However, this conversation with others can be disrupted, by media disclosure of highly personal information. Such disclosure:[416]

> … disrupts the freedom of close interaction between the complainant and the group by shocking their relationships with previously unknown facts, or pre-empting the complainant's ability to bring the facts into the conversation on his or her own terms, in his or her own time. If growth takes place within a zone of dialogue and facilitating ties, the risks of injuring relationships within that zone can be substantial.

The ECtHR has also given clear statements about the link between privacy and identity. In *Von Hannover v Germany (No 2)*, the Court reiterated that the right to privacy set out in the ECHR "is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings."[417]

It has also been recognised that the development of self is not a static exercise and that, as they grow and mature, people can substantially alter their beliefs and world views. Cohen notes that:[418]

> We do not experiment only with beliefs and associations, but also with every other conceivable type of taste and behaviour that expresses and defines self. The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo.

---

[412] Benn, above n 87.
[413] Westin, above n 143, at 323.
[414] Brian C Murchison "Revisiting the American Action for Public Disclosure of Private Facts" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 32 at 51.
[415] At 51.
[416] At 52–53.
[417] *Von Hannover v Germany (No. 2)* (2012) 55 EHRR 15 at [95].
[418] Julie E Cohen "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan L Rev 1373 at 1425.

Andrade argues that personal identity should be "perceived as a matter of choices, a process of continuous negotiation (with ourselves and others), never pre-determined and univocal, but one that can be constantly revised and changed."[419] Solove notes that: "Selfhood is a process of growth and development, not a fixed state of being"[420] and that it "grows throughout an entire lifetime."[421]

However, a person's ability to construct, de-construct and re-construct their identity may be constrained by the digital traces they have left behind. Mayer-Schönberger considered the issue of these digital traces – which he called digital dossiers or digital collages – and noted that:[422]

> Some worry that digital collages resemble momentary comprehensive snapshots of us frozen in time, like a photograph, but accessible to the world. Actually, digital collages are much more disquieting than that. They are not like one, but hundreds, perhaps thousands of snapshots taken over our lifetime superimposed over each other, but without the perspective of time. How can we grasp a sense of a person that way? How can we hope to understand how a person has evolved over the years, adjusting his values, adapting to his (changing) environment? How can we pretend to know who that person is today, and how his values, his thinking, his character have evolved, when all that we are shown is a timeless collage of personal facts thrown together?

For some, this "timeless collage of personal facts" is just that – facts – and they should be accessible to all.[423] As noted above, Posner argues that a person who actively tries to hide their past is engaging in false or misleading representations.[424] Posner asks: "Why should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims?"[425] Gavison, however, rejects Posner's argument where the information at issue is irrelevant.[426] Gavison argues that, while ideally people should be able to disregard irrelevant information and prejudices, it is "clear, however, that we cannot. Given this fact, it may be best to let one's ignorance mitigate one's prejudice."[427] Strandburg agrees. She argues that non-disclosure of information can be a way

---

[419] Noberto Nuno Gomes de Andrade "Oblivion: The Right to be Different from Oneself Reproposing the Right to be Forgotten" (2012) 13 IDP 122 at 129.
[420] Solove, above n 395, at 1037.
[421] At 1053.
[422] Viktor Mayer-Schönberger *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, Princeton, 2009) at 124.
[423] Harvey, above n 1, at 293–294.
[424] Posner, above n 92, at 233–234.
[425] Posner "The Right of Privacy", above n 160, at 400.
[426] Gavison, above n 91, at 454.
[427] At 454.

to deal with the fact that humans do not always act rationally. She points to the fact that human decision-makers:[428]

> … tend to weigh conspicuous, memorable, or vivid evidence disproportionately. Such information is distracting and, particularly when of low relevance to the decision at hand, likely to interfere with rational decision-making.

So people change and others are not always able to understand that change and rationally ignore an outdated version of that person. The key, therefore, is to identify when old and outdated information is being used prejudicially or irrationally, and causing genuine harm. Identifying such information is important, because it is also true that sometimes people do want to deceive or hide information that is embarrassing or negative. A possible solution might be found by considering the relationship between privacy and reputation.

The European tradition of privacy has a strong link with personal reputation. To this end, Whitman argued:[429]

> The core continental privacy rights are *rights to one's image, name, and reputation*, and what Germans call the *right to informational self-determination* – the right to control the sorts of information disclosed about oneself. These are closely linked forms of the same basic right: They are all rights to control your public image – rights to guarantee that people see you the way you want to be seen. They are, as it were, rights to be shielded against unwanted public exposure – to be spared embarrassment or humiliation … .

However, the traditional mechanism for protecting reputation is the law of defamation. According to the law, defamation: [430]

> … imposes liability for statements adverse to the plaintiff's reputation unless the statements made are shown to be true, or are made on an occasion of privilege, or are opinion which is honestly held.

A number of New Zealand courts have considered the relationship between privacy and defamation. In *Hosking v Runting*, Gault J had no issue with the disclosure tort addressing

---

[428] Katherine Strandburg "Privacy, Rationality, and Temptation: A Theory of Willpower Norms" (2005) 57 Rutgers L Rev 1235 at 1272.
[429] Whitman, above n 346, at 1161.
[430] *Lange v Atkinson* [1997] 2 NZLR 22 (HC) at 33.

reputational issues, while acknowledging that the key concern with privacy is hurt and distress rather than reputation. His Honour stated:[431]

> To the extent that a remedy in damages is awarded arising from publicity given to private information it may be seen as constituting a remedy for damage to reputation which hitherto has been the almost exclusive realm of defamation. But the true focus is on hurt and distress rather than standing in the eyes of others.

In *Driver v Radio New Zealand Ltd*, the Court also recognised that there could be "many situations in which the privacy tort will protect reputational interests in an indirect way."[432] However, the reputational impact should only be a secondary concern, with the focus on the "hurt and distress" of the invasion of privacy, irrespective of others' reactions to the information.[433] Despite this statement, the Judge did note that the fact that the disclosure of information might cause reputational harm could be considered as part of the determination of whether there is a reasonable expectation of privacy.[434]

In the English case of *Yeo v Times Newspapers Limited*, Justice Warby noted that while a defamatory publication can breach a right to a private life, not all do. In determining whether the right to privacy is engaged, his Honour focused on whether or not a publication "undermines 'personal integrity' as distinct from merely harming reputation."[435] To support his comments he cited *Karakó v Hungary* as follows:[436]

> For the Court, personal integrity rights falling within the ambit of [privacy] are unrelated to the external evaluation of the individual, whereas in matters of reputation, that evaluation is decisive: one may lose the esteem of society – perhaps rightly so – but not one's integrity, which remains inalienable.

Justice Warby continued by noting that a defamatory publication can "undermine personal integrity if it has 'an inevitable direct effect' on private life which is quite severe, such as ostracisation from a section of society."[437] While this decision relies heavily on the peculiarities of English privacy law (which is discussed in Chapter 6 below), it is a useful way to consider the boundary between matters that directly relate to privacy and reputation. A

---

[431] *Hosking*, above n 8, at [138].
[432] *Driver v Radio New Zealand Ltd* [2020] NZHC 2903 at [112].
[433] At [112].
[434] At [113].
[435] *Yeo v Times Newspapers Limited* [2015] EWHC 3375 (QB), [2015] All ER (D) 230 (Nov) at [145].
[436] *Karakó v Hungary* (App no 39311/05), 28 April 2009 at [23].
[437] *Yeo*, above n 435, at [145].

matter would engage the privacy interest when the publication impacts personal integrity, but where the information is related to external evaluations of a person, it would not. Returning to the vignette, if the old information is hampering Catelyn from forming relationships, or from building or conducting her life (for example, stopping her from finding employment), then her scenario engages appropriate privacy intuitions. The outcome may be different if the vignette was one where Catelyn simply did not want the information resurfacing because it reduced others esteem of her, but could point to no real harm or impact on her private life.

Another difficult aspect of the vignette scenario is the impact of Catelyn's own actions in exposing her past to the public by consenting to appear on a television show.[438] A person's ability to waive their right to privacy – including by consenting to publication of private information – has been recognised as far back as Warren and Brandeis, who noted that the right to privacy ceases where the subject published the material or consented to its publication.[439] A similar approach was picked up in *Melvin v Reid*, where the Court noted that the right to privacy "does not exist where the person has published the matter complained of, or consented thereto."[440]

However, the ability for consent to be a true defence to a privacy claim is relatively narrow, especially when the claim involves media defendants. Warby argues that media publication will usually be to a wide audience and "the defendant will have to show that the claimant consented to the extent of the publication."[441] For the purposes of the vignette, the question is whether this narrow approach applies temporally, that is, does a defendant have to show that a claimant consented to publication *for all time*? A 'yes' answer requires a nuanced view of consent, which is not unknown, however. In a New Zealand privacy decision of the Broadcasting Standards Authority (BSA), the Authority noted that there were limits to informed consent, and even if a person gave informed consent to the filming of a reality television show on their business premises, it "stretches credulity" to believe that the consent included the repetitive use of the footage for many years afterwards.[442] In the English case of *Weller v Associated Newspapers Ltd*, the Court of Appeal held that where a celebrity had spoken to the media about his family on a previous occasion, doing so did not deprive his

[438] Haga, above n 411, at 112. In the case on which the vignette is based, the defendant argued that "since the plaintiff openly disclosed the information about himself, he had consented to waive his privacy right."
[439] Warren and Brandeis, above n 71, at 218.
[440] *Melvin v Reid*, above n 4, at 93.
[441] Mark Warby "Justifications and Defences" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 529 at [12.07], [12.15]–[12.16].
[442] *FS v Television New Zealand Ltd* 19/12/2012, BSA Decision No 2012-036 at [27]. See Chapter 6(II) for a discussion of the Broadcasting Standards Authority [BSA] and its privacy framework.

family of protection against an unconsented publication.[443] A nuanced approach to consent also reflects the broader European approach, which, Whitman argues, "has resisted the notion that one can definitively alienate one's dignity."[444] This approach is shown in the 19th century French case of Alexandre Dumas. Dumas, his lover and her mother had posed for several "more or less salacious photographs",[445] and thereafter sold the rights in the photos to the photographer, who registered his copyright in the photos and then went on to widely publish them. Dumas sued. Despite Dumas having sold his rights to the photos, thereby losing effective control of the images, the Paris Court sided with Dumas, recognising a right to privacy which qualified the property right in the photos.[446] The Court held: [447]

> Even if a person had tacitly consented to the publication of embarrassing photos, that person must retain the right to withdraw his consent. "The very publication" of such photos could put such a person on notice "that he had forgotten to take care for his dignity, and remind him that *private life must be walled off* in the interest of individuals, and often in the interest of good morals as well."

Utilising a nuanced view of consent in the vignette would require moving past some vague sense that Catelyn waived all rights to privacy and considering the specific facts, including the actual publication which occurred.[448] Clearly when Catelyn consented to appear on the television show she could not have expected the rise of the internet and search engines.[449] She probably expected five minutes of public attention and then a quick fade into obscurity. It would be hard to argue that she unequivocally consented to publication for all eternity. If Catelyn's consent cannot be used to waive her right to privacy, then the vignette returns to the issues of self-development discussed above and a need for Catelyn to be able to prove an impact on her private life.

---

[443] *Weller v Associated Newspapers Ltd* [2015] EWCA Civ 1176, [2016] 1 WLR 1541.
[444] Whitman, above n 346, at 1193.
[445] At 1175.
[446] At 1176. The Court held that the photographer had to sell the photographs back to Dumas.
[447] At 1176.
[448] For a discussion of the role of consent see Ursula Cheer and Stephen Todd "Invasion of Privacy" in Stephen Todd and others (eds) *Todd on Torts* (8th ed, Thomson Reuters, Wellington, 2019) 977 at [17.4.06(1)].
[449] See Leta Jones, above n 155, at 84.

B Dignity

1 Vignette

A newspaper published an article on the front page which included a photo of a police statement made 40 years ago accusing Sam of homosexual activity when such activity was illegal. The statement was contained in court records which were open to the public, however, Sam himself was not the subject of a criminal investigation, nor had the statement been used in any court proceedings. Sam had never publicly discussed the accusation or his sexuality.[450]

2 Discussion

Respect for human dignity has been a powerful driver of privacy. The dignity at issue in the vignette is reminiscent of the wrong referred to by Bloustein when discussing *Melvin v Reid*, *Sidis* and other similar cases. Bloustein stated:[451]

> What the plaintiffs in these cases complain of is not that the public has been led to adopt a certain attitude or opinion concerning them – whether true or false, hostile or friendly – but rather that some aspect of their life has been held up to public scrutiny at all …, it is as if 100,000 people were suddenly peering in, as through a window, on one's private life.

Information about a person's sexuality is inherently private information, which makes the impact on dignity more severe. The idea that some information is innately or inherently private has formed common rhetoric in the development of legal protection for privacy. The oft quoted statement of Gleeson CJ in *Australian Broadcasting Commission v Lenah Game Meats Pt Ltd* serves to demonstrate: "Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private".[452] The idea that some information is "obviously" private was picked up in *Campbell v MGN Ltd*, where Lord Hope noted that if "the information is *obviously* private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected."[453]

---

[450] This scenario derives from *Uranga v Federated Publs Inc* 67 P 3d 29 (Idaho 2003).
[451] Bloustein "Human Dignity", above n 80, at 979.
[452] *Australian Broadcasting Corporation v Lenah Game Meats Ltd* (2001) 208 CLR 199 at [41].
[453] *Campbell*, above n 355, at [96] (emphasis added).

However, Moreham argues that relying on a category of obviously or inherently private information is fraught:[454]

> To say that one will have a reasonable expectation of privacy if the information in question is "obviously" private begs the question of what is private in the first place and seems to depend on the judge's own value judgements to an unacceptable degree. One need only refer to the fact that the Court of Appeal and two members of the House in *Campbell* held that what Lord Hope regarded as "obviously private" was not in fact private at all, to show how unpredictable such a yardstick could be.

Despite this valid challenge, through a range of cases, the English courts have established categories of information which is generally held to be private. Moreham calls this "usually-private" information and it includes matters related to the physical body, sexual activity, personal relationships, trauma, grief and strong emotion.[455] Statutory privacy and data protections have also recognised that there is a sub-category of personal information which deserves greater protection. Article 9 of the GDPR provides additional protections for processing "special categories of personal data", which includes information on sexual orientation, ethnic origin, political opinions and religious beliefts, and genetic and biometric data.[456] In Australia, similar information is called "sensitive information" and also subject to more stringent protection requirements under the Privacy Act 1998.[457]

It is not only the nature of the information which impacts on dignity in this vignette, it is also Sam's lack of choice as to whether his innately personal information was exposed to widespread publicity on the frontpage of a newspaper. As noted by Winkelmann CJ above, allowing people true autonomy affords them the respect each human deserves. Cheung describes the affront to dignity caused by a lack of autonomy as follows:[458]

> Privacy in a world of social beings is about control over information about ourselves … Losing it implies that we become 'merely permeable', a bundle of details, distortedly known, presumptuously categorised, instantly retrievable and transferable to numerous unspecified parties at all times. We lose our ability to decide when, to what degree, to whom, and under what circumstances we would like to relate to the outside world.

[454] Moreham, above n 102, at 646.
[455] At 659.
[456] GDPR, art 9.
[457] See Privacy Act 1988 (Cth), s 6(1), s 13B and Schedule 1, cl 3.1 and 3.2.
[458] Cheung, above n 341, at 210.

Even Gavison recognised that most people keep information hidden from others and that what is important is "not whether we should edit, but how and by whom the editing should be done."[459] That whom, Gavison is clear, is the individual concerned.

In the vignette, the newspaper has usurped Sam's ability to control when, to what degree, and with whom he discusses his sexuality. The vignette also starkly demonstrates the difference between information that is normatively public as distinct from descriptively public. Before publication in the newspaper, the statement was in hard-copy only, buried in the archives of a local courthouse, so it was descriptively private due to being relatively inaccessible. However, as part of the public record it was normatively public. By publishing that information on the front page of the newspaper, the information is now both normatively and descriptively public.

A more sensitive approach from both the perspectives of dignity and autonomy is seen in a determination made by Google following the decision in *Google Spain*. In the aftermath of *Google Spain*, Google established a process for requesting delinking or de-indexing search results.[460] By May 2022, the process has resulted in over 1,200,000 requests relating to over 4,900,000 URLs, with 49 per cent of requests being accepted and actioned.[461] One such request was made by a victim of alleged sexual assault, committed over 50 years previously. Fifteen years previously, the alleged victim agreed to a settlement with the Catholic Church regarding the alleged assaults and had spoken publicly about the matter at the time. However, media reports of the settlement were still widely available via Google search results.[462] Google accepted the person's request and delisted the URLs complained of. While there is no record of the reasoning behind Google's decision, the nature of the information at issue – extremely private and sensitive information about alleged sexual assaults – surely contributed to the decision, along with the length of time since the media articles. These factors must have weighed heavily to overcome the consensual component of the publicity.

While Google was more sensitive to dignity, the United States court was not in the decision on which the vignette is based. That Court dismissed the plaintiff's case due to the fact that

---

[459] Gavison, above n 91, at 454.
[460] "Requests to delist content under European privacy law" Google Transparency Report <https://transparencyreport.google.com/eu-privacy/overview?hl=en>.
[461] Google Transparency Report (last accessed 4 May 2022).
[462] In 2015, the BBC published a list of links that Google had 'delinked'. This list is available at http://www.bbc.co.uk/blogs/internet/entries/f4b01ccf-9128-45d8-8cac-23c1cf3455c1. The BBC has continued to publish lists which can be found though the following link: http://www.bbc.co.uk/blogs/internet/entries/6443f2c6-7f15-4968-a715-ea8af3f54917. This thesis has decided not to cite the link to the original article in deference to the wishes of the subject and Google's decision to delink it in its search results.

the plaintiff had been caught up in a newsworthy event 40 years ago and the right to freedom of expression does not provide "less protection to historians than to those reporting current events."[463]

The balance between protecting privacy and preserving history is a delicate one. It can be argued that deleting or obscuring information in the name of privacy amounts to a loss or re-writing of history. In some areas, the balance between history and privacy has already been struck. The rules under clean slate legislation allow for the historical offence to remain part of the official record but restricts how this information is used.[464] Where information is in a digital format, is easily searched and not subject to clear rules, difficulties arise. Some argue that "we owe the entire Internet to our descendants" and are greatly concerned about any loss or degradation of internet information.[465] However, degradation and decay of internet information does occur.[466] Furthermore, other legal rules require amendment to online archives.[467] Accordingly, history does not automatically trump competing interests. In any situation what is required is a careful consideration of the competing interests.

Guidance on how to balance history and privacy can be obtained from relevant cases. In *Hurbain v Belgium* the ECtHR had to determine whether privacy required the amendment of online news archives.[468] The Belgium Court had held that the RTBF required a newspaper to anonymise an online version of a 1994 article concerning a fatal road accident because the accident had resulted in a drink driving conviction, which was now spent.[469] On appeal, the ECtHR upheld the decision of the Belgium Court, despite recognising the importance of digital media archives and the potential for a chilling effect on freedom of expression. In particular, the Court was concerned to ensure that:[470]

> … the electronic archiving of an article relating to the offence committed should not create for the person concerned a kind of "virtual criminal record" … This is all the more so when, as in the present case, the person has served his sentence and has been rehabilitated.

---

[463] *Uranga*, above n 450, at 35.
[464] See the discussion above at Chapter 4(II)(A)(1).
[465] Leta Jones, above n 155, at 11.
[466] See below n 502.
[467] Hugh Tomlinson QC "Case Law, Belgium: *Olivier G v Le Soir*. 'Right to be forgotten' requires anonymisation of online newspaper archive" (19 July 2016) Inforrm Blog <https://inforrm.org>. The authors refer to defamation rules requiring amendments to online news archives.
[468] *Hurbain v Belgium* [2021] ECHR 544 (Grand Chamber). This case is only available in French and therefore the author has not been able to review the case itself and has relied on the case commentary of Hugh Tomlinson QC and Aidan Wills "Case Law, Strasbourg: *Hurbain v Belgium*, Order to anonymise newspaper archive did not violate Article 10" (7 July 2021) Inforrm Blog <https://inforrm.org>.
[469] See Tomlinson and Wills, above n 468.
[470] *Hurbain*, above n 468, at [109].

The Court also recognised the specific impact of digital archives versus paper archives and that the scope of the former "is much greater and the consequences for the private life of the named persons all the more serious especially in light of the role of search engines."[471]

The decision in *Hurbain* provides an example of how history can be retained while still preserving a person's privacy. Furthermore, it reiterates that history is not easily lost. To obtain anonymisation the applicant faces "substantial hurdles."[472] For example, the outcome is unlikely to be allowed "in the case of a public figure or someone involved in an event of historical significance … [or] where there has been more widespread primary media reporting."[473]

Leta Jones also points to "library ethics" as an example of how to weigh the importance of history and the dignity of persons caught up in that history. She notes that the Society of American Archivists has a Code of Ethics which states that archivists must: [474]

> …establish procedures and policies to protect the interests of the donors, individuals, groups and institutions whose public and private lives and activities are recorded in their holdings. As appropriate, archivists place access restrictions on collections to ensure privacy and confidentiality are maintained, particularly, for individuals and groups who have no voice or role in collections' creation, retention, or public use.

In New Zealand, the Archive and Records Association of New Zealand (ARANZ) has established a code of ethics which states that:[475]

> Members will at all times adhere to accepted principles of privacy, commercial sensitivity and national security. By this members must not abuse, allow unauthorised disclosure, or use, of any information acquired by them during the course of their professional work or research.

These rules from the profession of archivists demonstrate that privacy and history can and must be balanced.

---

[471] At [116].
[472] See Tomlinson and Wills, above n 469.
[473] Tomlinson and Wills, above n 469, who noted that: "The Court attached considerable weight to the fact that the nature of the measure imposed had ensured the integrity of the original article, because only the digital archives version would have to be anonymised. Anyone interested in the Article could still request access to it, even in digital form."
[474] Leta Jones, above n 155, at 112.
[475] "ARANZ Code of Ethics" (25 August 2006) ARANZ <https://www.aranz.org.nz>.

Most of the vignettes discussed in this chapter derive from the nature of modern technology – from the ubiquitous role of the internet and search engines to the pervasive drive to digitise all information and have it available. A central issue, therefore, is whether technology means that, despite a zone of privacy protection for once public facts engaging core values, it is futile (or worse, dishonest) to try and carve out a zone of protection for important interests, like privacy and the privacy interest in once public facts. Harvey argues that digital information technologies present "fundamental challenges to our assumptions about the law and may well revolutionise some established legal institutions and doctrines", including privacy law.[476] However, allowing technology to drive our underlying expectations of privacy could be viewed as an exercise in unchallenged technological inevitabilism[477] – an acceptance that modern technology is uncontrollable and society must bend its values to technology, rather than technology adapting to uphold those values. To understand these arguments better, it is critical to understand the technology that underpins these arguments.

III Technological Environment

It has been said that we are living in a time where:[478]

> … the generation of wealth, the exercise of power, and the creation of cultural codes … [depends] on the technological capacity of societies and individuals, with information technologies as the core of this capacity.

One of the central components of the information technology revolution is the exponential increase in storage capacity. Moore's law holds that circuit complexity will double roughly every 18 months.[479] As the storage capacity of integrated circuitry increases, the cost of storage has decreased substantially. Mayer-Schönberger notes that for "fifty years the cost of storage had roughly been cut in half every two years, while storage density increased 50-million fold".[480] The ability to store an ever increasing amount of information allows that information to be transmitted through time. Mayer-Schönberger argues that the

[476] Harvey, above n 1, at 18. See generally at 307 for a discussion of technology's impact on privacy.
[477] Shoshana Zuboff *The Age of Surveillance Capitalism* (Profile Books Ltd, London, 2019) at 225 argues that the technological inevitability rhetoric "presents the new apparatus of ubiquity as the product of technological forces that operate beyond human agency and the choices of communities".
[478] Martin Hilbert and Priscila López "The World's Technological Capacity to Store, Communicate, and Compute" (2011) 332 Science 60 at 60.
[479] Mayer-Schönberger, above n 422, at 64. Mayer-Schönberger further notes that Moore's law has held true over the last 40 years and is likely to hold for the foreseeable future (at 72).
[480] At 63.

"overabundance" of storage capacity has made forgetting expensive.[481] People no longer want to spend time deciding whether to keep or delete information, when it is so easy and cheap to retain it all.

The exponential growth in storage capacity means that people and organisations are now able to hold as much information as they wish (and are legally able) to collect. In response, there has been a proliferation in the collection of information. In 2007, Solove noted that "data is gathered about us at every turn."[482] In 2022, this statement is truer than ever before. Solove referred to 24-hour surveillance, cell-phone cameras and websites which allow people to post information and pictures – "obsessively documenting every aspect of their lives."[483] Today, data gathering happens from these tools and so many more. For example, people carry smart phones wherever they go, they wear watches that monitor every waking or sleeping moment of their lives,[484] and many ordinary devices used daily gather data about us. Zuboff notes that: "Real-world activity is continuously rendered from phones, cars, streets, homes, shops, bodies, trees, buildings, airports, and cities back to the digital realm".[485]

Assisting this move to pervasive collection of information and overabundant and cheap storage has been the digital revolution. The existence of information in a digital format means that all types of information can be stored, transmitted and reproduced in more efficient and standardised ways. Mayer-Schönberger contrasts the difference between sharing analogue versions of information like newspapers and movies – which involves actual newspapers or film being shipped around a city via trucks – with sharing digital versions of these documents via the internet.[486] Digitisation has also allowed information to be more dynamic – it can be easily updated, modified, copied and manipulated.[487] To this end, Harvey states:[488]

> Part of the dynamic of the digital environment is that information is copied when it is transmitted to a user's computer. Thus there is the potential for information to be other than static. If I receive a digital copy I can make another copy of it, or alternatively, alter it and communicate the new version. Reliance upon the print medium has been based upon the fact that every copy of a particular edition is identical until the next edition. In the digital paradigm authors and publishers con control content from minute to minute.

[481] At 68.
[482] Solove, above n 244, at 163.
[483] At 164.
[484] For an example of such a watch see the Whoop fitness tracker. For information on this product see https://www.whoop.com.
[485] Zuboff, above n 477, at 202.
[486] See Mayer-Schönberger, above n 422, at 57–61.
[487] Harvey, above n 1, at 29.
[488] At 29.

The digital revolution, along with the revolution in communication which is discussed next, has ultimately resulted in a democratisation of the dissemination of information and the rise of social media.[489] The communication revolution has predominantly, for the purposes of the present research, come in the form of the internet and the rise of networked computers.[490] Closely linked to the rise of the internet has been the World Wide Web (WWW), which is an information system that rests on the architecture of the internet. The internet and the WWW have turned information dissemination from the preserve of the media, to anyone with an internet connection and a webpage. The internet and the WWW have also enabled a flow of information towards the individual – the information is now instantly and easily accessible wherever the user is located. The user no longer has to go to the information.[491]

The rise of social media and SNS, on the backbone of the internet and the WWW, have elevated the participatory aspects of digital technology to a new level, allowing even more generation of, and interaction with, information. Powerful social media tools like Facebook, YouTube, Instagram, LinkedIn, and TikTok are now ubiquitous and provide opportunities for dissemination, engagement, collaboration and commerce that were unthinkable 20 years ago. All these tools, as well as the architecture of the WWW itself, have also become a rich source of data collection. Zuboff calls this data "behavioral surplus" – data on users' behaviours and preferences that is not used to provide the services of the platforms to customers.[492] A classic example of this behavioural surplus is the information generated from the 'Like' button on Facebook.[493] This behavioural surplus has been developed into what Zuboff calls "prediction products", which not only provide a detailed profile of people but can also influence their future behaviour.[494]

---

[489] See Harvey, above n 1, at 30, for a discussion of the democratisation of information, and 246–254, for a discussion of social media.
[490] See Shane Greenstein *How the Internet Became Commercial* (Princeton, Princeton University Press, 2015) 22–30 for a discussion about the development of the internet. Greenstein notes that while the United States military funded many key inventions for the internet, so did other government departments and private industry. See also Mayer-Schönberger, above n 422, at 59, who notes that the internet started out as a way to share processing power.
[491] Harvey, above n 1, at 35–36.
[492] Zuboff, above n 477, at 74–75.
[493] At 457.
[494] At 8 and 96–97. In *Google Spain*, above n 5, at [37], the Court of Justice of the European Union noted that processing of data conducted by a search engine like Google as the result of a search on an individual's name, allowed internet users to "obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him."

The technological environment of pervasive collection of data and almost limitless storage capacity appears to have resulted in a climate of information permanence or persistence. This permanence can be a blessing. Mayer-Schönberger notes that information persistence can support the fallible human memory, it can make companies more efficient, assisting them to create better products, and it can ensure information is available for future generations, so that past mistakes are not repeated.[495] However, information persistence can also be a curse. Mayer-Schönberger argues that there is value in forgetting. He says that forgetting plays a "central role in human decision-making … [allowing] us to act in time, cognizant of, but not shackled by, past events".[496] He says that "forgetting is not an annoying flaw but a life-saving advantage. As we forget, we regain the freedom to generalize, conceptualize, and most importantly to act."[497] However, the move to remembering has resulted in a loss of control and power for individuals. People can no longer rely on practical obscurity of information to protect their information. In the past, if a person lost control of personal information, they had a traditional (albeit, costly) exit strategy of moving to a new town to start afresh.[498] This strategy is no longer viable. Mayer-Schönberger states that:[499]

> Combine accessibility and durability, and humans can no longer successfully run away from their past. That past follows them, ready to be tapped into by anyone with an internet connection.

Those who know the most about others can also influence behaviour and exert control over actions in ways that were unthinkable even a few years ago. This influence might be as innocuous as recommending books to customers based on past purchases, or it could be more harmful. Zuboff gives the example of vehicle monitoring systems which would link a person's contractual obligations to pay a car loan to the car's computer systems, so that if a person falls behind in their loan repayments, the car is disabled.[500]

However, not all information is permanent. Harvey talks about format obsolescence, driven by the fact that digital information is incoherent and accessing it requires an intermediary, like hardware or software or both. When new versions of software are released that do not support

---

[495] Mayer-Schönberger, above n 422, at 10.
[496] At 12.
[497] At 118.
[498] At 99.
[499] At 103. See also Helen Fay Nissenbaum *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books, California, 2010) at 40 who recognised that "obscurity cannot be achieved through relocation … The grapevine is thorough, scientific, and precise: records of whom we are and what we have done follow us around and even sometimes precede us."
[500] Zuboff, above n 477, at 213.

older versions, then data becomes locked in – the data exists but is inaccessible.[501] Leta-Jones argues that "digital resources are less stable than their analog counterparts were, resulting in the corruption of the integrity and authenticity of the resource."[502] She points to a "laundry list" of reasons for this instability.[503] This list includes:[504]

> … media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures.

For Leta-Jones, the real issue is not that all information is permanent, rather that "*some* information lasts *longer* than the information subject, and probably society, deems appropriate."[505]

With an understanding of the characteristics of modern technology, the question becomes whether or not these characteristics have struck a fatal blow to the privacy interests at stake with once public facts. In some areas that answer is no. In the area of dignity and autonomy it is obvious that modern technology has *amplified* the impacts. The vignette scenario of Sam demonstrates that. However, the framing of modern technology has undoubtedly challenged other interests.

One of the core benefits of protecting once public facts is supporting a person's liberty to not disclosure their past, in the interests of rehabilitation or development of self. However, information persistence, cheap storage, the ease with which information is accessible, its global reach, and disregard for the passage of time all threaten this interest. However, it could be argued that the overwhelmingly participatory nature of technology, which has equipped people with a multitude of tools to provide the world with information about themselves and their identity, arguably makes legal controls redundant. If a Google search result is returning pejorative headlines, then simply drown those headlines out with positive ones – tweet, comment and post more, so that the negative headlines eventually move down the search result list. However, these self-help remedies simply accept the current framing of technology, without engaging with the central issue of whether the underlying interests are worth protecting and, if so, asking why the technology has been designed in a way that frustrates those interests.

---

[501] Harvey, above n 1, at 33–35.
[502] Leta-Jones, above n 152, at 105.
[503] At 105.
[504] At 105.
[505] At 110.

The question, therefore, is whether society values rehabilitation and development of self. One way to try and answer this question is to consider empirical data. If the decision in *Google Spain* is viewed as a way to protect the rehabilitation interest – and it certainly has been used this way, for example in *NT 1 & NT 2*[506] – then the empirical data related to that decision is instructive. In June 2014, a YouGov survey in the United States found that 55 per cent of respondents would support (either 'a little' (22 per cent) or 'strongly' (33 per cent)) the introduction of legislation "enabling people to request old or irrelevant information being removed from browser searches".[507] Interestingly, only 14 per cent opposed the legislation either 'strongly' or 'a little', but 31 per cent were 'unsure'. In September 2014, a Software Advice poll of 500 United States adults found that 61 per cent of respondents believed that some version of the RTBF was necessary.[508] In March 2015, a survey by Benenson Strategy Group and SKDKnickerbocker found that 88 per cent of United States voters supported (52 per cent who 'strongly' supported and 36 per cent who 'somewhat' supported) a law that would allow them to request search engines to remove certain personal information that appeared in search results.[509] In the European Union, a 2011 survey found that 75 per cent supported a RTBF.[510]

In New Zealand, there have been no surveys on the RTBF. However, when the Privacy Act 2020 was on its journey through Parliament, the Justice Select Committee received approximately 30 submissions on the RTBF and a majority of those were in support of its inclusion in the revised Act.[511] From a policy perspective, the prevalence of spent conviction legislation around the world demonstrates a broad societal commitment to rehabilitation. Furthermore, rehabilitation supported by spent conviction legislation appears to work. The recent empirical study on expungement in Michigan noted above found that those who obtain expungements tend to do very well – within a year they experience a wage increase of, on average, more than 20 per cent. The authors note that this wage increase is "mostly driven by

---

[506] See generally *NT 1 & NT 2,* above n 361, at [161]–[169].
[507] YouGov (2014) *Right to be Forgotten Omnibus Survey*. For information on the headline results and the full results see Jake Gammon "Americans would support 'right to be forgotten'" (3 June 2014) YouGov <https://today.yougov.com>.
[508] Software Advice (2014) *US Attitudes Toward the 'Right to Be Forgotten' Industry View* Survey. For a discussion of the survey results see Daniel Humphries "US Attitudes Toward the 'Right to Be Forgotten' Industry View" (5 September 2014) Software Advice <www.softwareadvice.com>.
[509] See Mario Trujillo "Public Wants 'Right to Be Forgotten' Online" (19 March 2015) The Hill <https://thehill.com>. The link to the actual survey results discussed in the article does not work. This survey, along with the YouGov and Software Advice surveys, are discussed by Zuboff, above n 477, at 61.
[510] European Commission (2011) *Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union* at 2.
[511] Kylie Jackson-Cox "A 21st Century Right? An Analysis of the Extent to which New Zealand's Privacy Act 1993 Provides a Right to Be Forgotten" (2019) 28 NZULR 561 at 570.

unemployed people finding work and minimally employed people finding steadier or higher-paying work."[512]

There are, therefore, empirical and policy reasons to argue that rehabilitation is valued by society. Does the same hold true for development of self and autonomy? A 2015 survey in the United States by Pew Research Centre found that 93 per cent of respondents said that "being in control of *who* can get info about you" was 'somewhat' or 'very' important (with 74 per cent saying it is 'very' important) and 90 per cent said that "controlling *what* information is collected about them is important" (with 65 per cent saying it was 'very' important).[513] However, while control of information was important, few (nine per cent) felt as if they had a lot of control over the information that was collected about them in daily life (38 per cent feel they had 'some' control). The greater percentage, and half the respondents, felt they had none or no control at all.[514] In New Zealand, a 2017 survey found that only 20 per cent of people 'somewhat' (15 per cent) or 'strongly' agreed (five per cent) with the statement: "I feel I can control my privacy online", with 50 per cent disagreeing and 28 per cent being undecided or neutral.[515]

It is difficult to find data on the linkage between privacy and identity development. However, there is data regarding the online actions users take to curate or manage their image. The 2015 Pew Research Centre survey discussed above found that 29 per cent of respondents had deleted or edited a previous post and 11 per cent had asked someone to remove something that was posted about them online.[516] The percentages were higher when age was factored in, with younger adults (18-29) more likely to have deleted or edited a previous post (36 per cent) or asked someone to remove something posted online (15 per cent).[517] A 2014 survey gave some insight into the type of information that people wanted removed (or corrected), with the most common type being photos or videos (65 per cent), followed by comments or blog postings (39 per cent), and other information, including financial statements or court records (13 per cent).[518] It appears, therefore, that people are concerned about the level of control they have over their information and that some people care about their online image and want to be able to manage it.

---

[512] Prescott and Starr, above n 368, at 2461 and 2467.
[513] Mary Madden and Lee Rainie Pew Research Centre (2015) *Americans' Attitudes About Privacy, Security and Surveillance* at 1 and 17.
[514] At 8.
[515] Antonio Diaz Andrade and others *World Internet Project: The Internet in New Zealand 2017* (New Zealand Work Research Institute, Auckland, 2018).
[516] Madden and Rainie, above n 513, at 33–34.
[517] At 33–34.
[518] Pew Research Centre (2014) *Public Perceptions of Privacy and Security in the Post-Snowden Era* at 43.

This brief summary of empirical data demonstrates that rehabilitation, autonomy, and to a lesser degree, self-development, are interests that society appears to value. However, despite this, it appears that these interests have sometimes been forgotten in the rush to develop new information technology. Zuboff argues that this development of technology has often proceeded on the basis that it is inevitable and "incontestable".[519] However, the inevitability of information technology and its impact does not need to be accepted. Cohen argues that the design decisions of social software reflect the circumstances in which they arose and the values of their designers.[520] Zuboff agrees. She argues that despite the rhetoric from technology companies, the architecture created by these companies is not inevitable, rather it was made by humans and they can control it, but have chosen not to.[521] Boyd has also argued that technology has been framed by its developers, based on their values and preferences and not those of the users. Boyd argues that, having framed technology this way, there is then an expectation that users will adapt to the technology, even if it requires operating in a way that is not usual or familiar. Boyd argues that "we've built technology that does not take into consideration the subtle nuances of the identity faceting with which people are already accustomed."[522]

These arguments against technological inevitability are useful. They provide hope that the design of technology can be reframed if there is the appropriate will (or legal imperative) to do so, to that the technology protects, rather than puts at risk, the core privacy values which society deems important.

IV Harm

The harm of ongoing association with a historical criminal conviction results from the stigma that exists in a criminal conviction.[523] Solove argued that those with stigma are not treated equally, and the stigma can spread to family members, for example, when children are stigmatised by a parent's criminal past.[524] As noted above, the stigma can hamper employment opportunities and result in social exclusion. At times, however, the harm from a

[519] See Zuboff, above n 477, at 222–225.
[520] Cohen, above n 191, at 265. Danah Boyd "Autistic Social Software" (speech given at Supernova Conference, 24 June 2004) 35 at 35 also argues that developers have framed "technological use rather than [built] technology based on users' practices and needs."
[521] Cohen, above n 191, at 226. See also Cohen, above n 190, at 1914.
[522] Boyd, above n 520, at 37.
[523] This stigma was legislatively recognised in New Zealand by the Criminal Records (Expungement of Convictions for Historical Homosexual Offences) Act 2018, s 3.
[524] Solove, above n 395, at 1041.

past criminal act moves from the social to the medical. In *Tucker*, the evidence that the plaintiff was likely to suffer severe emotional distress that could hamper a life-saving operation weighed heavily with the Judge.[525] In the Spanish case based on the decision in *Google Spain*, which was discussed above, the AEPD was influenced by the fact that medical evidence claimed that memory of the complainant's act would undermine the complainant's recovery from a severe mental illness.[526]

Even when the harm does not threaten life or health it can be considerably detrimental. Cheung refers to "internet persecution", the persecution that can follow from a person's unwitting exposure as a transgressor of a moral code.[527] Solove discusses the "dog poop girl", who failed to pick up the droppings when her dog pooped on the underground.[528] The incident went viral and the girl had to drop out of university. Mayer-Schönberger tells the story of the "drunken pirate", a prospective young teacher who was denied her teaching certificate because she posted a photo on her MySpace page of her drinking from a plastic cup while wearing a pirate's hat, and tagged it with the line "drunken pirate".[529] Ronson tells the story of Lindsey Stone, who in 2012 found herself the subject of significant internet trolling as the result of a picture posted on Facebook of her performing an inappropriate gesture at the Arlington National Cemetery in the United States. As a result, Ms Stone "fell into a depression, became an insomniac, and barely left home for a year."[530]

While the harms in these scenarios involve the immediate aftermath, Cheung notes that the long-term effects "may be worse than criminal sanctions".[531] She states that:[532]

> Unlike gossip, the images captured and disseminated are not fleeting or localised. They follow the lives of the individuals, grow old with them and are remembered, retrievable and available to all. The freedom and the right to start a new life may be greatly hindered. For instance, it is known that employers in the US search and look at internet profiles of prospective employees. Friedman argues that tying someone to the debris of the past goes against the societal belief in giving second chances to people to start over again and to begin a new life.

[525] *Tucker*, above n 385 at 724.
[526] Artemi Rallo Lombarte, above n 393.
[527] Cheung, above n 341, at 195–198.
[528] Solove, above n 244, at 1–2.
[529] Mayer-Schönberger, above n 422, at 1–2. The women, Stacy Snyder, unsuccessfully sued the university at which she was studying for her teaching degree.
[530] Ronson, above n 411, at 202 and 197–202.
[531] Cheung, above n 341, at 214.
[532] At 214.

Returning to Lindsey Stone's ill-conceived gesture at the Arlington National Cemetery in 2012, the photo is still readily available via a Google search of her name, with it being the first photo shown on the search results page. Furthermore, one of the top links on the search results page is to a change.org petition from 2012 to: "Fire Lindsey Stone for her disrespect of our nation while on company time."[533]

The long term impact of internet persecution was at the heart of the recent New Zealand Court of Appeal decision in *X v R*. The case was a name suppression application following the defendant's discharge without conviction on two assault charges. The case had received considerable publicity due to the fact that the charges arose from behaviour at a New Zealand Labour Party youth camp in 2018.[534] The High Court (despite rejecting the application) recognised that media coverage of the matter could have "deep and long-lasting" consequences.[535] On appeal, the Court of Appeal noted that "the effects of internet shaming will last for longer — potentially for the remainder of the young person's life."[536] In particular, the Court of Appeal noted the toxic nature of social media, calling its coverage "pernicious, judgemental, exponential, indelible, and often ill-informed".[537] The Court argued that, contrary to mainstream media coverage, there was no reasonable expectation that social media coverage would be fair or accurate and no "realistic way of controlling its content or its spread."[538] As a result, there was an extraordinary hardship for those caught up in it. The Court also referred to the recent phenomenon of the cancel culture, which it held to be an example of the weaponisation of social media "against those deemed to have transgressed the norms of any online group (or mob)".[539] As a result, the Court overturned the finding of the high court and upheld the name suppression application.

While some have lauded the Court's recognition in *X v R* of the effects of social media,[540] Harvey argues that the Court's characterisation of social media was narrow and ignored its complex nature.[541] Harvey takes issue, for example, with the Court's conclusion that internet

---

[533] The change.org petition is available at https://www.change.org/p/lindsey-stone-fire-lindsey-stone-for-her-disrespect-of-our-nation-while-on-company-time. The google.co.nz search was conducted on 1 March 2020.
[534] *X v R* [2020] NZCA 387 at [1]. The extent of the publicity is evident from a simple search engine search on the topic. The matter even embroiled the Prime Minister at the time who was forced to ensure an investigation into the matter was conducted. See "PM investigating reports of sexual assault at Labour event" (12 March 2018) RNZ <www.rnz.co.nz>.
[535] At [68].
[536] At [53].
[537] At [51].
[538] At [49].
[539] At [51].
[540] Alison Mau "Final act of Labour youth camp case could be a gamechanger" (6 September 2020) Stuff <www.stuff.co.nz>.
[541] David Harvey "Extreme Hardship and Social Media" (10 September 2020) The IT Countrey Justice <https://theitcountreyjustice.wordpress.com>.

persecution results in young people being forced off social media and thereby being excluded from social and economic opportunities. Harvey argues that contrary to this analysis, social media comprises a vast range of platforms and that persons who are persecuted on one platform can simply move to a new, more friendly, platform.[542] However, while moving platforms might be an option for SNSs, it does not apply to search engines, which access information across numerous platforms, nor does it stop the cancel culture effects, which can greatly hamper a person's future opportunities.[543]

The long-term harms of digital persistence can equally apply to the victims of an incident, as well as the perpetrators. In the vignette, Sam was the victim of an alleged sexual assault; however, 15 years after the apparent resolution of his claim against the Catholic Church, relevant information was still readily available on the WWW. Victims can suffer genuine harm and distress at having a constant reminder of such a traumatic event. Allen notes that: "Trauma often needs to recede into near oblivion."[544] Solove also refers to the harm a person can feel from being judged, or the fear of being judged, following the disclosure of personal information. He argues that the:[545]

> … person may constantly wonder whether particular people know about it [the personal information disclosed] and how the information might change people's perceptions. This can create a significant sense of unease … It can interfere with one's life in a profound way. Even if people are judged more favourably than they might fear, they still must live wondering what others really think of them.

The harm, therefore, from once public facts can be severe and long-lasting. While not everyone will experience such harm, for those that do, the harm is real and significant, and it adds weight to arguments that once public facts deserve legal protection in appropriate circumstances.

---

[542] Harvey, above n 541.
[543] See, for example, Brooks Barnes "Disney Fires 'Guardians of the Galaxy' Director Over Offensive Tweets" The New York Times (online ed, New York, 20 July 2018).
[544] Anita Allen "Dredging up the Past: Lifelogging, Memory, and Surveillance" (2008) 75 U Chi L Rev 47 at 64.
[545] Solove, above n 395, at 1045–1046. A similar harm was pleaded by the plaintiff in the New Zealand case of *Hammond v Credit Union Baywide* [2015] NZHRRT 6 at [54], where the plaintiff said that she suffered "anxiety wondering whether the prospective employer was aware of the NZCU Baywide's warning against employing her." While this case did not involve once public facts and involved particularly malicious behaviour on the part of the defendant, it does demonstrate the harm that can come from the fear of being judged based on disclosure of personal information.

V Conclusion

The discussion in this chapter has demonstrated that there are core privacy values at the heart of once public facts. Once public facts can genuinely affect a person's liberty of action, their ability to rehabilitate and continually grow and change, their sense of dignity and self-worth, and their ability to exercise autonomy and control over important information about their lives. Moreover, the publication of historical information can cause significant harm. Publication can blight a life – cause a person to be judged on the basis of out-dated and irrelevant information, hamper job opportunities and relationship-building, and install fear that they are being judged. At the extreme end, it can be life-threatening. These factors demonstrate that in the appropriate circumstances, once public facts deserve legal protection.

The existence of modern information technology does not negate this conclusion. Modern information technology might have made information considerably more accessible, with a much longer life-span, and it might have made trolling and cancelling easier, but technological capability has not necessarily made these activities morally right. It is for society to determine what rights and interests it deems important, not for the developers in Silicon Valley or other places to make those decisions. This chapter has demonstrated that society recognises and protects the core privacy values at the heart of once public facts and the frame of technology does not necessarily have to usurp these commitments. It does not mean that there are not hard questions and boundaries that need to be navigated. There are, and they need to be tackled head-on. However, for now, what is needed is an appreciation of the need and the benefits to be derived from recognising a zone of privacy for once public facts. Understanding these factors is critical for understanding the 'how' that is discussed in the following chapters.

The remainder of this thesis is dedicated to detailing how privacy law can provide a zone of protection for once public facts. It does so by considering the existing legal mechanisms – both statutory and common law – for protecting private information, and asking if those mechanisms can and should protect once public facts. A natural consequence of addressing this question is that gaps and areas for future development are identified. These gaps and areas and then fashioned in Chapter 9 into a package of amendments to enable appropriate protection for once public facts.

5 21st CENTURY RIGHT: TO WHAT EXTENT DOES NEW ZEALAND'S PRIVACY ACT 2020 PROVIDE A RIGHT TO BE FORGOTTEN?

I Introduction

The RTBF has become an important tool for the protection of once public facts.[546] Two of the vignettes discussed above used (or tried to use) the version of the RTBF seen in *Google Spain* to protect a person's interest in rehabilitation, self-development and dignity. The decision in *Google Spain* has been successfully used in cases in England, Germany and The Netherlands.[547] A version of the RTBF has also been legislatively established by art 17 of the GDPR – the right to erasure. In his submission to the Justice Select Committee on the Privacy Bill 2018, New Zealand's Privacy Commissioner advocated for a RTBF to be introduced into the Bill. Such a right was needed, he argued, because the provisions of the Privacy Act 1993 did not do enough to protect individuals from the potential harms caused by the information society.[548] However, the Privacy Act 2020 does not include a RTBF. As a result, New Zealanders who have their dignity, liberty, autonomy or right to be rehabilitated threatened by the publication of once public facts must rely on the existing provisions in the Privacy Act 2020 to obtain erasure of personal information. If the provisions of the Act do not provide effective means to request erasure, then these fundamental interests and concerns are not adequately protected at law, and there is an arguable case for amendment to rectify the gap.

This chapter investigates the extent to which the provisions of the Privacy Act 2020 can be used to provide a remedy akin to the RTBF seen in *Google Spain* and the GDPR.[549] First, the nature and value of the RTBF is explored, including the challenges in articulating the right and how it can operate as a buffer against the pervasive accumulation of vast amounts of data

---

[546] This chapter utilises parts of the following published work: Kylie Jackson-Cox "A 21st Century Right? An Analysis of the Extent to which New Zealand's Privacy Act 1993 Provides a Right to Be Forgotten" 561. The updates have been made to ensure the content of the published work is consistent with the remainder of the thesis and to take into account the changes brought about by the passage into law of the Privacy Act 2020.

[547] See *NT 1 & NT 2*, above n 361. See also Ben Knight "Germany's top court upholds murderer's right to be forgotten" DW.com 27 Nov 2019 and Daniel Boffey "Dutch surgeon wins landmark 'right to be forgotten' case" The Guardian (online ed, 21 January 2019).

[548] Privacy Commissioner "Submission on the Privacy Bill to the Justice Committee 2018" at [7.1]–[7.5]. The Privacy Bill's reference is Privacy Bill 2018 (34-2).

[549] The GDPR has been chosen as a benchmark for the RTBF out of the international comparator jurisdictions considered in this thesis – the United States, England (and the European Union), Canada and Australia – because it is the only data protection statute that includes a RTBF. It is noted that the rules under the GDPR have become English law via the Data Protection At 2018 (UK).

and support the core values of liberty, autonomy and dignity discussed above. Second, the provisions of the Privacy Act are explored and their adequacy tested by benchmarking the provisions against both the outcome in *Google Spain* and the erasure rules in the GDPR. The research determines that against these benchmarks the provisions in the Privacy Act are deficient. A *Google Spain* case under the Privacy Act would have a different and more difficult road. When compared to the erasure rules in the GDPR, the Act provides erasure grounds considerably narrower in scope. Essentially, for once public facts to gain protection under the Privacy Act they would have to satisfy an inaccuracy test that many could not satisfy. Furthermore, organisations (including search engines) only have to take reasonable steps to erase personal information. This qualification has the potential to provide a useful 'out' for organisations who are disinclined to erase valuable data. Third, as a result of the benchmarking exercise, the chapter identifies those aspects of the Privacy Act that must be addressed if New Zealand wants an effective tool to protect once public facts. While the overall contention of the chapter, and the previous one, is that an erasure is necessary in order to protect a zone of privacy for once public facts, the outline of such a tool is not provided until Chapter 9.

II The Right to be Forgotten

A What is the Right to be Forgotten?

The RTBF has been traced to the European legal concept of the 'right to oblivion', which was discussed above in relation to the right to rehabilitation.[550] The 'RTBF', however, gained prominence due to two developments in the European Union – its proposal to reform the data protection rules (which resulted in the GDPR)[551] and the decision in *Google Spain*. From the beginning, the European Union's proposal to reform its data protection legislation included a RTBF. The right was deemed necessary to enhance individual control over data and was defined as "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[552] For Bernal, this vision of the RTBF is different from the right to oblivion mentioned above. He states that: "It deals with deletion of data that is no longer needed, rather than anything as dramatic as erasing of past events or

[550] See discussion, above n 364.
[551] See above n 16.
[552] 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* (COM (2010) 609, 4 November 2010) at 8. The discussion on the RTBF is in para 2.1.3 entitled "Enhancing control over one's own data" at 7–8.

preventing any kind of speech."[553] The linkage of the RTBF with a right to delete, however, made it through the law reform process so that now, in the GDPR at least, the two concepts are linked.[554]

The second development, the decision in *Google Spain*, has commonly been described as establishing a RTBF.[555] However, in reality this is not true. The remedy in *Google Spain* is more about obscurity than forgetting[556] and has been called a qualified "right to be de-indexed" or "a qualified right not to figure in a public index of search results".[557] The obscurity in *Google Spain*, therefore, is similar to the practical obscurity concept which found favour in *US Department of Justice v Reporters Committee for Freedom of the Press*.[558] The CJEU in *Google Spain* recognised that search engines have a central role in establishing detailed profiles of individuals, which "without the search engine, could not have been interconnected or could have been only with great difficulty".[559] However, by forcing search engines to remove links, the decision in *Google Spain* ensures that profiles are a little less detailed and certain information is a bit harder to find.

While the European Union has been an important influence on the RTBF, it is not the only, nor the first, jurisdiction to grapple with the issue.[560] Before both *Google Spain* and the GDPR, Argentinian courts addressed legal claims against search engines for search results.[561] While some have put these Argentinian cases under the banner of the RTBF,[562] others have disagreed, arguing that these decisions not only found in favour of the search engines, but also

---

[553] Bernal, above n 364, at 2.
[554] The title of art 17 is "The Right to Erasure (right to be forgotten)". See European Data Protection Supervisor [EDPS] *Annex to Opinion 3/2015: Comparative table of GDPR Texts with EDPS Recommendations* (9 October 2015) at 96 for an overview of the different titles proposed for art 17 during the legislative process.
[555] See Lee A Bygrave "A Right to be Forgotten" (2015) 58 Communications of the ACM 35 at 35. See also Lawrence Siry "Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to be Forgotten" (2014) 103 Ky L J 311 at 322 and Andres Guadamuz "Developing a Right to be Forgotten" in Tatiana-Eleni Synodinou and others (eds) *EU Internet Law: Regulation and Enforcement* (Springer International Publishing AG, Switzerland, 2017) 59 at 67.
[556] See Selen Uncular "The Right to Removal in the Time of Post-Google Spain: Myth or Reality under General Data Protection Regulation?" (2019) 33(3) IRLCT at 3. Uncular points to the fact that *Google Spain* did not require the original publication to be removed and it did not prohibit searches involving other search terms, to conclude that the decision merely invents "a right to removal or right to obscurity at the most rather than a right to erasure let alone a right to be forgotten".
[557] Bygrave, above n 555, at 35. See also Guadamuz, above n 555, at 65.
[558] See discussion, above n 187.
[559] *Google Spain*, above n 5, at [80].
[560] W Gregory Voss and Céline Castets-Renard "Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms" (2016) 14 Colo Tech L J 281 at 324–333.
[561] The most prominent of the cases is Juzgado de Primera Instancia [1a Inst] [Court of First Instance], 29/7/2009, "Da Cunha Virginia c/ Yahoo de Argentina s/ Daños y Perjuicios," (Resulta, I, para 3) (Arg) <www.diariojudicial.com/documentos/adjuntos/DJArchadjunto17173.pdf>. See Edward L Carter "Argentina's Right to Be Forgotten" (2013) 27 Emory Int'l L Rev 23 for a discussion of Argentina's RTBF.
[562] Rosen, above n 365, at 88.

turned on unique aspects of Argentinian intellectual property law that protect against the commercial use of photographs of people without consent.[563] What these differences of opinion highlight is that the use of the phrase 'RTBF' can be misleading.[564] In response, some argue that the RTBF is actually a bundle of rights. Voss and Castets-Renard argue that the phrase represents five separate rights: (1) the right to rehabilitation/right to oblivion of the judicial past, which can be seen in the *droit à l'oubli* and *dirrito all'oblio*; (2) the right to erasure/deletion (as established by data protection legislation), which can be seen in the GDPR; (3) the right to delist or delink, which is evident in the decision in *Google Spain*; (4) a "right to obscurity", which is a lesser form of erasure than the other RTBF because information is not deleted, only made harder to find;[565] and (5) a "right to digital oblivion of data collected by information society services", which applies only to such services (for example, browsers, SNS and search engines) and is more than a right to delist or a right to erasure because it does not depend on proving that the data are "irrelevant, out-of-date, or illegal".[566] Koops similarly saw the RTBF as a cluster of rights encompassing: the "deletion of old or irrelevant data";[567] a clean slate; and an extra-legal interest in self-development which allows a person a "sense of liberty of expressing yourself freely in the here and now without fear that this might be used against you in the future."[568] Conceptualised like this, Koops sees particular value in the RTBF as a clean slate, arguing that existing protections in this space, like spent conviction legislation, could be broadened "to more areas in which people are particularly vulnerable to being unduly confronted with detrimental information about their past."[569]

The present research agrees that viewing the RTBF as a bundle of rights is the most appropriate approach. Accordingly, when discussing the RTBF, there must be clarity about the specific concept being discussed. This chapter is primarily interested in three of the rights in Voss and Castets-Renard's taxonomy – the right to delist or delink in *Google Spain*, the right to erasure established by data protection legislation and the right to digital oblivion.[570]

---

[563] See art 31 of the Argentine Intellectual Property Law No. 11.723 Sept. 30, 1933, B.O. (Arg.) (last amended Oct. 14, 1998). For more information see Carter, above n 520, at 38.
[564] Voss and Castets-Renard, above n 560, at 288.
[565] At 334–335.
[566] At 336. See also the discussion at 334–337.
[567] Koops "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right to be Forgotten' in the Big Data Practice" (2011) 8 SCRIPTed 229 at 233.
[568] At 233.
[569] At 255. Koops notes that clean slate protections may need to be broadened to "labour law, consumer law, and administrative and preventative criminal justice."
[570] Voss and Castets-Renard, above n 560, at 335–336. The authors argue that digital oblivion is seen in GDPR, art 17(f) which relates to erasure for minors and information society services. This right operates when information society services collect data from a child where consent is the lawful basis for the collection of the data. The right to erasure does not otherwise depend on the data now being irrelevant, out of date or illegal. A version might also be seen in a right to erasure which extends to personal information which is no longer

These versions of the RTBF are discussed next. The focus on these versions does not mean, however, that the present research ignores the other versions of the RTBF, rather that they are addressed by different discussions. The right to rehabilitation/oblivion of the judicial past, for example, was discussed in Chapter 4.

B Google Spain

As noted in Chapter 1, the privacy concern raised by the plaintiff was that when his name was searched via the Google search engine the predominant results related to historical home-foreclosure notices. Mr Gonzáles asked both Google and the newspaper that published the notices to remove the information. When they refused, he took his claim to the AEPD. The AEPD ordered Google to remove the links to the foreclosure notices.[571] Google appealed the AEPD's decision to the CJEU. The CJEU, however, agreed with Mr Gonzáles, basing its decision on arts 12(b) and 14(a) Directive 95/46/EC.

Article 12(b) of Directive 95/46/EC provided data subjects with the ability to obtain erasure of data where processing did not comply with the Directive.[572] The CJEU held that Mr Gonzáles could obtain the erasure requested because Google's processing of his data did not comply with arts 6(1)(c)–(e) or 7(f) of the Directive. Articles 6(1)(c)–(e) required personal data to be, amongst other things: adequate, relevant and not excessive in relation to the purpose of its use; accurate and up-to-date; and kept in a form which permits identification of data subjects for no longer than is necessary. The CJEU held that the search results were incompatible with these provisions because the:[573]

> … information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine … .

Article 7(f), which the CJEU held was the lawful basis on which Google processed Mr Gonzáles' data, allowed controllers to process data for their legitimate interests, except where those interests were overridden by the fundamental rights of the data subject.[574] To determine

necessary for the purposes for which it was collected (although this obligation applies to all organisations not just those providing 'information society services'). See s 22 Privacy Act 2020, s 22, principle 9.
[571] See discussion, above n 17.
[572] Directive 95/46/EC, art 12(b) states that member states will grant every data subject the right to obtain from the controller "the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."
[573] *Google Spain*, above n 5, at [94].
[574] At [73].

if Google had complied with art 7(f), the Court conducted a balancing exercise between the interests of Google and Mr Gonzáles. Ultimately, the CJEU found that the processing of data carried out by search engines did significantly affect the fundamental rights of data subjects as set out in arts 7 and 8 of the Charter of Fundamental Rights of the European Union.[575] Furthermore, as a general rule (and in the case in question) the rights of the individual override the economic interests of search engines.[576] Google therefore had no lawful basis to process the personal data of Mr Gonzáles.

The Court's determination regarding art 7(f) also provided the basis for the finding under art 14(a) of the Directive. Article 14(a) provided data subjects with the right to object to the processing of data when processing is conducted, *inter alia*, on the basis set out in art 7(f). If an objection was found to be justified, the processing by the controller could no longer involve that data.[577] Since Google's interests were overridden by those of Mr Gonzáles, the objection to the processing was justified and Google could no longer display the search results complained of.[578]

C The General Data Protection Regulation

The GDPR came into force on 25 May 2018. Article 17 sets out the "Right to erasure ('right to be forgotten')", with the grounds for erasure set out in ss (1), as follows:[579]

> The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

[575] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 7 secures respect for "private and family life, home and communications" and art 8 protects personal data, granting a data subject a right of protection of personal data, and rights to access and rectification of such data.
[576] *Google Spain*, above n 5, at [74]. The Court noted that factors like the sensitivity of the information at issue and the public interest in that information might potentially affect the balance struck (at [81]).
[577] At [76].
[578] At [88].
[579] GDPR, art 17(1).

(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

While the content of the right was the subject of considerable debate during its development,[580] from the start, the European Commission and its Vice-President at the time, Viviane Reding, were clear that the rights were not new, but rather an elaboration[581] or reinforcement[582] of the existing rights in art 12(b) of Directive 95/46/EC. Leta Jones argues that arts 17(1)(a), (c) and (d) can be found in the Directive, but that art 17(1)(b) is a "novel" ground for erasure.[583] The erasure ground in art 17(1)(f) is also new, as is the structure of the whole article.[584] In the Directive, the erasure mechanism was part of a person's right to access data and served the purpose of ensuring personal data concerning a person was correct and processed lawfully.[585] Now the access and erasure rules are contained in different articles.[586] Article 17 also extends the right provided for under *Google Spain*. The decision in *Google Spain* only applies to search engines; however, the right to have personal data erased applies to all personal data when the stated grounds are met, irrespective of the organisation which holds it and even if it has not been published. Where the data has been published publicly, art 17(2) imposes an additional obligation to advise third parties who are processing the public data that erasure has been requested, when a right to erasure has been established by the data subject.[587] Finally, art 17(3) ensures the right to erasure is not an absolute one, noting that the right does not apply to the extent the processing is necessary for, amongst other things, freedom of expression, historical research and statistical purposes.

---

[580] The legislative process took over four years, during which time, various changes to the article were promoted. See generally EDPS, above n 554, at 96–108. For a discussion of the legislative process see Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius "The European Union General Data Protection Regulation: What it is and What it means" (2019) 28 Information & Communications Technology Law 65 at 71.
[581] European Commission *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)* (COM/2012/011, 25 January 2012) at 9.
[582] Viviane Reding "The European Data Protection Framework for the Twenty-first Century" (2012) 2 IDPL 119 at 125.
[583] Leta Jones, above n 155, at 48. It should be noted that while Directive 95/46/EC did not state that withdrawal of consent was allowed and that it could form a basis for erasure of personal data, it was recognised under the Directive that consent could be withdrawn If consent was withdrawn, and no other lawful basis for processing was established, data should be deleted. See Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent* (WP 187, 13 July 2011).
[584] Children were singled out by the European Commission as requiring special attention in the law reform process. See European Commission, above n 515, at 6.
[585] See Directive 95/46/EC, Recital 41. See also Joined Cases C-141/12 *YS v Minister voor Immigratie, Integratie en Asiel* and C-372/12 *Minister voor Immigraties, Integratie en Asiel v M and S* ECLI:EU:C:2014:2081 at [44].
[586] GDPR, art 15 sets out data subject's rights of access to personal data.
[587] See Harvey, above n 1, at 304–305.

III Does the Privacy Act 2020 Provide a Right to be Forgotten?

To determine the extent to which the Privacy Act 2020 includes the version of the RTBF seen in *Google Spain* or the right to erasure under the GDPR, the discussion must start with the existing erasure rules. These are contained in IPP 7 and 9. The discussion below considers the wording of the IPPs as set out in the Privacy Act 2020. However, because the Act only came into force in December 2020, all the cases discussed in this chapter were decided under the 1993 Act. However, the relevant rules of the new Act have not fundamentally changed the substance of the IPPs in the 1993 Act, so the decisions under the 1993 Act are still relevant.

A New Zealand's Erasure Tools

1 Information Privacy Principle 7

IPP 7 provides the Privacy Act's rules regarding correction of personal information. The relevant subsections of IPP 7 state:[588]

> (1) An individual whose personal information is held by an agency is entitled to request the agency to correct the information.
> (2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

"Correction" is defined in the Act as a means to alter personal information by way of "correction, deletion, or addition".[589]

In his submission on the Privacy Bill, the Privacy Commissioner called IPP 7 a "limited" right to erasure. [590] However, the Privacy Commissioner's comments may be overstating the

[588] Privacy Act 2020, s 22. It will be noted that IPP 7(2) does not actually include the obligation to correct. In contrast, IPP 7(2) of Privacy Act 1993 stated that: "An agency that holds personal information shall … take such steps (if any) *to correct* that information" (emphasis added). The omission of the verb in the Privacy Act 2020 appears to be an error in the drafting and the provision is intended to impose an obligation on agencies to correct information. The present research analyses IPP 7(2) on the basis that the omission is an error.
[589] Pursuant to the definition of "correction", it could be questioned whether information is "altered" by complete erasure or deletion. However, Paul Roth *Privacy Law and Practice* (online ed, LexisNexis, Wellington, 2018) at PA22.83(b) believes it can be. He notes that: "The term 'correction' may include removing information entirely."
[590] Privacy Commissioner, above n 548, at [7.3].

matter. The IPP (and most other IPPs in the Act) does not confer any legal rights that are enforceable in a court of law.[591] Redress under the Act for a breach of an IPP is available via the complaints mechanisms set out in the Act, which include complaints to the Privacy Commissioner and civil proceedings in the Human Rights Review Tribunal (the Tribunal) (which is not a court of law).[592] Further, individuals only have the ability to *request* correction, which, as discussed below, has been held not to amount to a blanket right to have information erased or deleted.

The exact status of an agency's obligation to correct has been subject to some disagreement. In *Macdonald v Healthcare Hawkes Bay*, the plaintiff requested the removal of a sentence in a document. However, the accuracy of the sentence was disputed by the parties. In response, the Tribunal stated that: "We think this is the reason why agencies have the ability pursuant to IPP 7 to *choose* whether to correct information or attach a statement of correction to it."[593] However, in *Henderson v Commissioner of Inland Revenue* the Tribunal made a contrary finding as follows:[594]

> We would not go so far as to suggest that an agency has a free choice in every case to choose whether it will correct information or adopt the 'correction sought but not made' procedure instead. There will be cases where the kind of information at issue, the extent of the inaccuracy in it and the likely future use of the information will mandate correction rather than relying on a statement of correction sought but not made … .

In *Plumtree v Attorney-General on behalf of the New Zealand Defence Force,* the Tribunal noted that IPP 7 "does not require an agency to accede to every request for correction".[595] In addition, the Privacy Commissioner has stated that: "Although a person can ask an agency to correct personal information, they cannot compel an agency to delete information."[596] The extent of IPP 7 must also be interpreted in light of the words of the principle itself. IPP 7(2) uses 'must', which is an imperative. Must is different to 'may', which implies a choice. While

[591] Privacy Act 2020, s 31. The exception is the right of access against public sector agencies under IPP 6.
[592] See Roth, above n 589, at PA31.2. This lack of legal rights in the Privacy Act contrasts with the GDPR which states at art 79(1) that "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed". Article 79(2) states that proceedings shall be brought before the courts of the Member State where the controller or processor is established.
[593] *Macdonald v Healthcare Hawkes Bay* [2000] NZCRT 35 at [3] (emphasis added). This quote referred to IPP 7(3) under the Privacy Act 1993. That requirement is now IPP 7(4) under the Privacy Act 2020. The IPP allows individuals to request a statement of correction to be attached to information if the agency does not make a correction which has been requested.
[594] *Henderson v Commissioner of Inland Revenue* HRRT 49/02, 10 June 2004 at [71].
[595] *Plumtree v Attorney-General on behalf of the New Zealand Defence Force* HRRT 29-01, 2 October 2002 at [54].
[596] See *Case Note 284027* [2018] NZPrivCmr 1 (18 January 2018).

'must' is clear, confusion arises internally with the wording of IPP 7(4) because IPP 7(4) states: "If an agency … is not *willing* to correct that information".[597] The use of 'willing' implies that agencies have a discretion about whether or not to correct information. While this language is confusing, IPP 7(2) obliges agencies to correct information in the circumstances described. Accordingly, the finding in *Henderson v Commissioner of Inland Revenue* represents the most appropriate summation of the law. The key is that the imperative to correct or erase does not operate all the time – only when it is a reasonable step to ensure the accuracy of information considering the purposes for which the information may be lawfully used. In short, IPP 7(2) provides a qualified compulsion.

To understand when erasure is required, the qualifications are, therefore, important. The first is that an agency only has to take *reasonable steps* to correct or erase personal information to ensure accuracy.[598] In *Plumtree* (which was a correction [not erasure] case), the Tribunal noted:[599]

> … in the absence of any suggestion that anything turns on the accuracy of the record, there is nothing in Principle 7(2) that would have obliged the army to conduct a full scale inquiry to determine conclusively whether its records are right or wrong.

In *Case Note 15376*, the Privacy Commissioner held that impracticable steps were not reasonable steps:[600]

> The hospital considered that [sealing 28-year-old admission notes] would be impracticable because of the nature of its records filing system. Given the large number of patients who have received and will receive treatment from the hospital and taking into account the difficult task of maintaining a large volume of medical records, I considered that the hospital had a good reason for not acceding to this request.

However, in *EFG v Commissioner of Police*, while discussing the reasonable steps required to meet the accuracy before use obligation under IPP 8, the Tribunal recognised that in some circumstances, like the release of information to a third party, reasonable steps might require

[597] Interestingly, IPP 7(4) has a 'must' (which under the Privacy Act 1993 was a 'shall'), which has been interpreted as an imperative, requiring that a statement of correction is attached to information where an agency is not prepared to correct information. See *Macdonald,* above n 593*,* at [3].
[598] See Privacy Act 2020, s 22 principle 7(2).
[599] *Plumtree*, above n 595, at [55] (emphasis added).
[600] *Case Note 15376* [2001] NZPrivCmr 1 (April 2001).

"particular care to be taken".[601] Accordingly, what are reasonable steps will depend on the circumstances of each case, including the particular use of the information and what steps are practical in the circumstances.

The second qualification is that IPP 7 performs a data quality role only, allowing erasure to ensure the accuracy of personal information.[602] The accuracy standard is set at "accurate, up to date, complete, and not misleading".[603] In *Henderson v Commissioner of Inland Revenue*, the Tribunal recognised that the principle "contains four adjectives to describe information and each conveys a different idea about the respects in which information can be thought of as being incorrect."[604] Despite this recognition, the Tribunal did not consider the individual meaning of the words, favouring instead the fact that together they set an accuracy standard that agencies must meet.[605]

The accuracy standard must also be considered in relation to the lawful use of the information at issue. In *EFG*, the Tribunal raised the idea that a different accuracy standard may apply if the information is only used internally. In that case, which dealt with information provided by the Police on a vetting form, the Tribunal stated that: "Perhaps the information in the noting might have been adequate if it was to be used for internal Police purposes."[606] Similarly, in the earlier decision of *Wilson v Accident Compensation Corporation*, which dealt with a claim under the IPP 7(2) equivalent in the Health Information Privacy Code that certain internal records of ACC were not accurate,[607] the Tribunal noted that: "If the computer records were indeed no more than an internal record … then we would be inclined to think that in that context the information was sufficiently accurate."[608] The Tribunal, however, came to a different conclusion in *Plumtree.* In *Plumtree*, the plaintiff requested correction of his historical army records. The Tribunal agreed and ordered the New Zealand Army to update the records, noting that "the army has an obligation under Principle 7(2) to ensure that the

[601] *EFG v Commissioner of Police* HRRT 11/2005, 21 December 2006 at [70(e)]. IPP 8 requires agencies to take reasonable steps, before using information, "to ensure that information is accurate, up to date, complete, relevant, and not misleading." It includes the word 'relevant' which is not in the IPP 7 accuracy standard.
[602] This focus on data quality is demonstrated by the use of a similar phrase, "accurate, complete and kept up-to-date", in the Data Quality Principle (para 8) of "The OECD Privacy Framework" (2013) The OECD <www.oecd.org> at 14. See also "Paragraph 8: Data Quality Principle" at 56. The IPPs in the Privacy Act draw heavily from the OECD Privacy Guidelines, as noted in Privacy Act 2020, s 3 which states that: "The purpose of this Act is to promote and protect individual privacy by … giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines".
[603] Privacy Act 2020, s 22 principle 7(2).
[604] *Henderson*, above n 594, at [55].
[605] At [55].
[606] *EFG*, above n 601, at [70(e)].
[607] Health Information Privacy Code 1994, r 7.
[608] *Wilson v Accident Compensation Corporation* HRRT 14/2002, 1 July 2003 at [25].

information is … accurate."[609] Roth questions this conclusion, arguing that because the information was 40 years old and "not useful for any purpose (save for unlikely historical interest)", such updating was not required.[610]

IPP 7(2), therefore, imposes a *qualified* compulsion on agencies to erase information. Such erasure is only required when erasure would be a reasonably practical step and it is necessary to ensure the information is accurate in terms of the lawful use of the information.

2 Information Privacy Principle 9

The second erasure mechanism is provided by IPP 9, which requires that: "An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used."[611]

By putting a limit on the length of time an agency can hold personal information, IPP 9 ensures that personal information is deleted (or anonymised) when its purposes are spent.[612] However, the Privacy Commissioner doubted the usefulness of the IPP in his submission on the Privacy Bill. He argued that the IPP "is rendered meaningless" in the face of advanced algorithms and artificial intelligence that have a "thirst" for personal information.[613] To assess whether or not IPP 9 is truly meaningless, the operation of other IPPs must be considered.

IPP 1 states that an agency cannot collect personal information unless it is collected for a lawful purpose connected with a function of the agency and the collection is necessary for that purpose. 'Lawful purpose' is not defined but provided the activity of the agency is not against the law, personal information can be collected where the information is necessary for the activities of the agency. It is for an agency to determine that its purpose for collecting personal information is necessary. IPP 3 then requires an agency to advise a person from whom they are collecting personal information the purpose of the collection. IPP 10 provides the limits on use of information, stating that personal information cannot be used for purposes other than those for which the information was collected, unless a stated ground is met. These stated grounds include (amongst other things) if the information is publicly available or the other purpose is authorised by the data subject.[614] The interplay of these requirements, along

[609] *Plumtree*, above n 595, at [67].
[610] Roth, above n 589, at PA22.84.
[611] Privacy Act 2020, s 22 principle 9.
[612] Roth, above n 589, at PA22.39.
[613] Privacy Commissioner, above n 548, at [7.15].
[614] Privacy Act 2020, s 22 principle 10.

with the increasing data needs of organisations,[615] means that agencies collecting data provide purpose statements which are customarily broad to mitigate any risk that a future use is not allowed under IPP 10.[616] However, these broad purposes enable data to be kept for long periods of time. Google's privacy policy, for example, states that it collects data to "make improvements to our services".[617] Most companies engage in processes of continuous improvement, therefore, with such a broad purpose they are able to keep data for a very long period of time.[618]

Furthermore, IPP 9 is not restricted to the purposes for which the information was collected, but to any lawful use that the information may be put. Such lawful use is often dictated by other legislation that may set mandatory record retention periods to which agencies must adhere.[619] Whether retention of personal information was lawful was considered by the Privacy Commissioner in *Case Note 13066*. In the case, the complainant argued that his employer should have destroyed information about a former disciplinary process to which he had been subject. In 1984, the person had been suspended and then reinstated on the basis that the reasons for his suspension would remain on his file for two years and if there was a repeat of the incident, he would be dismissed. Eleven years later, the man was involved in another incident and suspended pending inquiry. While the agency had removed the information about his previous suspension from his file, they had retained it in their archives and subsequently presented it during the inquiry into his recent suspension. The Privacy Commissioner held that the agency's retention of the data met a lawful purpose because the agency "has an interest in ensuring that its professional staff work in accordance with appropriate professional and personal standards".[620]

That IPP 9 has limited utility is an argument hard to counter. In his submission on the Privacy Bill, Roth argued that IPP 9 was not necessary. He argued that IPP 9 was rarely invoked and even less frequently successful.[621] However, the Ministry of Justice recommended keeping it, noting that IPP 9 "reminded agencies to think about whether they need to retain personal

[615] See discussion in Chapter 4(III) above.
[616] For some examples of broad purpose statements, see Google's Privacy Policy at "Privacy Policy" (22 January 2019) Google.com <https://policies.google.com/privacy> or Facebook's Data Policy at "Data Policy" (19 April 2018) Facebook.com <https://www.facebook.com/about/privacy/update>.
[617] Google's Privacy Policy, above n 616.
[618] The New Zealand Privacy Commissioner has noted that IPP 9 does not mean that personal information can be held indefinitely. See *Case Note 218236* [2011] NZ PrivCmr 4 (1 February 2011).
[619] See for example *Case Note 284027*, above n 596, where the agency had to retain information for insurance claim purposes.
[620] *Case Note 13066* [1998] NZPrivCmr 10 (1 April 1998).
[621] Paul Roth "Submission to the Justice Select Committee on the Privacy Bill 2018" (29 June 2018) New Zealand Parliament: Privacy Bill <www.parliament.nz> at 5.

information".[622] The role of IPP 9 as a reminder was also evident in the Privacy Commissioner's *Necessary and Desirable – Privacy Act 1993 Review* report, published in November 1998. In the report, the Privacy Commissioner noted that:[623]

> The principle discourages agencies from continuing to retain personal information that is no longer needed. A privacy risk exists where such personal data is retained since:
>
> - the information may become out of date and therefore should not be used (see also principle 8);
> - accumulations of personal information create a risk that they will be used regardless of the purpose for which the information was obtained or the ability to approach the individual directly for the same information (see also principles 2 and 11);
> - the retention of personal information well beyond its "use by date" represents an additional and avoidable security risk as it may inadvertently be disclosed (see also principles 5 and 11).

Over 20 years after the publication of *Necessary and Desirable*, it is even harder to argue that personal information is no longer necessary to an agency's operations. Furthermore, while a role of focusing agencies' attention on retention is admirable, in light of infrequent use and even less frequent successful challenge, there is a real question about whether it is achieving that purpose. However, for the time being, the issue has been put to rest and IPP 9 remains, although it is likely that it will continue to provide little impetus for organisations to actually erase personal information.

What New Zealand has, therefore, are two erasure tools. One related to the accuracy and quality of personal information, the other to spent purposes. However, to determine the extent to which these tools can be used to provide the versions of the RTBF discussed above, the tools must be benchmarked against those versions of the RTBF. First, the chapter considers whether the outcome in *Google Spain* could have been achieved via the Privacy Act's provisions. Second, the provisions are directly compared against art 17 of the GDPR.

[622] Ministry of Justice *Departmental Report on the Privacy Bill – Part Two (*March 2019) at 160.
[623] Privacy Commissioner *Necessary and Desirable – Privacy Act 1993 Review* (November 1998) at [2.11.1].

B Benchmarking New Zealand's Erasure Tools

1 Google Spain v Privacy Act

To determine if a similar outcome to the decision in *Google Spain* could have occurred under the Privacy Act, the first issue is one of territoriality. In *Google Spain*, Google was held by the CJEU to be within the ambit of Directive 95/46/EC due to the specific wording of that legislation, which applied to the processing of personal data "carried out in the context of the activities of an establishment of the controller on the territory of the Member State".[624] The Privacy Act 2020 includes new extra-territoriality provisions, which state that the Act applies to an overseas agency that collects or holds personal information in course of carrying on business in New Zealand. [625] While 'carrying on business' is not defined, s 4(3) clarifies that it does not require the agency to have a commercial operation or a place of business in New Zealand or to receive any money or make any profit in New Zealand. In discussing the applicability of *Google Spain* to New Zealand under the 1993 Act, Liddicoat argued that factors like Google being established in New Zealand for tax purposes and having a small local business established for marketing services to New Zealand businesses involving New Zealand customer information would weigh in favour of the Act's applicability to Google.[626] These arguments are even stronger under the 2020 Act which includes a specific reference to carrying on business in New Zealand. In Toy's advocacy for the extra-territoriality of the Privacy Act 2020, he argued that an agency carrying on business in New Zealand should include an overseas SNS to which New Zealand consumers contract and which have millions of customers who view information on their screens located in New Zealand. This same analysis would apply to Google in regard to its search engine.[627] Accordingly, in light of the new extra-territoriality provisions, it is likely that Google or other overseas search engine will be subject to the Privacy Act 2020.

Google Spain was argued on two grounds – a request to erase data and objection to processing. The Privacy Act does not have the concept of objection to processing, so the logical starting place would be the erasure rules in IPP 7. Under IPP 7 a person whose information is *held* by an agency can request correction or deletion. To ask Google to delete

[624] Directive 95/46/EC, art 4(1)(a).
[625] Privacy Act 2020, s 4(b).
[626] Joy Liddicoat "The Right to be Forgotten" (paper presented during Privacy Week to New Zealand Law Society, Continuing Legal Education, and IT & Online Law conferences, May 2015) Privacy Commission <www.privacy.org.nz> at 7.
[627] Dr Alan Toy "Submission to the Justice Committee on the Privacy Bill 2018" at 2. Google's terms of service are set out at the bottom of the standard search page at https://www.google.co.nz and are available by clicking the 'terms' hyperlink.

search results, Google must first be found to 'hold' personal information. 'Hold' or 'holding' are not defined in the Act, nor does the concept have a direct equivalent in Directive 95/46/EC. However, the Directive's definition of 'processing' included 'organisation' and 'storage' of information – concepts similar to 'holding' information. Accordingly, the CJEU's conclusion that Google's activities amount to processing may be relevant. Here the Court stated:[628]

> … in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results.

In indexing and storing information on its servers as described by the CJEU, there is a good argument that Google 'holds' personal information under the Privacy Act.

As an agency that holds personal information, upon a request for erasure, Google would have to take reasonable steps to delete the information to ensure it is accurate, up to date, complete and not misleading, having regard to the purposes for which the information may be lawfully used. Turning first to the accuracy standard, it is clear that the Privacy Act's data quality focus is different from the focus of art 6(1(c)-(e) of Directive 95/EC/46. The Directive's wording speaks to relevance and excessiveness, which encompasses components of the proportionality principle.[629]

Mr Gonzáles' argument to the CJEU was that the information was irrelevant. The auction notice had been placed in the newspaper to ensure a wide audience and attract as many bidders as possible for the foreclosure sale. Twelve years later, this purpose was spent and therefore the information was irrelevant.[630] However, without the concept of proportionality in IPP 7(2), Mr Gonzáles would have to argue based on accuracy and lack of data quality and this is problematic because the information at issue in *Google Spain* was accurate.[631]

---

[628] *Google Spain*, above n 5, at [28].
[629] See Lee A Bygrave *Data Privacy Law: An International Perspective* (Oxford University Press, Oxford, 2014) at 148. The proportionality principle is used to determine if interference with rights are justified. The concept employs concepts of suitability, necessity and fair balance. It is further discussed in Chapter 7(VI).
[630] *Google Spain*, above n 5, at [14]–[16].
[631] Opinion of Advocate General Jääskinen in Case C-131/12 *Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales* ECLI:EU:C:2013:424 at [105].

Mr Gonzales may be able to construct an argument based on Google's *purpose* for using the personal information. Such an argument would focus on the fact that Google's purpose is to "create a dynamic profile of what they consider to be the most 'relevant' information available online which is available to be indexed in relation to that individual".[632] The argument would then be that, because the information at issue is spent, it is no longer relevant, and therefore it is not "up to date, complete and not misleading" having regard to Google's purpose of displaying the most 'relevant' information as a result of search queries.[633] This argument might become stronger where there is potential for harm to the person concerned and no corresponding public interest in the information.[634] However, this argument is strained and requires an uneasy extension of the intent of the IPP in order to be accepted. A standard linked to proportionality in IPP 7 would avoid these issues. Furthermore, the principle of proportionality is not unknown in the Privacy Act and in privacy law more generally. IPP 1 holds that personal information should be collected only to the extent necessary to achieve the purposes for which it is collected.[635] Furthermore, as is discussed in Chapter 7, proportionality has been central when privacy is balanced against competing interests, like freedom of expression, in the disclosure tort.[636]

The second consideration is that the obligation on agencies is to take reasonable steps to ensure the accuracy standard is met. Reasonableness was not a component of the *Google Spain* decision[637] and the issue has not come before New Zealand decision bodies, so the question of whether delisting or delinking search results is a reasonable step for a search engine to take is a novel one.[638] However, some factors might be relevant to the assessment. First, the process of conducting the delisting is obviously an involved one. Google's Transparency Report highlights five steps in the delisting process: (1) receive request; (2) manual review; (3) request for further information (if required); (4) assessment against criteria developed to meet the Article 29 Data Protection Working Group Guidelines (which includes balancing the differing rights and interests at stake);[639] and (5) notification of decision, including a brief explanation if the decision is to not delist.[640] A complex process, coupled

[632] Office of the Privacy Commissioner of Canada *Draft OPC Position on Online Reputation* (26 January 2018).
[633] Privacy Act 2020, s 22 principle 7(2).
[634] See Office of the Privacy Commissioner of Canada, above n 632.
[635] Gunasekara and Toy, above n 53, at 543.
[636] At 543. See also Chapter 7(VI) below.
[637] Reasonable steps are not mentioned in the proportionality test of art 6(1)(c) of Directive 95/46/EC. There was a test of "every reasonable step" in art 6(1)(d), but this provision was not the main basis for the decision in *Google Spain*.
[638] Liddicoat, above n 626, at 6–7.
[639] Article 29 Data Protection Working Party Guidelines Working Party, above n 394. See also Aleksandra Kuczerawy and Jef Ausloos "From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain" (2016) 14 Colo Tech LJ 219 at 231.
[640] Google Transparency Report, above n 460.

with the potential number of requests that might be made, means that the steps may be considered impractical.[641] Certainly, the United Kingdom's House of Lords concluded that the decision in *Google Spain* imposed an unreasonable burden on Google which was ultimately unworkable.[642] Pointing in the opposite direction, however, is the fact that, aside from the decision in *Google Spain*, search engines provide a level of filtering or removal of links to comply with copyright requirements of various jurisdictions.[643] Furthermore, the fact that Google's model is based on displaying *relevant* results means that there is inbuilt filtering in their tool. So decisions (albeit, algorithmic ones) are being made anyway to determine which results to display.

It is a question of conjecture how these factors would influence the outcome of the reasonable assessment. If the case was a novel one, that had never come before the CJEU, it is arguable that the New Zealand decision makers would have held delisting to be unreasonable steps. However, following the decision in *Google Spain*, that argument is open to challenge. To a certain extent, Google may be a victim of its success in effecting the solution. However, while the result of a reasonability assessment is uncertain, what is clear is that the reasonableness requirement of IPP 7(2) adds an additional hurdle that was not present in *Google Spain* and impacts on the Privacy Act as an effective erasure tool.

In conclusion, this thesis argues that it is unlikely *Google Spain* would have been decided the same way under the Privacy Act 2020. Even now, in the aftermath of *Google Spain*, a similar finding appears to stretch the Privacy Act beyond its intent. However, while IPP 7 may be too limited to provide a Mr Gonazeles' plaintiff with an appropriate remedy there are other tools within the Privacy Act that could potentially be used. As noted above, the CJEU was clear that Google's processing of Mr Gonzales' data involved disclosure, so that IPPs 8 and 11 provide potential routes to prevent Google from disclosing the information complained of.[644]

---

[641] See *Case Note 15376*, above n 600. While there is no available data on the number of Google searches in New Zealand, Google does report the number of delisting requests it receives in the European Union, which for the previous year is over 10,000 a month. While numbers in New Zealand would be considerably less, using a blunt population percentage calculation (that is, New Zealand has one per cent the population of the European Union) there could be over 100 a month in New Zealand.

[642] House of Lords European Union Committee *EU Data Protection Law: A 'Right to Be Forgotten'?* (2nd Report of Session 2014–15, HL 40, 30 July 2014) at 33–34 and 56.

[643] See Office of the Privacy Commissioner of Canada, above n 632.

[644] When the Office of the Privacy Commissioner of Canada considered whether its Federal Personal Information Protection and Electronic Documents Act 2000, SC 2000 (PIPEDA) required search engines to remove search results, it found additional grounds existed to support a claim similar to Mr Gonzáles' under its s 5 requirement that an organisation may only collect, use or disclosure personal information for purposes that a reasonable person would consider are *appropriate*. See Office of the Privacy Commissioner of Canada, above n 632. The Privacy Act 2020 has no equivalent provision. Considering that Mr Gonzales argued that the foreclosure notices were spent, it is logical to think that in New Zealand he may also argue his case under IPP 9, which as noted above, addresses spent purposes. However, the spent purposes of Mr Gonzales' information relates to its original purpose as a foreclosure notice. An IPP 9 claim would look at Google's purpose of holding

While not a deletion, these disclosure limits would have the same net effect of stopping Google from displaying the search results complained of.

IPP 8 is the 'accuracy before use' principle, and states that:[645]

> An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Like IPP 7, IPP 8 is related to data quality,[646] although it is noteworthy that IPP 8 includes the word 'relevant', whereas IPP 7 does not. However, despite the difference, it is arguable that IPP 8 is no closer to importing a sense of proportionality than IPP 7. The relevance in IPP 8 is more akin to the information's relatedness to purpose rather than the proportionality principle discussed above, which is directed towards suitability, necessity and excessiveness.[647] Accordingly, under IPP 8, the accuracy standard poses similar issues as discussed in regard to IPP 7. IPP 8 also suffers from the same drawback as IPP 7 regarding reasonable steps.[648] Furthermore, breaches of IPP 8 are only considered interferences with privacy if the breach causes loss or damage, significant humiliation, loss of dignity or injury to feelings.[649] These harms were not pleaded in *Google Spain* (because harm was not required in order to establish Mr Gonzáles' claim), therefore there is no evidence of what harm, if any, the plaintiff suffered.[650] However, to rely on IPP 8, a Mr Gonzales plaintiff would have to point to some harm to establish an interference with privacy. In contrast, a breach of IPP 7 is itself an interference of privacy, provided the Privacy Commissioner or the Tribunal concludes there is no proper basis for the agency to refuse to correct or erase the information. A determination of interference does not turn on whether there was harm (although the lack of harm may go to the remedy provided for the breach).[651]

---

the information, and as noted above, that is a much broader purpose – creating a profile of relevant information available to index. Furthermore, Google's privacy policy states that it uses personal information for even wider purpose – to "make improvements to our services" (see above n 616) – accordingly, it is much harder to argue that keeping the information is no longer relevant to those broad purposes.

[645] Privacy Act 2020, s 22 principle 8.

[646] OECD Privacy Framework, above n 602, at 56.

[647] At 56.

[648] The argument that delinking or delisting search results is an unreasonable action is likely to be stronger under IPP 8 because IPP 8 operates *before* use. Considering that the display of search results is an automated process, and the volume of search results Google is likely to action daily, it is hard to see that checking accuracy before use would be reasonable.

[649] Privacy Act 2020, s 69(2).

[650] *Google Spain*, above n 5, at [96]. See also Voss and Castets-Renard, above n 560, at 326.

[651] See *Henderson*, above n 594, at [116].

IPP 11 states that:[652]

> An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds,—
> (a) …
> (d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information;

The information at issue in *Google Spain* was sourced from a publicly available newspaper website, therefore, the issue under IPP 11 is whether Google's disclosure would be fair and reasonable. The "fair and reasonable" test was included in IPP 11 following the introduction of the HDCA. In recommending the amendment, the NZLC noted that the standard of "unfair or unreasonable" was less than a "highly offensive" standard.[653] While not providing any further guidance on what might be unfair or unreasonable, previous reports from the NZLC alluded to some "extreme" examples which might meet the standard, including the posting of sensitive personal information obtained by hacking or the posting of naked photos of a person on a SNS without that person's consent.[654] Furthermore, the NZLC has also recognised that:[655]

> … it may be that some material is of such sensitivity that the subject of it can *reasonably* expect that even if it has been widely published previously it will nevertheless not be published again.

Continuing this line of thought, the NZLC then said: "Likewise, a conviction which appeared in the media at the time may now be so far in the past that it would be *unreasonable* to revive it."[656] Therefore, it might be unreasonable for the purposes of IP 11 to disclose old convictions or sensitive information.

Mr Gonzáles' information was not an extreme example, nor was it a past conviction. However, the CJEU considered the information was sensitive to the data subject's private life.[657] That said, it is still uncertain if the information would reach the standard anticipated by

[652] Privacy Act 2020, s 22 principle 11.
[653] Law Commission *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (NZLC MB3, 2012) at [4.125].
[654] Law Commission *Review of the Privacy Act 1993* (NZLC R123, June 2011) at [2.98].
[655] Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, March 2009) at [6.40] (emphasis added). This statement was made during a discussion of the disclosure tort in New Zealand.
[656] At [6.40] (emphasis added).
[657] *Google Spain*, above n 5, at [98].

the NZLC. Again, it may be that the gulf between Mr Gonzales' complaint and the wording of the Privacy Act is too large for IPP 11 to provide an effective remedy.

Despite the limitations just discussed, for the right plaintiff, IPP 8 and 11 might provide some recourse. This conclusion does not mean, however, that these IPPs make up for the deficiencies of IPP 7 as an erasure tool. A finding based on IPP 8 or 11 implies a preventative action – that Google should not have used or disclosed the search results. However, a search engine would never know that these IPPs were breached until they were advised by the data subject of the prejudicial nature of the personal information. Accordingly, a regulatory framework that allows search engines and other organisations to react to requests for erasure from individuals is more workable and appropriate.[658] Such a framework has the benefit of providing people with more ongoing control over their information and provides a mechanism for people to force agencies to justify why they are holding personal information.[659] These measures would also strengthen the Privacy Act's commitment to the general principle of individual participation, which is one of the fundamental data protection principles underpinning most modern data protection statutes.[660]

While there is a clear need to strengthen the erasure provisions, there is also benefit to ensuring that the other options within the Privacy Act for protecting once public facts are as effective as possible. In particular, there is benefit in broadening the obligation under IPP 8 so that agencies not only have to ensure personal information is accurate before use, but that the use is proportionate. Including proportionality in IPP 8 would also potentially provide a form of RTBF akin to the right to judicial oblivion discussed above, where the focus is on whether or not information can be used or disclosed rather than whether or not it is deleted.[661]

2 General Data Protection Regulation v Privacy Act 2020

The first ground for erasure under art 17 of the GDPR is where "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed".[662] This purpose expiry concept is reflected in IPP 9 of the Privacy Act, although it is not a ground on which a person can request erasure by an agency under IPP 7. Under IPP 9 a person who believes an agency is holding information for longer than necessary would

[658] This reactive nature of a search engine is discussed by Kuczerawy and Ausloos, above n 639, at 226.
[659] Bernal, above n 364, at 15.
[660] See OECD Privacy Framework, above n 602, at 15 and 58.
[661] See Koops, above n 567, who argued that there was value in using the RTBF to achieve a clean slate and Leta Jones, above n 155, at 130.
[662] GDPR, art 17(1)(a).

make a complaint to the Privacy Commissioner in order to force an agency to delete data. Not only is purpose expiry difficult to establish for the reasons discussed above, like IPP 8 and 11, a breach of it will only be an interference with privacy if the breach causes loss or damage, or significant humiliation, loss of dignity or injury to feelings.

It could be argued that because the net effect of IPP 9 is that an agency could be forced to erase data, the different routes in the GDPR and the Privacy Act do not matter. However, such a conclusion is too simplistic. Article 17 of the GDPR is about a person's control over data. IPP 9 is not. IPP 9 is about ensuring that agencies adhere to the principle of purpose limitation.[663] Furthermore, IPP 9 does not provide a tool for data subjects to directly check the actions of agencies, requiring the agencies to justify their holding of personal information and allowing data subjects continued engagement with their data once they have handed it to the agency.[664]

The second ground for erasure operates when a data subject has withdrawn consent to processing.[665] Leta Jones argues that this ground seeks to "establish a balanced environment where individuals can continually and effectively re-evaluate their consent [to data processing]".[666] Consent in the Privacy Act plays a different role than in the GDPR. In the GDPR, consent is one of the lawful grounds for processing personal data. However, the Privacy Act does not require lawful grounds to collect or use personal information, rather, collection and use is lawful if such activities meet the requirements of the Act. Consent is not a component of this requirement.[667] Therefore, because consent is not a requirement for collection or use, lack of consent is not a ground for erasure.

The third ground is where a data subject objects to processing – a concept which has no equivalent in the Privacy Act. [668] However, erasure following an objection to processing is of interest because it operates where the lawful basis of processing is the legitimate interests of the controller (art 6(1)(f) of the GDPR),[669] which was one of the grounds of the decision in

[663] Leta Jones, above n 155, at 48.
[664] See Cécile de Terwangne "Internet Privacy and the Right to be Forgotten/Right to Oblivion" (2012) 13 IDP 109 at 114.
[665] GDPR, art 17(1)(b).
[666] Leta Jones, above n 155, at 48–49.
[667] A type of consent can be seen at the collection stage by the fact IPP 3 requires agencies to advise individuals of the collection of personal information and the purpose and use of that information. If people do not want their information used in that way they do not have to provide it. As a result, if they do, they have 'consented' or 'authorised' that use. However, compared to the GDPR, this consent is very weak. Article 7 of the GDPR is clear that consent must be freely and clearly given. See also Recital 32 of the GDPR.
[668] GDPR, art 17(1)(c).
[669] The equivalent under Directive 95/46/EC was art 7(f).

Google Spain. This ground of erasure ensures that erasure can occur when a person demonstrates that their interests and fundamental rights and freedoms override those of the controller. Establishing this ground requires a balancing of interests, as discussed in *Google Spain*. No such balancing is required for erasure decisions in New Zealand.[670] Accordingly, if a person's circumstances change after data collection and compelling reasons arise for them to want to keep information private, this does not provide a ground for erasure of data where the information still meets the accuracy standard.

The fourth ground of erasure is where personal data has been unlawfully processed.[671] While there is no direct comparator in the Privacy Act, a similar outcome could be achieved via other mechanisms in the Act. First, IPP 9 may provide some protection because if personal information is collected, stored and used unlawfully, then it is unlikely to meet the retention test of "purposes for which the information may lawfully be used".[672] However, this IPP suffers from the drawbacks discussed earlier. Second, erasure could be a remedy ordered by the Privacy Commissioner via a Compliance Notice,[673] or by the Tribunal under s 102(2)(d) where there has been found to be an interference with the privacy of a person.[674] However, these remedies are not a right that a person can pursue directly against an agency in the first instance, allowing people to directly check the actions of agencies and requiring the agencies to justify their holding of personal information to the individual concerned.

The final relevant ground operates in relation to personal data collected from children. The issue of children consenting to the use of data without fully understanding the risks was central to the introduction of art 17.[675] Under the Privacy Act, the data of children are not dealt with differently to any other personal information, although the 2020 amendments do include an amendment to IPP 4 that references children. IPP 4 states that an agency can only collect information by a lawful means, and by a means that, "in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons)", is fair and does not unreasonably intrude on the personal affairs of the

[670] See Chaper 7(IV)(c) for a discussion of the balancing which does exist in the Privacy Act 2020.
[671] GDPR, art 17(1)(d).
[672] Privacy Act 2020, s 22 principle 9.
[673] Sections 123–125. A Compliance Notice can be issued if the Privacy Commissioner believes there has been a breach of the Act or an IPP.
[674] Section 102(2)(d) allows the Tribunal to "order that the defendant perform any acts specified in the order with a view of remedying the interference". An interference with the privacy of an individual could result from a breach of any of the IPPs (see ss 69(1) and 102(1). An example where erasure has been ordered as a remedy is *Armfield v Naughton* [2014] NZHRRT 48.
[675] European Commission, above n 581, at 51. See also Reding, above n 582, at 125; European Commission, above n 552, at 6; and the GDPR, Recital 65.

individual.[676] No further guidance is provided on the intended impacts of this amendment. Children are also not a particular consideration in the erasure provisions of the Privacy Act.

Concerns over the specific vulnerability of children have also gained traction in the United States. In California, the "Privacy Rights for California Minors in the Digital World" legislation was passed in 2013 and took effect in 2015.[677] The law applies to entities that operate websites, online services or provide online or mobile applications targeted to minors. The provisions require such entities to permit minors who register for their services to remove or request removal of content posted on the entities website, service or application by the user. While the law provides a form of the RTBF, notably the right to digital oblivion put forward by Voss and Castets-Renard, the right is limited. The right does not cover content posted by other users, posted anonymously or posts that have been copied and reposted by third parties. The right is also limited to information society services. In contrast, New Zealand's Privacy Act applies to all agencies, including information society services, and to all personal information, whether of minors or adults. However, its erasure tools suffer the limitations herein discussed.

In conclusion, the GDPR provides a range of grounds based for erasure which are considerably more fulsome than in the Privacy Act, and which provide far stronger individual control over personal information.

C Do New Zealand's Erasure Tools Provide a Right to be Forgotten?

This chapter has considered whether the Privacy Act 2020 provides New Zealander's with a RTBF that reflects the decision in *Google Spain*, the right to erasure established by the GDPR or a right to digital oblivion. The limited scope of the erasure rules under IPP 7 of the Privacy Act mean that a decision similar to *Google Spain* is unlikely to occur. The grounds for people to exercise the right to request erasure are limited to accuracy. Questions of excessiveness and proportionality are not part of the test. Furthermore, even if the erasure grounds were broader, agencies still only have to take reasonable steps. The steps did not have to be reasonable under Directive 95/46/EC, nor do they have to be under the GDPR. The GDPR requires controllers to erase without undue delay once the grounds are established (provided there are no competing interests which override the erasure right).

[676] Privacy Act 2020, s 22 principle 4.
[677] CA Bus & Prof Code § 22581. Section 22580(d) states that a minor is a person under 18 years of age.

IPPs 8 and 11 might provide alternate routes to erasure in the form of delisting or delinking search engine result. However, there are hurdles to surmount. Both require a degree of significant harm to establish an interference with privacy, IPP 8 is limited to accuracy and data quality and only requires agencies to take reasonable steps. IPP 11 requires a determination that disclosure was unfair or unreasonable. Furthermore, neither of these provisions provides a person with the ability to, in the first instance, directly check the actions of agencies and require the agencies to justify their holding of personal information.

In comparison to the GDPR, the erasure tools in the Privacy Act are also limited. IPP 7 has one accuracy ground compared to six grounds provided by the GDPR. While purpose expiry under IPP 9 technically provides a marker for when an agency must erase (or anonymise) personal information, its protection is largely illusory and it does not create a point at which a person can exercise authority over their personal information. Information provided when a person was a minor, or where a person's circumstances have changed since they provided the personal information and they have an interest in keeping the information private (for example, a person is subject to a threat of harm and wants to keep their address secret), do not provide any basis on which to erase personal information. There is also no ability for people to request erasure in the event that an organisation breaches an IPP in regard to the organisation's storage or use of that person's personal information. Essentially, individuals provide their personal information to agencies based on broad purpose statements; however, in return, there is limited opportunity for people to continually and effectively re-evaluate whether they want agencies to hold and use their data. A one-time-only surrender of data seems simplistic in the technologically advanced 21st century.

The conclusion must be reached, therefore, that New Zealand's Privacy Act does not provide a RTBF equivalent to either art 17 of the GDPR or the decision in *Google Spain*. What New Zealander's have is the ability to require personal information to be erased in limited circumstances. As a result, New Zealander's have one less tool to protect once public facts and the corresponding interests in liberty, rehabilitation and dignity. Accordingly, this thesis argues that changes to the Privacy Act 2020 are required to remedy this gap. That New Zealander's need a RTBF or a right to erasure was argued by the Privacy Commissioner, and also by many submitters on the Privacy Bill.[678] It is a right that people in England and in Europe have. The Canadian Office of the Privacy Commissioner has found that in some instances Canadian's have a RTBF akin to the decision in *Google Spain*, pursuant to s 5 of

[678] See Jackson-Cox, above n 511.

Canada's Federal Personal Information Protection and Electronic Documents Act 2000 (PIPEDA).[679]

The intent of this chapter is not to set out the shape of any proposed right to erasure or provide specific details of other changes required to the IPPs. The intent is to make the case for such changes and to identify those deficiencies in the Privacy Act which need to be addressed. The shape of the right will be put forward as part of the overall package of amendments in Chapter 9. However, before moving on, there are some specific critiques of the RTBF that need to be addressed.

The first critique is that a RTBF in the form of the outcome in *Google Spain* is inappropriate because it puts the balancing of two critical rights – privacy and freedom of expression – in the hands of a private organisation. Harvey argues that it "is against the rule of law that Google is party, 'judge, jury and executioner' as a result of *Google Spain*."[680] However, privately owned traditional media have been making decisions between privacy and free speech for many years in response to the disclosure tort and the statutory rules under the Broadcasting Act 1989, as will be seen in Chapter 7. Even under the Privacy Act, organisations are required to make decisions regarding competing interests when dealing with access requests under IPP 6.[681] Introducing such a requirement as part of an erasure tool in the Privacy Act is, therefore, not new.

Second, critiques also point to a potential "chilling effect" of the decision in *Google Spain*, whereby private organisations will default to erasure rather than risk costly litigation.[682] However, Google's experience following *Google Spain* does not support this argument. Google's own reporting notes that it has acceded to less than half of the requests made. Furthermore, as noted above, decisions between privacy and speech have been made for many decades under the disclosure tort by traditional media. As a result, a considerable body of jurisprudence has built up on balancing privacy and free speech which could be usefully fashioned into guidance to be deployed when exercising the rights to erasure.

---

[679] Office of the Privacy Commissioner of Canada, above n 632.
[680] Harvey, above n 1, at 303.
[681] See, for example, Privacy Act 2020, s 52(1) which allows agencies to refuse access to information if disclosure would be "likely to unreasonably prejudice the commercial position of the person who supplied the information". However, this ground does not apply if withholding information is "outweighed by other considerations that make it desirable, in the public interest, to make the information available" (ss (2)).
[682] Harvey, above n 1, at 303. See also Gollogly, above n 379, at 136–137. Gollogly argues that: "Proper, independent oversight would require mandatory reporting of de-indexing, alongside justification and review by an independent body tasked with protecting freedom of expression." See also Leta Jones, above n 155, at 130–131 who argues that the decision in *Google Spain* might result in the loss of too much information.

The third is that any erasure tool would apply to all agencies subject to the Act, not just deep-pocket organisations like Google or Facebook. For smaller, less wealthy organisations the tool might impose a burden that could threaten the viability of the organisation or their business model. This burden may increase if the reasonable steps limitation is removed. This is a valid concern and the package of amendments in Chapter 9 addresses this issue.

IV Conclusion

New Zealand's Privacy Act does not provide a strong erasure mechanism. This state of affairs must be remedied. The Ministry of Justice in its report on the Privacy Bill saw this as a topic for future law reform because it would be "a significant extension on the laws New Zealand already has in place".[683] Such a new tool may be a significant extension, but it is also of significant benefit. It would support fundamental values of liberty, rehabilitation, dignity and autonomy, it would support the governmental policy set out in the Clean Slate Act, and it would assist people to manage the impacts of modern technology, where ever increasing amounts of information remain easily accessible on the internet. Furthermore, an erasure tool was supported by the Privacy Commissioner and by many of those who took the time to submit on the Privacy Bill before it passed into law.[684] In addition, this law reform needs to happen sooner rather than later. The decision in *Google Spain* was delivered in 2014 and the GDPR passed in 2016. It is now 2022 and, as time passes, New Zealand's already deficient tools will only become more deficient.

This chapter has also identified the particular aspects which make the Privacy Act deficient. It is these areas any reform must address. The reform must provide a tool which operates on grounds wider than accuracy, it must address the issue of reasonable steps, and it must enable consideration to be given to changed personal circumstances that result in individual rights overriding the rights of agencies. The accuracy before use and disclosure requirements in IPP 8 must also be considered. Like IPP 7, these are too narrow. These aspects are addressed in the package of amendments set out in Chapter 9.

Once public fact scenarios have not only arisen in cases involving statutory privacy protections. In *NT 1 & NT 2*, the plaintiffs brought their case under the English version of the

[683] Ministry of Justice *Departmental Report – Part One: Privacy Bill (*March 2019) at 41 and Ministry of Justice, above n 622, at 61.
[684] This conclusion is the result of analysis conducted by the author on the submissions made by individuals (that is, no agencies or organisations) on the Privacy Bill 2018. These submissions are available at "Privacy Bill, Submissions & Advice" NZ Parliament <www.parliament.nz>.

disclosure tort as well as the Data Protection Act 1998.[685] Furthermore, the seminal once public fact cases of *Melvin v Reid*, *Briscoe* and *Sidis* were all disclosure tort cases in the United States. The tort is, therefore, an important weapon in the arsenal for protecting once public facts. This is particularly the situation in New Zealand where news activities are excluded from the ambit of the Privacy Act.[686] As a result, if a person wishes to challenge the media's publication of once public facts in a news article, then they cannot complain under the Privacy Act. The person needs to use the disclosure tort or make a complaint to the BSA under the Broadcasting Act 1989. Both of these mechanisms are discussed in the following chapters.

[685] Data Protection Act 1998 (UK).
[686] Privacy Act 2020, s 8.

6 PUBLIC DISCLOSURE OF PUBLIC INFORMATION: USING THE PRIVACY TORT TO PROTECT ONCE PUBLIC FACTS

I Introduction

The disclosure tort was given judicial recognition in New Zealand by a majority of the Court of Appeal in *Hosking v Runting*. The elements of the cause of action, set out in the judgment of Gault J, were as follows:[687]

> 1. The existence of facts in respect of which there is a reasonable expectation of privacy; and
> 2. Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

In addition, his Honour recognised a defence of legitimate public concern. While *Hosking* established the cause of action, the case was not a once public facts case, so it is still an open judicial question whether the disclosure tort can protect once public facts.[688] Nonetheless, there have been a number of judicial statements which lend support to the argument that the tort can protect once public facts. However, it is not enough to point to some judicial statements and then conclude that the disclosure tort should cover once public facts. What is needed is a close inspection of the elements of the cause of action to determine if once public facts can satisfy those elements and whether that interpretation is consistent with the development of the disclosure tort generally. This chapter provides that close inspection. The chapter also takes the opportunity to identify any ways in which elements of the cause of action need to develop to ensure it is fit for purpose and can provide appropriate protection for once public facts in the right circumstances. This chapter does not, however, consider the defence of legitimate public concern. The defence is discussed in the next chapter as part of a wider discussion about how privacy is balanced against the important competing value of free speech.

[687] *Hosking*, above n 8, at [117]. This formulation of the cause of action was agreed by two out of the three majority judges. Tipping J, the third majority judge, believed that the offensiveness in the second element should be controlled within the first element of a reasonable expectation of privacy. See discussion in Chapter 6(III)(A) below.

[688] Penk, above n 338, at 432. No once public fact case has made its way to a senior court in New Zealand.

The development of the disclosure tort has not occurred in a vacuum. The shape of the tort has been heavily influenced by the experiences of other statutory systems and jurisdictions. In regard to the former, the jurisprudence of the BSA has had a particular influence. In regard to the latter, the jurisprudence of the United States, England, Australia and Canada has had the most influence. Accordingly, to better understand the drivers for the tort and also to determine if there are ways the tort can be improved, the chapter considers these wider influences in more detail.

As a result of the present research, the chapter finds that the current cause of action is broad enough to protect once public facts and that such protection, in the appropriate circumstances, is consistent with developments in New Zealand and internationally. However, this conclusion does not mean that refinements of the tort are not welcome or required. The chapter proposes specific ways in which the disclosure tort should be developed in order to better protect people's intuitions about privacy and embed a zone of privacy around once public facts. While this final discussion leads towards a model for the disclosure tort, the actual content of that model and its operation is part of the package of amendments in Chapter 9.

II Reasonable Expectations of Privacy

A Common Law

Twenty years before the decision in *Hosking,* the emergence of the disclosure tort began with the case of *Tucker. Tucker* involved a plaintiff who suffered from serious heart disease and required a life-saving heart transplant operation in Australia. In order to raise funds for the operation, the plaintiff engaged in public fundraising. During the fundraising drive the defendant media organisation obtained information that the plaintiff had been convicted of criminal offences in the past, which had resulted in imprisonment.[689] The defendant wanted to publish the information, but the plaintiff sought an injunction to stop publication. While the specific particulars of the case meant that the Judge did not have to determine the invasion of privacy issue,[690] McGechan J held that the facts of the case presented a serious question to be tried in terms of whether the proposed publication breached the plaintiff's privacy. In discussing the nature of the privacy action, McGechan J noted with approval the words of

[689] *Tucker*, above n 385, at 722. Mr Tucker's most recent conviction had been four years before his case.
[690] The case was not a trial of the substantive issues; rather, an application to discharge or vary interim injunctions against the plaintiff which prohibited it from referring to the defendant's criminal convictions.

Jeffries J (who heard the application for an interim injunction), who had noted that the gravamen of the action was the "unwarranted publication of intimate details of the plaintiff's private life which are outside the realm of legitimate public concern, or curiosity."[691] While the cause of action revolved around intimate and private information, McGechan J had no concerns finding that the information at issue – a criminal conviction on the public record – could arguably satisfy this description. Furthermore, in advocating for the introduction into New Zealand common law of the disclosure tort, McGechan J cited with approval the cases of *Melvin v Reid* and *Brisco*e.[692] The protection of once public facts, therefore, finds considerable support in *Tucker*.

Following *Tucker*, the High Court in *Bradley v Wingnut Films Ltd* considered a claim that aspects of the cult New Zealand film "Brain Dead" invaded the plaintiff's privacy by showing a tombstone in the plaintiff's burial plot in a Wellington cemetery.[693] In accepting that the tort existed in New Zealand, Gallen J relied on the formulation of the cause of action in *Prosser and Keeton on the Law of Torts* (5th ed), which required "public disclosure of private facts, which is highly offensive and objectionable to a reasonable person of ordinary sensibilities."[694] No test was put forward for establishing private facts. This may be because the facts at issue – a tombstone in a public cemetery – were not private. In fact, Gallen J said "there could scarcely be anything less private" than a tombstone in a public cemetery.[695]

In *P v D*, which was decided seven years after *Bradley*, a well known plaintiff brought proceedings against a national newspaper to stop publication of the fact the plaintiff had been treated at a psychiatric hospital.[696] Drawing upon the decisions in *Tucker* and *Bradley*, Nicholson J held that the disclosure tort now existed in New Zealand. Nicholson J adopted the three-part test of Gallen J: (1) public disclosure; (2) of private facts; and (3) which are highly offensive and objectionable to a reasonable person of ordinary sensibilities. However, his Honour added a fourth element – the level of legitimate public interest in the matter.[697] In *P v D*, the Judge easily found that information that a person was being treated at psychiatric hospital was private.[698] Two years after *P v D*, 'L', a prostitute, brought a claim for breach of privacy against a former client for the publication of sexually explicit photographs of her in

[691] *Tucker*, above n 385, at 732.
[692] At 733.
[693] *Bradley v Wingnut Films Ltd* [1993] 1 NZLR 415 (HC). Brain Dead is a well known 1992 New Zealand film produced by the defendant, Wingnut Films Ltd, and written and directed by Sir Peter Jackson.
[694] At 423, citing William Lloyd Prosser and Page Keeton *Prosser and Keeton on the law of torts* (5th ed, West Publishing Co, St Paul, 1984) at 851.
[695] *Bradley*, above n 693, at 424.
[696] *P v D* [2000] 2 NZLR 591 (HC).
[697] At [33]–[34].
[698] At [36].

an adult magazine. Applying a similar test to Nicholson J in *P v D*, the District Court Judge who heard L's case, found that the information at issue was inherently private.[699]

The cause of action as set out in *L v G* was where the development of the disclosure tort had landed when the *Hosking* case came before the courts. *Hosking* arose from an application for an injunction to prohibit the publication of photos of the well known plaintiff's young daughters, taken while the children and their mother were walking on a public street in Auckland. In the High Court, Randerson J concluded that New Zealand should not recognise a privacy tort, believing that such development was better left to Parliament.[700] The plaintiff appealed to the Court of Appeal, where a majority of the court decided to recognise the existence of the disclosure tort in New Zealand law.

In the majority decision of Gault and Blanchard JJ, delivered by Gault J, his Honour described two main drivers for the adoption of the reasonable expectation of privacy test as the first element of the cause of action: (1) English law, which gave "a right of action in respect of the publication of personal information of which the subject has a reasonable expectation of privacy";[701] and (2) Canadian jurisprudence, where the rights against search and seizure, contained in s 8 of the Canadian Charter of Rights and Freedoms 1982 (Canadian Charter), have been interpreted to "include a right of a reasonable expectation of privacy in relation to governmental acts".[702] However, while Gault J articulated the first element of the test as "the existence of facts in respect of which there is a reasonable expectation of privacy", he also proceeded to treat the test as the same as a 'private facts' test.[703] However, it is generally recognised that the two tests are different and that the reasonable expectation test is wider than the private facts test.[704] For example, Panckhurt J in the Court of Appeal case of *Television New Zealand Ltd v Rogers* stated that:[705]

> … we are clear the tort is not confined to facts about private life; that is inherently private matters. Obviously inherently private facts will ordinarily attract a reasonable expectation of privacy. But so may facts which do not have an inherent quality of privacy.

---

[699] *L v G* [2002] NZAR 495 (DC) at 506. In *Hosking*, above n 8, at [84] Gault J noted that *L v G* may have been better dealt with as a breach of confidence claim.
[700] *Hosking*, above n 8, at [184].
[701] At [42]. The jurisprudence from England is discussed in Chapter 6(IV)(D) below.
[702] At [60]. See the Canadian Charter of Rights and Freedoms (Part I of the Constitution Act 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11), s 8.
[703] At [119]–[124]. Tobin, above n 386, at 98.
[704] Tobin, above n 386, at 97 also argues that the reasonable expectation test is potentially wider than the private facts test. A similar belief is held by John Burrows "Invasion of Privacy – *Hosking* and Beyond" (2006) NZ Law Review 389 at 392–394.
[705] *Rogers v Television New Zealand Ltd* [2007] 1 NZLR 156 (CA) at [59].

In determining what qualify as private facts, Gault J noted that private facts did not have to be secret facts. Private facts could be known to some, just not to the whole world.[706] He also said the identification of private facts will be analogous to the test of 'information with the necessary quality of confidence' under breach of confidence.[707] In addition, his Honour endorsed the words of Gleeson CJ in *Lenah Game Meats*, as follows:[708]

> There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private … Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand meant to be unobserved.

Tipping J, who delivered a separate judgment in *Hosking*, also endorsed the reasonable expectation of privacy test, noting that the necessary expectation "can arise from the nature of the information or material or the circumstances in which the defendant came into possession of it, or both."[709] He also believed that reasonable expectations of privacy will reflect "contemporary societal values" and that "the content of the law will in this respect be capable of accommodating changes in those values."[710]

Applying these tests to the facts of the case, all majority judges found that there was no reasonable expectation of privacy in the information. The fact that the children were on a public street, the photos displayed nothing more than what an observer on that street that day could have seen, and a certain amount of information about the children was already on the public record due to the celebrity nature of their parents weighed heavily with the judges.[711]

---

[706] *Hosking*, above n 8, at [119].
[707] Mark Warby, Adam Speker and David Hirst "Breach of Confidence" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 163 at [4.16] note that there is no "clearly established set of rules for determining whether any given type of information" has the necessary quality of confidence. However, generally they argue the information must be inaccessible and not in the public domain. Furthermore, they note that some classes of information are generally considered confidential, including information about health and medical treatment, a person's sex life, a person's appearance, and financial and business information (at [4.17]).
[708] *Hosking*, above n 8, at [119], citing *Lenah Game Meats*, above n 670.
[709] At [249].
[710] At [250].
[711] At [164]. See also at [260] where Tipping J provides his reasoning for why there is no reasonable expectation of privacy in this case.

Moreham argues that *Hosking* identifies a range of factors that will be relevant in determining whether there is a reasonable expectation of privacy, including: [712]

> The plaintiff's location, the nature of the activity depicted, public accessibility of the 'facts' which the photograph conveyed (which they said, were the existence of the twins, their age, and the fact that the parents were separated), and the plaintiff's particular attributes including the fact that they were children and that they had a celebrity parent.

After *Hosking*, the next case in the development of the disclosure tort was *Brown*. *Brown* involved the publication of a flyer by the Police which identified the plaintiff as a recently released paedophile, stated his name and address and included a photograph. The flyer was distributed in the suburban neighbourhood in which the plaintiff lived. The plaintiff brought an action for breach of privacy. In applying the *Hosking* test, the District Court Judge noted that the reasonable expectation test required "an assessment in the context of the existing circumstances."[713] In *Brown*, these circumstances included the lack of consent to use the photo for non-police business and the fact that the plaintiff was transitioning to a life outside prison.[714] The Judge also considered whether public facts would ever qualify to meet the reasonable expectation of privacy test.[715] The Judge rejected the position that once a fact is public it cannot become private over time *and* the contention from the plaintiff that the statutory environment indicated a trend to allow initially public facts to become private over time, favouring instead a straight-forward application of the reasonable expectation test.[716] To this end, his Honour stated in regard to conviction and sentence records: [717]

> … it cannot be said that they will remain public information forever. An example might be a prominent individual who, in his or her teenage years, was convicted say of possession of cannabis or of driving with an excess breath alcohol level. Thirty years of unblemished commitment to the community later, surely the passage of time and other relevant circumstances would operate such that there might well be a reasonable expectation that that information would remain private except only for the "legitimate public concern" defence.

---

[712] N A Moreham "Abandoning the 'High Offensiveness' Privacy Test" (2018) 4 Canadian Journal of Comparative and Contemporary Law 161 at 165.
[713] *Brown*, above n 391, at [71].
[714] At [71].
[715] At [61].
[716] At [64]. The plaintiff's argument referred to the Clean Slate Act and the restrictions on the public search of court records under s 71(4) of the Family Proceedings Act 1957.
[717] At [66].

In *Brown*, the plaintiff's conviction and sentence had "not come close to being contemplated as private information."[718] However, the Judge held that the flyer went further than simply mentioning information which was in the public domain, it included a photograph and his address, which the plaintiff would have a reasonable expectation of being private information.[719]

Following *Brown*, the next privacy case was *Andrews v Television New Zealand Ltd*, which involved the broadcast in a reality television show of an intimate conversation between a couple who had been involved in a car accident on a public road. Applying *Hosking*, the High Court had to decide if the plaintiffs had a reasonable expectation of privacy in the conversation. Ultimately, Allan J found that they did. Despite the fact the conversation would have been heard by those at the scene (approximately 30-odd people), the plaintiffs "had a legitimate expectation that there would be no additional publicity."[720] Central to this finding was that the conversation was of a private and intimate nature, the couple were filmed at close range for a considerable period of time without being aware of it, and the disclosure went considerably further than general news footage of an accident.[721]

Following *Andrews* was the difficult case of *Rogers v Television New Zealand Ltd*.[722] The three *Rogers* cases involved a taped murder confession Mr Rogers had made to the Police, which had been ruled inadmissible in his murder trial due to it having been obtained in breach of his rights. However, the defendant wanted to include the taped confession in a documentary about the murder. The High Court, and a majority in the Court of Appeal, found that the plaintiff had a reasonable expectation of privacy in the taped confession. These two courts found that while he had a reasonable expectation the confession would be used in the trial, he did not have a reasonable expectation it would be released to the media.

In discussing the reasonable expectation of privacy test, Panckhurst J in the Court of Appeal noted that the facts giving rise to a reasonable expectation of privacy must be judged at the time the publication occurs and that *Tucker* was authority for "the proposition that what were once public facts may, through the passage of time, become private."[723] Panckhurst J

[718] At [68]. At the time the flyer was distributed the plaintiff had recently been released from prison after serving 3 and a half years of a five year sentence.
[719] At [75].
[720] *Andrews v Television New Zealand Ltd* [2009] 1 NZLR 220 (HC) at [65]. The plaintiffs lost the case due to not satisfying the second element of the New Zealand disclosure tort cause of action.
[721] At [65].
[722] *Rogers v Television New Zealand Ltd* 22 CRNZ 668 (HC); *Rogers* (CA), above n 705 and *Rogers v Television New Zealand Ltd* [2007] NZSC 91, [2008] 2 NZLR 277 (SC). Tobin, above n 386, at 96 argues that cases are procedurally unsatisfactory and should have been argued in breach of confidence or defamation.
[723] *Rogers* (CA), above n 705, at [53].

recognised that this proposition had been strengthened by the passage of the Clean Slate Act. The Judge stated that:[724]

> … the passage of time and changed circumstances may influence the reasonable expectations held in relation to facts. And the transition may be from public to private, or vice versa. Similarly, facts that are public for one purpose (in this case Court proceedings) are not "public" for all purposes. Although information has been made known to others, a degree of privacy may remain.

In *Rogers*, the fact that it could not have been anticipated that the videotape would come into the possession of the media, that the videotape had been inadmissible at trial and that the plaintiff had been acquitted, all pointed to a reasonable expectation that the tape had become private.[725] However, it was found by the majority of the Court of Appeal that the privacy interest was at the low end of the scale.[726] In contrast, William Young P, in the minority in the Court of Appeal, doubted whether "an on-the-record confession to murder is sufficiently private or sufficiently personal to Mr Rogers to be legitimately within the scope of the tort."[727] For William Young P, what was expected at the time of confession was more relevant than what actually happened, and at the time of his confession Mr Rogers must have expected wide publicity of his confession.[728] However, despite this conclusion, William Young P did note that he was prepared to accept that the tort:[729]

> … is not necessarily confined to facts which are directly associated with the private life of the plaintiff. For instance, there are passages in *Hosking* which could suggest that 'public facts' about a plaintiff might become 'private' by reason of the effluxion of time … Further, I accept that expectations of privacy may have a conditional quality so that certain types of publicity may be expected but not other types.

By the time of *Rogers,* the *Hosking* reasonable expectation test had become well established. Since then, several privacy cases have applied the test to a range of fact scenarios, none of which involve once public facts, although some do involve public information in the form of criminal charges. In 2012, in *Clague v APN News and Media Ltd,* the principal of a well-respected private school brought a claim for breach of privacy for the publication of information regarding a Police investigation into an allegation of domestic assault. In

[724] At [54].
[725] At [56]–[57].
[726] At [59].
[727] At [124].
[728] At [124].
[729] At [123]. See *Hosking*, above n 8 at [69] and [105].

dismissing the plaintiff's claim, Toogood J concluded that a principal of a high-profile high school could have no reasonable expectation of privacy regarding information that the Police were investigating an allegation of assault against him. While the Judge has not been forthcoming about the basis on which the conclusion rests, it appears to be a combination of the nature of the charge and the fact that the plaintiff's role made him somewhat of a public figure.[730]

In *Driver v Radio New Zealand Limited* the High Court had to consider if the plaintiff had a reasonable expectation of privacy in information of her arrest and detention in India, which had been published by the defendant in New Zealand.[731] In discussing the reasonable expectation of privacy test, Clark J noted that it was contextual, requiring consideration of the particular circumstances, the nature of the information and the nature of the invasion itself.[732] Clark J also identified the need to consider contemporary standards of morals and behaviour and noted the risk that incorporating such standards into the test may result in retrograde developments in society also being incorporated into the test.[733] To guard against this risk, Clark J said the test must consider a normative component of how society *should* treat privacy interests in a particular case. For Clark J, therefore, "the contemporary standards of behaviour must be cross-checked against a minimum standard of privacy."[734]

In applying the law to the case at hand, Clark J noted that it was possible for there to be an expectation of privacy in the fact of arrest and that the seriousness of the offence would be a relevant factor, noting that: "Many New Zealanders are likely to be perturbed by having their arrest for a low-level offence publicised on the evening news."[735] This expectation of privacy was supported by the media's general practice of refraining from identifying alleged offenders before being charged and the hurt and distress caused by the stigma of a criminal

[730] *Clague v APN News and Media Ltd* [2012] NZHC 2898, [2013] NZAR 99 at [37]. The Judge noted that the defence counsels' argument that the plaintiff was a person in which the public had a legitimate interest was persuasive (at [31]). However, if this argument was persuasive, it should have been a factor at the defence stage not at the reasonable expectation of privacy stage. See also Clark J's summation of the decision in *Driver*, above n 432, at [89].
[731] *Driver*, above n 432. The Plaintiff also claimed a breach of privacy for the broadcast of footage recorded when the Indian Police arrested her at her hotel room. Clark J found that this claim followed the publication claim and, in fact, presented a stronger expectation of privacy (at [140]). Two years after her arrest in India, the plaintiff was acquitted of all charges.
[732] The factors derived from the English case of *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch 481.
[733] Clark J referred to Moreham, above n 454 and Winkelmann CJ, above n 342, when discussing this risk of retrograde development. See the discussion in Chapter 6(V)(A) below.
[734] *Driver*, above n 432, at [96].
[735] At [101].

investigation.[736] However, other factors told against an expectation of privacy, including the Police using publicity to locate a suspect or wanting corroborating evidence and the public's legitimate interest in knowing about serious criminal activity. [737] While Clark J found that if the plaintiff had been subject to a police investigation in New Zealand, she would have had a reasonable expectation of privacy, the plaintiff was not subject to investigation in New Zealand. The plaintiff had been arrested in India and India's criminal process is substantially different and more open and public than in New Zealand. Furthermore, the case had received considerable publicity in India. The issue, therefore, became whether these factors affected the plaintiff's reasonable expectation of privacy. Ultimately, the Court found they did not. Clark J recognised that an invasion of privacy:[738]

> … can occur when publicity given to private information is increased by an order of magnitude. Local news reporting on an internal workplace matter or national media attention given to an article in a student magazine could be examples. Another example might be international media attention given to the domestic news of another country, as happened here.

Clark J held that the defendant should not have "coat-tailed" off the overseas publicity, when that publicity in New Zealand would constitute an invasion of privacy had the arrest occurred in New Zealand.[739]

In the same year as *Driver*, the High Court, in *Henderson v Walker*, had to consider whether the disclosure of various documents to the Inland Revenue Department, the office of the Official Assignee, the Police, lawyers and private individuals by the defendant, who was the liquidator of companies associated with the plaintiff, was an invasion of privacy. It is noteworthy that the case involves a non-media defendant. However, the High Court had no issue using the tort in such circumstances, with Thomas J noting that: "I am satisfied that providing private information to third parties without authorisation is the kind of conduct that the privacy tort should encompass."[740]

---

[736] At [103]–[114]. Clark J also noted the differences between the arrest processes in India and New Zealand, highlighting that in New Zealand Mrs Driver would not have been arrested because at the time of her arrest the Indian Police were still conducting the investigation into her activities.
[737] At [103].
[738] At [128].
[739] At [128].
[740] *Henderson v Walker* [2019] NZHC 2184 at [217]. In a later case involving the same broad fact scenario, but with a different plaintiff, Thomas J also found that the disclosure of personal emails satisfied the 'reasonable expectation of privacy' test. See *Hyndman v Walker* [2019] NZHC 2188 at [94].

In discussing the reasonable expectation of privacy test, Thomas J noted that the test essentially requires private facts, which in turn requires consideration of contemporary standards of morals and behaviour, as set out by Gleeson CJ in *Lenah Game Meats*.[741] However, like Clark J, Thomas J also referred to concerns over incorporating into the test retrograde developments in society, and, therefore, the need to consider the "minimum standards needed to secure the community and individual benefits of privacy."[742] In the case at hand, Thomas J found that the plaintiff had a reasonable expectation of privacy in a range of personal emails between the plaintiff, his wife and friends. These emails related to personal matters like marriage issues, health and medical matters, and photographs of family and friends, as well as legally privileged and business matters unrelated to the defendant's activities.[743]

In *Peters v Bennett*, the High Court had to consider whether politician and then Deputy Prime Minister, Winston Peters, had a reasonable expectation of privacy in the fact that he had been overpaid New Zealand Superannuation by the Ministry of Social Development (MSD) and was the subject of an investigation by MSD.[744] Ultimately, the Court held that these were facts which Mr Peters' could reasonably expect not to be disclosed wider than to those who had a proper purpose in knowing them (for example, MSD staff and management who were dealing with the issue). It is noteworthy, that the Court dismissed the argument that because Mr Peter's is a public figure his reasonable expectations were less. The Judge noted that the information did not have a "realistic impact on his character or fitness for public office" [745] and, despite his public status, Mr Peters actively sought to protect his privacy and personal life.

It is clear from the above that the reasonable expectation test is highly circumstantial. The cases provide a laundry list of factors that the courts have considered in assessing if the test is met: the nature of the activity; the location of the plaintiff; attributes of the plaintiff (for example, whether they are a public figure); the passage of time and changed circumstances; previous publicity (which is not necessarily fatal) and its extent; and the circumstances surrounding the alleged invasion (for example, plaintiff's consent). However, it is also clear that there has been a relatively broad and nuanced approach to what facts can be reasonably expected to be private. The test is broader than just inherently private and intimate

[741] *Henderson v Walker*, above n 740, at [200].
[742] At [202], citing Winkelmann CJ, above n 342, at 19.
[743] *Henderson v Walker*, above n 740, at [221], [222] and [41].
[744] *Peters v Bennett* [2020] NZHC 761.
[745] At [115]–[116].

information. The test has been held to cover facts that occurred in public, facts about public officials, facts about accused or convicted persons, a taped murder confession and facts which have had a degree of public exposure. There has been clear recognition for once public facts within the test. The Court in *Tucker* saw the possibility of privacy in historical criminal convictions. In *Brown,* the District Court thought that the passage of time and rehabilitation could foster a reasonable expectation of privacy in historic bad behaviour. Similarly, the Court of Appeal in *Rogers* held that passage of time and changed circumstances could affect expectations of privacy. As a result of this analysis, the present research contends that disclosure of once public facts can, in appropriate circumstances, sustain a reasonable expectation of privacy, and that this conclusion is consistent with the development of the disclosure tort.[746]

B The Broadcasting Standards Authority

The reasonable expectation test has not just been the preserve of the disclosure tort. The test has played a key role in the decisions of the BSA, which investigates complaints against broadcasters for breaches of privacy. Section 4 of the Broadcasting Act 1989 requires every broadcaster to maintain standards which are consistent with the privacy of the individual.[747] To encourage compliance with this obligation, the BSA has established codes of practice and guidance, the most recent of which is the "Broadcasting Standards in New Zealand Codebook for Radio, Free-to-Air Television (FTA TV) and Pay Television".[748] The Codebook sets out standards for the three broadcasting mediums, each of which includes the same privacy standards and guidance. As an example, the privacy standard for FTA TV states as follows:[749]

> 10(c) There must be a *reasonable expectation of privacy* in relation to the information or material disclosed. Factors to consider, but are not limited to, whether the information or material is not in the public domain, and/or is intimate or sensitive in nature; and/or the individual could reasonably expect it would not be disclosed.
>
> 10(d) A person will not usually have a reasonable expectation of privacy in relation to matters in the public domain. In some circumstances, there may be a reasonable

[746] See also Tobin, above n 386, at 99–100.
[747] Broadcasting Act 1989, s 4.
[748] Section 21(1)(e)(vii). Broadcasting Standards Authority [BSA] *Broadcasting Standards in New Zealand Codebook for Radio, Free-to-Air Television* (2016). The Codebook took effect on 1 April 2016. See Rosemary Tobin "Media Regulation: The Press Council and the Broadcasting Standards Authority" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 243 at 251–254 for a discussion of the history of the BSA privacy principles and guidelines.
[749] *BSA Codebook*, above n 748, at 41 (emphasis added).

> expectation of privacy in relation to such information or material even though it is in the public domain.

While the BSA Codebook uses the reasonable expectation test, it has been argued that its requirements "can encompass a wider spectrum of behaviour than that of the tort."[750] In particular, in 2015, Cheer noted that the BSA's privacy principles (as they were called then) could cover "harassment by disclosure of past events, even though the common law tort of privacy at that stage might not."[751] In 2015, the BSA privacy principles were different from the current standards. The principles stated that:[752]

> It is inconsistent with an individual's privacy to allow the public disclosure of some kinds of public facts. The "public" facts contemplated concern events (such as criminal behaviour) which have, in effect, become private again, for example through the passage of time. Nevertheless, the public disclosure of public facts will have to be highly offensive to an objective reasonable person.

The explicit recognition of once public facts was removed from the BSA privacy standards in 2016. However, the existing standards have not completely closed the door on once public facts. The recognition in the standard that there can be a reasonable expectation of privacy in some public domain information, combined with a lack of guidance in the Codebook of what public information will sustain a reasonable expectation of privacy, arguably leaves room for the cases decided under the previous standard to still have some influence.[753] These decisions demonstrate that some once public facts have been considered private. In *Drury v TV3 Network Services Ltd* facts about a sexual misconduct allegation 12 years previously were held to be public facts which had become private facts again due to the passage of time.[754] In *MM v TV3 Network Services Ltd*, a six-year-old conviction for assault was held to have become private again due to the relatively minor nature of the conviction and the passage of years since the conviction was entered.[755]

However, not all once public facts have been found to become private. In *Anne Baker (2) v Television New Zealand Ltd* an event which occurred 57 years ago was held not to have

[750] Tobin, above n 748, at 258. See also Cheer, above n 392, at 378.
[751] Cheer, above n 392, at 378.
[752] The privacy principles applicable in 2015 were issued by the BSA on 1 August 2006. See Tobin, above n 748, at 214 for the principles applicable before 2016.
[753] It appears that the issue of once public facts has not come before the BSA since the Codebook was introduced in 2016. In such a circumstance it is not unreasonable for the BSA to consider its decisions under the previous principles, especially considering the wording of standard 10(d).
[754] *Drury v TV3 Network Services Ltd* 10/10/96, BSA Decision Nos 130-96, 131-96 and 132-96.
[755] *MM v TV3 Network Services Ltd* 15/07/99, Decision Nos 1999-103, 1999-104.

regained its privacy due to "ongoing interest" in the matter.[756] In *Devereux v Television New Zealand Ltd* a "well-known, serious and tragic event in New Zealand [that was] widely reported at the time" was held not to have become private again despite 17 years having passed since it occurred.[757] In *Arthur v Television New Zealand Ltd*, the facts that the complainant had been convicted of supplying the drug P and that he was a teacher meant that three years was not enough for his conviction to become private again.[758] In *Reekie v Television New Zealand Ltd* a conviction 16 years old was held not to have regained its private status due to the serious nature of the offences and the fact that more recent offending had put the earlier convictions back in the public arena.[759] What is relevant, therefore, from a BSA perspective has been the nature of the facts in question, the passage of time, the public's right to know, and, if a criminal conviction is involved, the seriousness of the conviction.

The BSA's approach to once public facts has been welcomed, although some have argued that the policy under the Clean Slate Act needs to be considered more by the BSA when criminal convictions are at issue.[760] Tobin argues, for example, that the Clean Slate Act would provide the BSA with a "good guide both the period that need elapse before a public fact might become private, and also for the types of public fact that can become private."[761]

III Highly Offensive

A Common Law

The second element of the test for the disclosure tort relates to the publicity rather than whether the facts themselves are private and asks whether that publicity would be considered

[756] *Anne Baker (2) v Television New Zealand Ltd* 12/12/96, Decision Nos 1996-170, 1996-171. The event was the body snatching of a dead man with the intent of a faking a death for insurance purposes.
[757] *Devereux v Television New Zealand Ltd* 25/08/15, BSA Decision Nos 2015-027 at [11]. Unsurprisingly, shorter timeframes have been held to be not long enough for public information to regain privacy. In *Television New Zealand Ltd v Walden* 19/9/06, Decision No 2006-061, 13 months between the event – being forcibly ejected from a stadium by police and security staff – and the broadcast was held not to be sufficient time for a public fact to regain its privacy. In *T v Television New Zealand Ltd* 1/10/98, BSA Decision No 1998-119 it was held that one year was not enough time for public facts about T's conviction for fraud against the student loan scheme to become private.
[758] *Arthur v Television New Zealand Ltd* 22/02/07, BSA Decision No 2006-115.
[759] *Reekie v Television New Zealand Ltd,* above n 390. The recent serious offending, rape, was also held not to have become private after five or six years. See also *Reekie v Television New Zealand Ltd* HC Auckland CIV-2009-404-003728, 8 February 2010 at [53].
[760] Dr Nicole Moreham "Private Matters: A Review of the Privacy Decisions of the Broadcasting Standards Authority" December , BSA <www.bsa.govt.nz> 7.
[761] Tobin, above n 748, at 260.

highly offensive to an objective reasonable person.[762] The test exists to ensure that the tort does not become weighted down with trivial claims. As Gault J in *Hosking* stated:[763]

> … publicity, even extensive publicity, of matters which, although private, are not really sensitive should not give rise to legal liability. The concern is with publicity that is truly humiliating and distressful or otherwise harmful to the individual concerned. The right of action, therefore, should be only in respect of publicity determined objectively, by reference to its extent and nature, to be offensive by causing real hurt or harm.

The test is an objective one. An objective person in the shoes of the plaintiff must consider the publication highly offensive.[764] Moreham argues that there were three main inspirations for the adoption of the test in *Hosking*: (1) the United States disclosure tort, which requires offensiveness for the invasion of privacy to be actionable; (2) the words of Gleeson CJ in *Lenah Game Meats*, who noted that: "The requirement that disclosure … would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private";[765] and (3) the English Court of Appeal's use of the test in *Campbell*.[766]

The first real discussion of the test in New Zealand came in *Bradley*, which also contains one of the more fulsome applications of the test, even though the discussion was not necessary because the Judge had previously found there were no private facts. In discussing whether the element was satisfied, the Judge noted that very little in the film directly reflects on the tombstone and certainly nothing unpleasant. The tombstone was only part of the general background of the cemetery, it was shown for a short period of time, it was not shown in full, and it was impossible to identify a name upon it. Therefore, the test was not satisfied. The Judge did note, however, that had the tombstone been more actively part of the film – "if for example the clergyman had been impaled upon it or the zombie had been seen to appear out of it" – then the situation may have been different.[767]

Offensiveness was also an important consideration in *P v D*. Nicholson J noted that the "increasingly enlightened public attitude" towards mental illness meant that publication of information about being treated in a psychiatric hospital may not be the source of

---

[762] *Hosking*, above n 8, at [127].
[763] At [126].
[764] See Tobin, above n 386, at 103–104.
[765] *Lenah Game Meats*, above n 670, at [41].
[766] Moreham, above n 712, at 166. The House of Lords decision in *Campbell*, above n 355, abandoned the highly offensive test.
[767] *Bradley*, above n 693, at 424–425.

embarrassment or upset that it once was.[768] However, despite making this statement, he ultimately concluded that it was an "idealistic point of view" which did not adequately account for the "value which people place on having intimate information such as their medical treatment kept private."[769] Therefore publication of this information was, just, highly offensive. However, Nicholson J did note that information that the Police had come to a person's aid over an emergency medical situation would *not* be highly offensive to a reasonable person on its own. This conclusion was driven by the fact that the statement about Police aid could relate to a wide range of, presumably inoffensive, reasons, like the "giving of emergency medical aid to hapless road accident victims."[770]

In *L v G,* the District Court Judge had issues applying the reasonable person standard to an extraordinary situation – a plaintiff who was a prostitute and who had consented to intimate photos being taken. A similar difficulty was experienced in *Brown,* where the Judge noted that:[771]

> The "man in the street", who is not a paedophile, might well consider that the publication of private details, relating to the residence and identity of a convicted paedophile, is not inherently offensive.

However, Judge Spear notes that the test is not the objective reasonable paedophile, but "a reasonable person in the shoes of the person that the publication is about".[772] Therefore, the Judge stated that he was "just able" to find the test satisfied.[773] Similarly, in *L v* G, the Judge was able to find that the test was satisfied on the facts, presumably because most reasonable persons, even in the shoes of a prostitute, would find it highly offensive to have intimate photos taken for private purposes published in an adult magazine.[774]

In *Hosking*, like in *Bradley*, the highly offensive element was not strictly required to be considered, because the first element was not satisfied. Gault J did note, however, that he was "not convinced" that the publication of the photos met the test, even considering young children were involved.[775] In contrast, Tipping J doubted that the test was even needed. While recognising the test was an aspect of United States jurisprudence, he noted: "I would myself

[768] *P v D*, above n 696, at [37].
[769] At [37].
[770] At [41].
[771] *Brown*, above n 391, at [80].
[772] At [81], citing *P v D*, above n 696, at [39].
[773] *Brown*, above n 391, at [81].
[774] *L v G*, above n 699, at 509–510.
[775] *Hosking*, above n 8, at [168].

prefer that the question of offensiveness be controlled within the need for there to be a reasonable expectation of privacy."[776] His Honour preferred that the level of offensiveness required was substantial rather than high, envisaging times when the high level might be too restrictive.[777]

In *Andrews*, Allan J noted that the highly offensive test was a high hurdle to pass. He held that the manner of disclosure was relevant, so the extent and tone of a publication might make it highly offensive.[778] In the case at hand, his Honour found the disclosure did not meet the test because the plaintiffs were not shown in a bad light by the broadcast and there was nothing humiliating, embarrassing or offensive in the broadcast. In *Rogers*, Winkelmann and Venning JJ in the High Court, held that the offensiveness test required consideration of the context of the publication and the publication's likely impact.[779] In the case itself, the fact that the screening of the confession would raise doubt about the jury's decision, the plaintiff had not had an opportunity to meet the evidence at trial, and it had been obtained in breach of his rights, led the Judges to find the test satisfied.[780] In the Court of Appeal, the majority were not persuaded that the High Court decision on offensiveness was wrong.[781]

In contrast, William Young P, like Tipping J in *Hosking*, doubted the usefulness of the test, stating that it and the reasonable expectation test are "interconnected".[782] He noted that:[783]

> In most cases it will be the defeating of a reasonable expectation of privacy which makes publication objectionable, and likewise if publicity could fairly be seen as objectionable that might well suggest that there was a reasonable expectation of privacy in relation to the information in question.

Similarly, in the Supreme Court *Rogers* decision, Elias CJ doubted the application of the test, arguing that the Court should "reserve its position" on the test because the House of Lords in *Campbell* had doubted the test.[784]

---

[776] At [256].
[777] At [256].
[778] *Andrews*, above n 720, at [51], citing *Rogers* (CA), above n 705, at [68].
[779] *Rogers* (HC), above n 722, at [54].
[780] At [60]. The majority of the Court of Appeal upheld the High Court finding. The Supreme Court did not need to consider this question of offensiveness because the reasonable expectation test had not been met.
[781] *Rogers* (CA), above n 705, at [69].
[782] At [69]
[783] At [122]. William Young P did not have to apply the highly offensive test because he had found that there was no reasonable expectation of privacy on the facts at issue.
[784] *Rogers* (SC), above n 722, at [25].

In *Clague,* the Judge noted that while it might be embarrassing for the plaintiff to have the information publicised and distressing to him and his family, it did not reach the threshold of the highly offensive test. It is difficult, however, to reconcile that finding with the words of Gault J, who said that the tort was concerned with publicity that "is truly humiliating and distressful or otherwise harmful to the individual."[785] In the Judge's own words in *Clague*, the publicity would be embarrassing and harmful to the plaintiff and his family.

In *Henderson v Walker*, Thomas J noted the controversy surrounding the test, but applied it nonetheless because it was still good law. Thomas J noted that the relevant considerations were the nature of the information, the circumstances and extent of publication, and the relationship between the parties.[786] Applying the test to the facts of the case, Thomas J found that where the disclosures involved "a limited amount of information, which was innocuous in nature, and were to a limited number of people" they were not highly offensive.[787] However, where the disclosures involved highly personal information, large volumes of documents, a breach of confidence, and were knowingly made by a defendant who acted in a way that was "cavalier (and arguably malicious)" to the plaintiff's privacy, then the disclosures met the test.[788] In the Court of Appeal case of *Hyndman v Walker*, Miller J noted that, while "disclosure to a small class" of persons may be able to sustain a claim that disclosure was highly offensive, the "broader publicity and the less prior knowledge in the audience, the more like it is that disclosure will be highly offensive."[789] In that case the disclosure was to a very small number of people only, who had prior knowledge, therefore disclosure was not highly offensive.[790] In *Driver*, the Judge followed the approach of Thomas J, and found the test satisfied because of the national nature of the coverage, its coverage over a two-day cycle, the seriousness of the allegations and the likelihood of causing distress.[791]

From the case law, several factors can be identified for assessing whether the test has been met. Unlike the reasonable expectation test, the list is not a long one and focuses predominantly on the nature of the information and the circumstances of publication. The latter include the extent and tone of publication, as well as the nature of the disclosure and even the actions of the defendant, for example, whether or not they have breached a

[785] *Hosking*, above n 8, at [128].
[786] *Henderson v Walker*, above n 740, at [97].
[787] At [234].
[788] At [240].
[789] *Hyndman v Walker* [2021] NZCA 25 at [50].
[790] At [50]. The Judge also noted that the plaintiff did not provide any evidence of distress regarding the disclosure complained of, rather his distress was at the whole situation he was involved in with the defendant (at [52]).
[791] *Driver*, above n 432, at [138].

relationship of confidence. The overarching position is that the test is a high one, which is focused on publicity that is truly humiliating and distressful. Furthermore, the test has been subject to some judicial doubt. For the purposes of the present research, it must also be noted that there has been no judicial consideration of once public facts from an offensiveness perspective.

B Broadcasting Standards Authority

The highly offensive test is also part of the BSA privacy standard. The Codebook states:[792]

> 10(b) Broadcasters should not disclose private information or material about an individual in a way that is highly offensive to an objective reasonable person in the position of the person affected.

Like the tort test, the cl 10(b) test is objective and is considered a high standard.[793] What is offensive has been held to be something that is "hurtful, harmful, injurious", and which is more than something that is merely "displeasing, annoying, insulting".[794] Unlike the courts, however, the BSA has considered some lapse of time situations. In *Lewis v TVNZ,* the BSA considered whether the disclosure, after two years, of information that a person had been caught with a small amount of undersized paua and issued with a $250 fine was a breach of privacy. While the Authority made no determination of whether there was a private fact, it did find that such a disclosure was not highly offensive. The Authority noted offensiveness was a high threshold and that the information at issue was not of the type which had been found offensive in the past – for example, that a person had been sexually abused, was mentally ill, and had tried to commit suicide.[795] In contrast, in *TJ v Television New Zealand Ltd* the Authority found that the lapse of eight years since an act was filmed, and the fact it was repeatedly broadcast, against the complainant's wishes, as part of the opening sequence to a television show, contributed to the privacy intrusion being considered highly offensive.[796]

The disclosure tort in New Zealand, therefore, requires facts in respect of which there is a reasonable expectation of privacy and publicity that is highly offensive to an objective

---

[792] *BSA Codebook*, above n 748, at 41.
[793] See *TVNZ v KW* HC Auckland CIV-2007-485-1609, 18 December 2008 at [38]. See *MA v TVNZ Ltd*, 22/02/11, BSA Decision No 2010-084 at [38] for a discussion of the objective test.
[794] *TVNZ v KW*, above n 793, at [68].
[795] *Lewis v TVNZ* 12/02/08, BSA Decision No 2007-109 at [23].
[796] *TJ v Television New Zealand Ltd* 17/06/04, BSA Decision No 2013-092 at [23]–[24]. The fact the complainant did not wish to participate in the television programme, and had contacted the production company at least twice to complain about the use of his image, was also a contributing factor to the claim being considered highly offensive.

reasonable person. It has been seen that a range of factors are relevant in meeting both tests, and that these factors are highly contextual and fact specific. Before moving onto critiques and clarifications of these tests, it is useful to put the New Zealand test into context by considering the application of the reasonable expectation test in other jurisdictions. Considering other jurisdictions is important because the development of the disclosure tort in New Zealand has been influenced by the development of the cause of action in other jurisdictions. Furthermore, how these jurisdictions have continued to develop their tests is valuable information when it comes to assessing what, if any, amendments are required to New Zealand's disclosure tort. The next section, therefore, considers the disclosure tort in the United States, Canada, Australia and England.

IV Disclosure Tort in Comparative Jurisdictions

A United States

Tort law in the United States protects invasions of privacy under four distinct causes of action: the public disclosure of private facts; interference with seclusion and solitude; publicity that places a person in a false light; and appropriation of another's name or likeness. This classification derives from the work of Prosser in 1960, who surveyed over 300 decided cases to determine that the tort was "not one tort, but a complex of four".[797] Prosser's classification was adopted by the American Law Institute's *Restatement (Second) of Torts,*[798] has been accepted in most states[799] and is now "the foundation of modern tort privacy" in the United States.[800] Section 652D of the *Restatement* sets out the cause of action for the disclosure tort as follows:[801]

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that:
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.

The cause of action requires the plaintiff to prove four separate elements to succeed: (1) public disclosure; (2) of private facts; (3) where the disclosure would be offensive and

[797] William Prosser "Privacy" (1960) 48 Cal L Rev 383 at 389.
[798] *Restatement*, above n 210, at § 652.
[799] Law Commission, above n 655, at [4.8].
[800] Neil M Richards "The Limits of Tort Privacy" (2011) 9 J on Telecomm & High Tech L 357 at 364.
[801] *Restatement*, above n 210, at § 652D.

objectionable to a reasonable person of ordinary sensibilities; and (4) the disclosure is not of legitimate public concern.

Central to the cause of action is the existence of private facts. In the United States, what is a private fact relies heavily on a "definitional bifurcation" between private and public.[802] Private facts are typically intimate or highly personal facts, including facts about "sexual relations … family quarrels, many unpleasant or disgraceful or humiliating illnesses, most intimate letters, most details of a [persons] life in [their] home".[803] For McNulty, a focus on intimate matters not only provides definitional clarity but also "gives meaning and substance to the offensiveness element of the tort in that only the most serious transgressions of privacy are deemed worthy of remedy."[804] Clearly excluded from private facts are those that are sourced from or located in the public prior to the disclosure complained of.[805] This exclusion applies to matters on the public record.

The clear exclusion of matters on the public record was seen in the case of *Cox Broadcasting Corp v Cohn. Cox* involved publication of the name of a rape and murder victim in contravention of a state law that made such publication an offence.[806] However, the Supreme Court of the United States found in favour of the publisher because the name had been obtained from court documents during the murder trial. Relying on the fact that the information at issue was part of the public record, Justice White stated:[807]

> Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business.

It does not matter if the public record is in the dusty bowels of a courthouse or other public archive, or if the record was made public accidentally;[808] provided that the record is open to

---

[802] Chris D L Hunt "Reasonable Expectations of Privacy in Canadian Tort Law" in Margaret I Hall (ed) *The Canadian Law of Obligations: Private Law for the 21st Century and Beyond* (LexisNexis Canada Inc, Toronto, 2018) 269 at 288. See also Patrick J McNulty "The Public Disclosure of Private Facts: There is Life after *Florida Star*" (2001) 50 Drave L Rev 93 at 102.
[803] *Restatement*, above n 210, at § 652D cmt b. See also McNulty, above n 802, at 104.
[804] McNulty, above n 802, at 104.
[805] At 134.
[806] *Cox Broadcasting Corp v Cohn* 420 US 469 (1975).
[807] At 495. The United States Constitution, amend 1 protects freedom of expression. The United States Constitution, amend 14 requires that no state shall "deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws".
[808] *Florida Star*, above n 229, at 458.

public inspection it will be considered a public record.[809] However, if the public record is not open to public inspection, like income tax returns, it is not public.[810]

There is generally no liability, also, if a person gives further publicity to matters already made public.[811] In *Moreno v Hanford Sentinel Inc*, for example, because the plaintiff had put the information complained of on her publicly accessible MySpace page, further publication of the same information in a local newspaper was held not to breach her privacy.[812] However, Strahilevitz notes that there is room for what he calls "limited" privacy, especially where the initial publicity does not involve the media.[813] He notes that limited privacy is:[814]

> … the idea that when an individual reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further.

Limited privacy was seen in *YG v Jewish Hospital* and *Multimedia WMAZ v Kubach*. In the former, the Court found that a couple who had participated in an IVF programme had not waived their right to privacy by attending a limited gathering with other participants of the programme.[815] In the latter, the Court found that the plaintiff's disclosure of his HIV status to friends and family did not waive his expectation of privacy regarding wider publication of his condition.[816]

The cases of *Melvin v Reid* and *Briscoe* might suggest that in the United States some once public facts are capable of being considered private facts. However, *Cox* has led to the findings in these cases being overruled.[817] The general position is that the lapse of time does not make private that which was public.[818] However, the *Restatement* does note that a person's past history which they would prefer to forget *might* support a claim for private facts. It states that: "When these intimate details of his life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy".[819] One such case was *Roshto v Hebert*, where the Supreme Court of Louisiana

---

[809] An example of this approach can be seen in *Uranga*, above n 450.
[810] *Restatement*, above n 210, at § 652D cmt b.
[811] At § 652D, para b.
[812] *Moreno v. Hanford Sentinel Inc* 172 Cal App 4th 1125 (2009).
[813] Lior Jacob Strahilevitz "A Social Networks Theory of Privacy" (2005) 72 U Chi L Rev 919 at 939.
[814] At 939.
[815] *YG*, above n 259, at 502.
[816] *Multimedia WMAZ v Kubach* 443 SE 2d 491 (Ga App 1994).
[817] See *Gates v Discovery Communications Inc* 101 P 3d 552 (Cal 2004) at 559.
[818] *Restatement*, above n 210, at § 652D cmt k. See also Jonathan B Mintz "The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain" (1996) 55 Md L Rev 425 at 447.
[819] *Restatement*, above n 210, at § 652D(b).

found that the reproduction of a 25-year old article which described the details of criminal convictions for which the plaintiffs were subsequently pardoned was an invasion of privacy because of the lapse of time involved (25 years).[820] The Judge noted that:[821]

> … when a person convicted of a crime has served his sentence, changed his name, moved to a faraway city, concealed his identity, and led an obscure, respectable and useful life for 20 years, a newspaper reporter who institutes an investigation of the little-known citizen's past history and reveals the conviction in a newspaper published in the citizen's new community (far from the site of the crime), the reporter possibly may be liable for damages for invasion of privacy, even though the information is true and is contained in the public records.

However, findings of this nature in the United States are rare.

It has been argued that not only has *Cox*, and similar Supreme Court cases like *Smith v Daily Mail Publishing Co*[822] and *Florida Star v BJF,*[823] dealt an almost fatal blow to once public facts in the United States, it has also "laid to rest" the entire disclosure tort.[824] However, not all agree with this argument. Jurata points to the fact that the Supreme Court in *Florida Star* "expressly rejected the newspaper's claim that the press could never be held liable for publishing the truth."[825] McNulty also argues that "reports of the demise of the public disclosure action have been exaggerated", noting that the decisions only apply where the private facts have been released to the public domain by the government.[826] For McNulty, the future of the disclosure tort lies in private facts, unlawfully obtained from private sources, where the disclosure is made to a small or limited audience by a non-media defendant.[827]

---

[820] *Roshto v Hebert* 439 So 2d 428 (La 1983).
[821] At 431.
[822] *Smith v Daily Mail Publishing Co* 443 US 97 (1979). In this case, the newspaper had obtained from persons present at the scene of a shooting, shortly after it happened, the name of the 14 year old student who had allegedly shot and killed a classmate. The newspaper published the name of the student despite a West Virginia statute making it a crime for a newspaper to publish the name of any youth charged as a juvenile offender, without the written approval of the juvenile court. The Supreme Court held that the statute violated the United States Constitution.
[823] *Florida Star*, above n 229. In this case, the newspaper published the name of a rape victim who had filed a report with her local sheriff's department. The newspaper had obtained the victim's name from the sheriff department's report of the incident which had been placed in the sheriff department's pressroom. The rape victim sued the newspaper for negligent violation of a Florida statue which made it unlawful to publish the name of any victim of a sexual offence. The Supreme Court found in favour of the newspaper on the basis of its decision in *Smith v Daily Mail*.
[824] McClurg, above n 252, at 1002. McClurg cites the minority decision of Justice White in *Florida Star* who argued that the majority decision essentially obliterated the disclosure tort in the United States. See *Florida Star*, above n 229, at 550.
[825] John A Jurata Jr "The Tort that Refuses to Go Away: The Subtle Re-emergence of Public Disclosure of Private Facts" (1999) 36 San Diego L Rev 489 at 501.
[826] McNulty, above n 802, at 98.
[827] At 131–142 and 151–157.

However, while McNulty's conclusion might leave theoretical room for the disclosure tort, practically it is very narrow.

As a result of the use of the phrase 'private life' in the *Restatement*, the United States jurisprudence has considerably less discussion about reasonable expectations of privacy. However, where reasonable expectations of privacy are discussed, it is not as a test, rather, as an overarching state which is established if the tort test is satisfied.[828] In California, for example, art 1(1) of its Constitution provides that all persons have a right to privacy.[829] To establish whether that right has been violated the plaintiff must prove a legally protected privacy interest, a reasonable expectation of privacy under the circumstances and a serious invasion of the privacy interest.[830] However, in practice, the application of the reasonable expectation test is still linked to the tort test. Therefore, for an invasion of privacy by public disclosure of private facts, the elements of the disclosure tort must be established in order to determine whether the constitutional test has been satisfied. This approach was seen in *Moreno*, where the Court held that posting information on publicly accessible MySpace pages was not private, and therefore the plaintiff could not establish a reasonable expectation of privacy in information published on such pages.[831] This approach has led some commentators to argue that in California "privacy tort law and constitutional privacy law have essentially merged."[832]

The highly offensive element of the disclosure tort test appears to have been the subject of little scholarly or judicial discussion in the United States. This gap likely reflects the fact that most cases fall at the question of whether there are private facts, and even if there are facts, most cases find that there was legitimate public concern in the publication.[833] Penk notes that in almost 90 per cent of intrusion cases the defendant prevails and the numbers are *greater* for disclosure cases.[834] This outcome is driven predominantly by the strength of the constitutional protection for freedom of expression, which commonly overrides a person's complaint of invasion of privacy. While free speech is discussed in the next chapter, its tentacles are seen

[828] See, for example, Bryce Clayton Newell "Rethinking Reasonable Expectations of Privacy in Online Social Networks" (2011) 12 Rich J L & Tech 12 at 12 and Strahilevitz, above n 813, at 920–921. Strahilevitz essentially treats the two tests as interchangeable.
[829] California Constitution, art I, s 1. For a discussion of the California constitutional right to privacy see *Hill v. National Collegiate Athletic Assn* P 2d 633 (Cal 1994) at 641.
[830] *Hill*, above n 829, at 652.
[831] *Moreno*, above n 812, at 1129. See also Newell, above n 828, at 13.
[832] Lior Jacob Strahilevitz "Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Reunifying Privacy Law" (2010) 98 Cal L Rev 2007 at 2044, citing *Hernandez v. Hillsides Inc* 211 P 3d 1063 (Cal 2009) at 1073–1074.
[833] See the discussion in Chapter 7(V) below.
[834] Stephen Penk "Common Law Privacy Protection in Other Jurisdictions" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 113 at 150–151.

in the discussion above, with facts on the public record, facts occurring in publicly accessible places and facts known to other persons held to not be private. The United States tort, therefore, promises much and delivers little. Despite this, some commentators still argue that New Zealand should look to the United States for inspiration.[835] However, this thesis argues that New Zealand should look to the United States only for what not to do. The private facts tests in the United States relies on a rigid bifurcation between what is public and private, not on a context-specific consideration of whether there was a reasonable expectation of privacy. New Zealand jurisprudence shows a more nuanced and flexible approach. Therefore, relying on a jurisdiction with such a rigid approach is inconsistent with the way the disclosure tort has developed in New Zealand to date.

B Canada

The disclosure tort found its foothold in Canada in the Ontario case of *Jane Doe 464533 v ND*.[836] This case involved the publication of a sexually explicit video of the plaintiff on a pornographic website. The video was on the site for three weeks before the plaintiff had it removed, but in that time she "experienced severe humiliation and embarrassment, causing serious depression and emotional upset."[837] The Court upheld the invasion of privacy claim, endorsing the United States disclosure tort test with one amendment (shown underlined) as follows: (1) publicity of a matter concerning the private life of another; (2) where the matter publicised or the act of publication would be highly offensive to a reasonable person; and (3) the matter is not of legitimate concern to the public.[838] Berryman notes that the amendment to the test allows:[839]

> … liability even where publication does not actually occur but where the defendant attempts to post the highly offensive material, or where the material is made available to a secured smaller group.

In the same year as *Jane Doe*, the Canadian federal courts had to consider whether Canadian common law included a disclosure tort in *Canada v John Doe*.[840] The case involved a mailout

[835] Beswick and Fotherby, above n 20, at 267 and 227–228. The authors argue that because New Zealand privacy law has more in common with the United States, Canada and Australia, those are better jurisdictions for inspiration for privacy law in New Zealand than English law.
[836] *Jane Doe 464533 v ND* 2016 ONSC 541, [2016] OJ No 382 (SC).
[837] Jeff Berryman "Remedies for Breach of Privacy in Canada" in Jason NE Varuhas and N A Moreham (eds) *Remedies for Breach of Privacy* (Bloomsbury Academic, London, 2018) 323 at 333. See *Jane Doe 464533*, above n 836, at [13].
[838] *Jane Doe 464533*, above n 836, at [46].
[839] Berryman, above n 837, at 333.
[840] *Canada v John Doe* 2016 FCA 191, [2016] FCJ No 695 (CA).

by Health Canada to 40,000 participants registered for a medical marijuana programme. The envelopes used in the mailout included a visible return address of the programme, thereby identifying the addressees as participants in the programme. The plaintiff alleged a range of causes of action, including the disclosure tort. At the initial trial, the Judge had refused to strike out the cause of action, despite recognising that it was a novel claim in Canada.[841] In the Supreme Court, the Court noted the reluctance of Canadian courts to recognise a separate privacy tort, but also recognised that the acceptance of the intrusion tort in Ontario (in the case of *Jones v Tsige*)[842] had opened the door to the privacy tort in Canada. As a result, the Court held that the cause of action should not be dismissed just because it was novel;[843] instead, the cause of action should be rejected because it was not supported on the facts. Relying on the United States disclosure tort test, the Court found that the case at hand would not be sufficient to meet the publicity requirement of the test.[844]

While the "fledgling" [845] status of the Canadian disclosure tort provides it with limited comparator value, it is useful to note that where it has been discussed, it has relied on the cause of action established in the United States tort. Where the Canadian experience gets interesting, however, is in the existence of several provincial statutory privacy torts. Saskatchewan,[846] Manitoba,[847] Newfoundland,[848] and British Columbia have all introduced such torts.[849] Hunt notes that while the statutes have differences, they are "nearly identical in most respects."[850] Therefore, this thesis only sets out one of the relevant provisions by way of illustration. Section 1 of the British Columbia Privacy Act states:[851]

> (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.
> (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.

---

[841] At [13].
[842] *Jones v. Tsige* 2012 ONCA 32, [2012] OJ No 148 (CA).
[843] *Canada v John Doe*, above n 840, at [53].
[844] At [52]–[56].
[845] Chris D L Hunt "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37 Queens LJ 167. See also Beswick and Fotherby, above n 20, at 239.
[846] Saskatchewan Privacy Act RSS 1978 c P-24.
[847] Manitoba Privacy Act CCSM 1987 c P125.
[848] Newfoundland Privacy Act RSNL 1990 c P-22.
[849] British Columbia Privacy Act RSBC 1996 c 373.
[850] Hunt, above n 802, at 269.
[851] At 270. Hunt also uses the British Columbian statute when discussing the torts, noting that it is "broadly representative". Berryman, above n 837, at 325 notes that the Manitoba Act is the only one that does not require the actions of the defendant to be "wilful". However, the Act does require the infringement to be "substantial or unreasonable" (see Manitoba Privacy Act, s 2(1)).

(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
(4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

The broad nature of ss (1) makes ss (2) important in determining whether there has been a violation of privacy. Subsection (2) pegs the cause of action to reasonability, and Hunt has argued that the "courts have typically approached privacy claims by asking whether a reasonable expectation of privacy exists."[852] However, while the reasonable expectation test is therefore relevant, Hunt also argues that the courts have not engaged in any "careful discussion of the factors relevant to its application."[853]

While there might be little principled analysis, the case law demonstrates that various types of information have been found to be private, including information regarding health, medical treatment, personal financial information, sexual conduct, and sexual orientation.[854] These types of information fit within a "biographical core" of information which has been recognised by the Canadian Charter jurisprudence as being information in which there is a reasonable expectation of privacy.[855] However, Hunt notes that what is private under statutory tort law is broader than this biographical core of information.[856] Certainly, "mundane"[857] information like name and address were protected in the case of *Griffin v Sullivan*, where the posting of that information, along with a photograph, to a website which was predominantly used anonymously was held to be an invasion of privacy.[858] In regard to once public facts, Hunts notes that the Canadian statutory torts are silent on the issue.[859] While the use of a statutory tort is interesting, the reality is that there have been few actions under the statutes (which could reflect the fact that cases can only be brought in senior courts, making them less accessible and costly) and success for plaintiffs has been rare.[860] It is also worthwhile noting that in 2010 the NZLC recommended against introducing a statutory tort. It argued that New Zealand's common law tort was already established and that statutes run the risk of becoming

[852] Chris D L Hunt and Nikita Shirazian "Canada's Statutory Privacy Torts in Commonwealth Perspective" (2016) Oxford U Comparative L Forum 3 <ouclf.law.ox.ac.uk>, text after note 183.
[853] At text after note 14.
[854] Hunt, above n 802, at 281.
[855] See *R v Cole* [2012] SCJ No 53, 2012 SCC 53.
[856] Hunt, above n 802, at 280.
[857] Hunt and Shirazian, above 852, text after note 246.
[858] *Griffin v Sullivan* 2008 BCSC 827, [2008] BCJ No 1333 (SC).
[859] Hunt, above n 845, at 295. Hunt argues that Canada should follow English law and recognise that further publication of information already disclosed to the public can be an invasion of privacy (at 296–300).
[860] Law Commission, above n 655, at [4.127].

inflexible and out-of-date. Furthermore, if statutes are drafted in such a way as to mitigate this risk, then they become very broad and arguably add little to what already exists at common law.[861]

C Australia

The common law has yet to develop protection for invasion of privacy in Australia, with the future of the tort described by the Australian Law Reform Commission (ALRC) as "uncertain".[862] While the oft-quoted case of *Lenah Game Meats* opened the door to recognition of the tort, few have stepped through and none at an appellate level.[863] One of the few cases which has addressed the tort of privacy is *Jane Doe v Australian Broadcasting Corporation*. The case involved a claim for invasion of privacy and breach of confidence (amongst other causes of action) for the defendant's broadcast of the plaintiff's identity as a victim of rape within marriage. Finding against the defendant, the Judge found that *Lenah Game Meats* provided sufficient support to recognise a privacy tort in the case at hand.[864] The Judge also held that the reasonable expectation of privacy test was the appropriate test for establishing whether the matter involved private (and confidential) information.[865] In applying the test, her Honour stated:[866]

> I am satisfied that the nature of the information under consideration in this case, identifying a person as the victim of a sexual assault, is information capable of being characterised as information which the person to whom it relates has a reasonable expectation would remain private. The information is not only about participation in sexual activity, which is generally a private matter, but also about non-consenting sexual activity, that is about Ms Doe being subjected to criminal acts of a sexual nature. In addition, the identity of the perpetrator as her estranged husband, is relevant to the characterisation of the information as private.

While the tort has struggled to gain a foothold, the traditional breach of confidence cause of action has been used to protect privacy. In *Lenah Game Meats*, Gleeson CJ preferred this

---

[861] At [7.8]–[7.13].
[862] Australia Law Reform Commission [ALRC] *Serious Invasions of Privacy in the Digital Age* (ALRC Final Report 123, 2014) at [3.56].
[863] Penk, above n 834, at 114–116. See generally Des Butler "A Tort of Invasion of Privacy in Australia" (2005) 29 MULR 339. Lower court decisions that have recognised a tort of invasion of privacy include *Grosse v Purvis* [2003] QDC 151, (2003) Aust Torts Reports 81-706 (DC) and *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281 (CC). However, other Australian cases have found that recognition of a tort of invasion of privacy is unlikely. See ALRC, above n 862, at [3.54].
[864] *Jane Doe*, above n 863, at [157].
[865] At [116].
[866] At [119].

approach and other state-level cases have also allowed protection of private information this way.[867]

While consideration of the Australian jurisprudence does not further the existing understanding of the disclosure tort, Australia has also done some work in the area of statutory torts. Over the years there have been multiple state and federal reports on the issue.[868] However, the most useful for the purposes of the present research is the 2014 report of the ALRC. In the report, the ALRC recommended establishing a statutory tort covering both intrusion upon seclusion and misuse of private information, with the following essential elements: [869]

> (1) It must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances;
> (2) the invasion must have been committed intentionally or recklessly — mere negligence is not sufficient;
> (3) the invasion must be serious;
> (4) the invasion need not cause actual damage, and damages for emotional distress may be awarded; and
> (5) the court must be satisfied that the public interest in privacy outweighs any countervailing public interests.

The report noted that the reasonable expectation of privacy test is an objective test.[870] It also provided a non-exhaustive list of the circumstances a court should consider when determining whether a reasonable expectation of privacy existed. This list, which covers both types of invasion, includes:[871]

> (a) the nature of the private information, including whether it relates to intimate or family matters, health or medical matters, or financial matters;

---

[867] *Lenah Game Meats*, above n 670, at [41]. See also *Giller v Procopets* [2008] VSCA 236 (CA), (2008) 24 VR 1 and *Wilson v Ferguson* [2015] WASC 15 (SC).
[868] See ALRC *For Your Information: Privacy Law and Practice* (ALRC Report 108, 2008); New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC R120, 2009); and Victorian Law Reform Commission *Surveillance in Public Places* (VLRC R18, 2010). The most recent law reform initiative is the New South Wales Parliament Legislative Council Standing Committee on Law and Justice *Remedies for the Serious Invasion of Privacy in New South Wales* (R57, 2016). However, the latter report's recommendation on the statutory tort was based on ALRC *Serious Invasions of Privacy in the Digital Age*, above n 827 (see NSW Report at 10).
[869] ALCR, above n 862, at [1. 11]. In referring to the two types of invasions that the statutory tort should cover, the ALRC clearly stated it was drawing upon two of the four categories of privacy tort seen in the United States (see [5.11]).
[870] At [6.7].
[871] At 96.

(b) the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology;
(c) the place where the intrusion occurred, such as in the plaintiff's home;
(d) the purpose of the misuse, disclosure or intrusion;
(e) how the private information was held or communicated, such as in private correspondence or a personal diary;
(f) whether and to what extent the private information was already in the public domain;
(g) the relevant attributes of the plaintiff, including the plaintiff's age, occupation and cultural background; and
(h) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy.

The ALRC also noted that the definition of "sensitive information" from Australia's Privacy Act 1998 may be relevant.[872] In regard to the place of intrusion, the ALRC was clear that in some circumstances a person may have a reasonable expectation of privacy in public, although such expectations will be lower than when a person is in their own home.[873] Similarly, the ALRC recognised that just because information is in the public domain does not stop it from being private information, so that subsequent use or publication of the information could also be an invasion of privacy.[874] The ALRC also considered that the conduct of the plaintiff will be relevant, including whether the plaintiff consented to the privacy-invading conduct (noting that the ALRC also recommended that consent be a defence to the tort).[875] However, the ALRC recognised that consent can be of a limited nature – people might consent to publication in one way but not another. Similarly, people might reveal some facts about their personal life but want to shield other aspects.

The ALRC eschewed the highly offensive test, believing that the intent of the test could be controlled either as part of the reasonable expectation test or the "serious" element of the cause of action.[876] The seriousness test proposed requires the courts to have regard to, amongst other factors:[877]

(a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff; and

[872] At [6.36]. The ALRC notes that just because information falls within the definition of 'sensitive information' does not necessarily mean there is a reasonable expectation of privacy in the information.
[873] At [6.44]–[6.51].
[874] At [6.62]–[6.64].
[875] At [6.72]–[6.79]. See [11.52]–[11.80] for information on the consent defence.
[876] At [8.38].
[877] At 132.

(b) whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff.

The ALRC is clear that this standard is lower than the highly offensive test, although still a necessary filter to ensure that trivial breaches of privacy are not actionable.[878] Although, the ALRC report was issued in June 2014, by 2022 the Australian Government has yet to action the report, so no statutory tort has been enacted in Australia at either state or federal level.[879] The absence of a statutory tort, as well as the limited nature of its common law, makes Australia, like Canada, of limited comparator value for the purposes of this thesis.

D England

English law has exerted significant influence on the development of the disclosure tort in New Zealand. However, English developments have taken their own unique path. This path has been significantly influenced by the right to privacy contained in the ECHR,[880] which was brought into domestic effect by the Human Rights Act 1998 (HRA).[881] England's protection of privacy has grown out of the equitable action for breach of confidence,[882] with breach of confidence now having two distinct versions – the traditional breach of confidence cause of action, which rests on secrecy and confidences, and misuse of private information, a rights-based cause of action that protects privacy.[883] However, misuse of private information has recently been recognised as a tort.[884] More important than labels, however, is the rights-based character of the cause of action. The impact of the HRA has been described as follows:[885]

> The language has changed following the coming into operation of the Human Rights Act 1998 … We now talk about the right to respect for private life and the countervailing right to freedom of expression. The jurisprudence of the European Court offers important guidance as to how these competing rights ought to be approached and analysed.

[878] At [8.6] and [8.24].
[879] Normann Witzleb "Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy" in Moreham and Varuhas (eds) *Remedies for Breach of Privacy* (Bloomsbury, Oxford, 2018) 377 at 377.
[880] Beswick and Fotherby, above n 20, at 227.
[881] Human Rights Act 1998 (UK). Section 6 of the Act states that courts cannot act in a way incompatible with ECHR rights. Under s 2(1)(a) the courts must take into account any decision of the European Court of Human Rights (ECtHR).
[882] Penk, above n 834, at 126.
[883] Mark Warby, Adam Speker and David Hirst "Misuse of Personal Information" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 223 at [5.04].
[884] *Vidal-Hall and others v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003 at [43].
[885] *Campbell*, above n 355, at [86].

The misuse of private information cause of action requires satisfaction of two components: (1) the objective test of whether a person has a reasonable expectation of privacy; and (2) if the answer to the first question is yes, there must be a balancing of the art 8 ECHR right to privacy and the discloser's art 10 ECHR right to freedom of expression.[886] What is notable with this test is that the test does not require offensiveness to establish a *prima facie* claim for invasion of privacy; rather, offensiveness is part of the assessment in the second part of the test.[887] The second part of the test is discussed in Chapter 7.

In *Murray*, the Court noted that the first test was "what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity."[888] Elaborating, the Court said:[889]

> As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher.

Murray involved the taking of photographs of the plaintiff (the young son of author JK Rowling) and his family while they were walking down an Edinburgh Street. The case is strikingly similar to *Hosking*, and while *Hosking* was an important influence on the trial Judge's decision in *Murray*,[890] the Court of Appeal declined to follow it.[891] The two cases show a marked difference in application of the disclosure tort. In *Hosking,* the Court could not find any fact in which there was a reasonable expectation of privacy.[892] In contrast, the Court of Appeal in *Murray* believed that it was entirely reasonable to protect children's freedom to "live normal lives without the constant fear of media intrusion".[893] The Court stated:[894]

---

[886] See *Murray*, above n 732, at [35]–[40]; *Campbell*, above n 355, at [21]; and *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), [2008] All ER (D) 322 (Jul) at [10]. See also Eric Barendt "'A Reasonable Expectation of Privacy': A Coherent or Redundant Concept?" in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 96 at 102.
[887] See *Campbell*, above n 355, at [22] and *Murray*, above n 732, at [26].
[888] *Murray*, above n 732, at [35].
[889] At [36].
[890] At [35].
[891] At [51].
[892] *Hosking*, above n 8, at [164].
[893] *Murray*, above n 732, at [50].
[894] At [55].

> … an expedition to a café of the kind which occurred here seems to us to be at least arguably part of each member of the family's recreation time intended to be enjoyed by them and such that publicity of it is intrusive and as such adversely affect such activities in the future.

In addition, the Court in *Murray* focused on the fact that the defendant deliberately photographed the plaintiff in secret with a view to publication and profit, and "no doubt in the knowledge that the parents would have objected to them."[895] The Court of Appeal was influenced by the House of Lords decision in *Campbell* and the ECtHR decision in *Von Hannover v Germany*. The former case related to articles and pictures taken of the supermodel Naomi Campbell as she was leaving a Narcotics Anonymous meeting. Finding in favour of the plaintiff, a majority of the House of Lords established the reasonable expectation test for determining whether art 8 ECHR is engaged.[896] The latter case involved the publication of photos of Princess Caroline of Monaco engaged in a range of private activities like shopping, eating and horse-riding. In that case, the ECtHR noted that the concept of private life protected by art 8 protects personal identity, including a person's name, picture and their "physical and psychological integrity".[897] This protection applied even in public. As a result, the ECtHR held that the complained-of photos were within the applicant's private life.[898]

Reasonable expectations of privacy have been found in other English cases, including the publication of photos of a celebrity wedding,[899] photos of a public figure engaging in a sadomasochistic bondage session,[900] pictures of a celebrity's children shopping on a street in Los Angeles,[901] and the fact of a police investigation into historical sexual offending.[902] In the latter case, the fact that stigma attaches to such an investigation was a key component of the case. In this regard the Court noted:[903]

> If the presumption of innocence were perfectly understood and given effect to, and if the general public was universally capable of adopting a completely open- and broad-minded view of the fact of an investigation so that there was no risk of taint either during the investigation or afterwards (assuming no charge) then the position might be different. But

[895] At [50].
[896] *Campbell*, above n 355, at [21].
[897] *Von Hannover v Germany* (2005) 40 EHRR 1 at [50].
[898] At [53].
[899] See *OBG Ltd v Allan; Douglas v Hello! Ltd* (No 3) [2007] UKHL 21, [2008] 1 AC 1 at [105].
[900] See *Mosley*, above n 886.
[901] See *Weller*, above n 443.
[902] See *Richard v British Broadcasting Corporation* [2018] EWHC 1837 (Ch), [2018] 3 WLR 1715. This case related to the investigation into allegations of historical sex offending against Sir Cliff Richard.
[903] At [248].

> neither of those things is true. The fact of an investigation, as a general rule, will of itself carry some stigma, no matter how often one says it should not.

English courts have also found that there can be an invasion of privacy by giving further publicity to public information. In *McKennitt v Ash*, Eady J held that the protection afforded by the law would not be withdrawn "unless and until it is clear that a stage has been reached where there is no longer anything left to be protected."[904] The Judge continued:[905]

> … it does not necessarily follow that because personal information has been revealed impermissibly to one set of newspapers, or to readers within one jurisdiction, that there can be no further intrusion upon a claimant's privacy by further revelations. Fresh revelations to different groups of people can still cause distress and damage to an individual's emotional or mental well-being … .

This approach was endorsed in *PJS v News Group Newspapers Ltd*, where the Supreme Court noted that:[906]

> … repetition of [a] disclosure or publication on further occasions is capable of constituting a further tort of invasion of privacy, even in relation to person to whom disclosure or publication is previously made – especially if it occurs in a different medium.

In that case, the Court held that there was a qualitative difference between information being widely available online and being "blazoned" on the front page of a national paper.[907] Where the republication occurs after some time, reasonable expectations of privacy have also been found. In *R v Broadcasting Complaints Commission, ex parte Granada Television Limited*, Balcombe LJ held that:[908]

> In my judgment it is clear that the fact that a matter has once been in the public domain cannot prevent its resurrection, possibly many years later, from being an infringement of privacy.

While this case involved information about two young murder victims, a similar approach has been seen when the information is about an offender. In *R v Chief Constable of the North*

---

[904] *McKennitt and others v Ash and another* [2005] EWHC 3003 (QB), [2006] IP & T 605 at [81].
[905] At [81].
[906] *PJS v News Group Newspapers Ltd* [2016] UKSC 26, [2016] AC 1081 at [32].
[907] At [31].
[908] *R v Broadcasting Complaints Commission, ex parte Granada Television Limited* [1995] EMLR 163 (CA) at 168. Warby, Speker and Hirst, above n 883, at [5.79] note that this case was followed in *A v B, C and D* (QBD, 2 March 2001, Mackay J), where a pop star obtained an injunction "preventing the unauthorised publication in a pornographic magazine and a tabloid newspaper of sexually explicit photographs taken of her before she became famous."

Wales Police and others, ex parte AB and another, Buxton J noted, in *obiter*, that "a wish that certain facts in one's past, however notorious at the time, should remain in the past" was an aspect of a person's private life.[909]

Recently, in *NT 1 & NT 2*, the English courts had to consider whether there was a reasonable expectation of privacy in spent convictions. To this end, Justice Warby noted that:[910]

> As a general rule … the point in time at which Parliament has determined that a conviction should become spent may be regarded as the point when the convict's art 8 rights are engaged by any use or disclosure of information about the crime, conviction, or sentence.

However, the Judge was clear that the "general rule" did not create a right to privacy in spent convictions; rather, the fact a conviction was spent was a "weighty factor" in balancing competing interests.[911] This conclusion was borne out in the decision of the case itself, where only NT 2 had a reasonable expectation of privacy in the spent conviction.[912] While NT 1's conviction was spent, the Judge found no expectation of privacy because the conviction was only marginally spent[913] and the impact on his private life was minimal.

In *XKF v BBC*, the Court found that a former criminal had a reasonable expectation of privacy in relation to attempts to rehabilitate himself even where the spent conviction itself might not sustain a reasonable expectation of privacy.[914] The case involved the proposed broadcast of an interview with a former policeman who had been convicted of fraud. The former policeman had changed his name following his conviction becoming spent and moved to a new area. In finding for the plaintiff, the Judge noted that the interest at stake was more than recognition of the policy behind spent convictions; it reflected what the plaintiff had done to rehabilitate since his release from prison, and on that front the plaintiff had "made significant efforts."[915] While this case might appear to broaden the ambit of spent convictions, with a focus on rehabilitative efforts rather than simply time frame, the reality might be more constrained.

---

[909] *R v Chief Constable of the North Wales Police and others, ex parte AB and another* [1997] 3 WLR 724 (QB) at 738. The case involved information about two recently released paedophiles.
[910] *NT 1 & NT 2*, above n 361, at [166(2)].
[911] At [166(2)].
[912] At [171]. Justice Warby's finding regarding NT 2 was influenced by the fact NT 2 had young children and that ongoing availability of the information would have an adverse impact on his family life (at [222(3)] and [224]).
[913] At [170]. For a discussion of the validity of the Judges analysis on NT 1's spent conviction see below n 1143.
[914] *XKF v BBC* [2018] EWHC 1560 (QB) at [30]. The Judge stated that the conviction might not sustain a reasonable expectation of privacy due to the level of public interest in the conviction.
[915] At [36].

One of the key factors of the decision was the method employed by the defendant to obtain the interview – door-stopping – a method which the Judge viewed particularly dimly.[916]

As noted above, the disclosure tort developments in English law owe much to the HRA and the ECHR. The art 8 right to a private life has been interpreted broadly by the ECtHR. In *ML and WW v Germany* the court noted that the concept is:[917]

> … a broad term not susceptible to exhaustive definition, which covers the physical and psychological integrity of a person and can therefore embrace multiple aspects of a person's identity, such as gender identification and sexual orientation, name or elements relating to a person's right to their image. The concept covers personal information which individuals can legitimately expect should not be published without their consent.

The Court has also held that comments on a person's Facebook page "affected the applicants' psychological well-being and dignity, thus falling within the sphere of their private life"[918] and that the "compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable" raises private life considerations.[919] Furthermore, just because the information is already in the public domain does not necessarily exclude information from being private.[920] Recently, the ECtHR has also held that the art 8 right protects against the continued publication of an offender's name after his conviction has become spent.[921]

The broad interpretation of the right to a private life under the ECHR has clearly influenced the protection of privacy under the disclosure tort in England. It is arguable, therefore, that the role played by the ECHR does limit the applicability of the English decisions in New Zealand which does not have an overriding right to privacy in its Bill of Rights.[922] However, even with these constitutional differences, the above discussion demonstrates that New Zealand's approach to the disclosure tort and reasonable expectations of privacy exhibit a flexibility and nuance similar to English law rather than United States law. New Zealand's approach is focused on surrounding circumstances rather than a rigid adherence to categories of information.

---

[916] At [36]. The method used to approach and interview the plaintiff was also a factor in the Judge finding that the plaintiff's ECHR, art 8 rights outweighed the defendants ECHR, art 10 rights (see [10]).
[917] *ML and WW v Germany* [2018] ECHR 554 (ECHR) at [86] (emphasis added).
[918] *Beizaras and Levickas v Lithuania* [2020] ECHR 19 (ECHR) at [117].
[919] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* ECHR 931/13, 27 June 2017, at [136].
[920] See *Von Hannover,* above n 897.
[921] *Hurbain,* above n 468.
[922] See above n 1118.

V Critiques and Clarifications

While the cause of action for the disclosure tort is well established in New Zealand, it is not without its critiques and refinements. These critiques and refinements attempt to make sense of the requirements to establish an invasion of privacy, both theoretically and operationally, and are therefore useful for understanding the tort and identifying ways (if any) it should be developed in the future.

A Reasonable Expectation of Privacy

It is helpful to begin a discussion on the reasonable expectation of privacy test by considering its structure and drivers. The reasonable expectation of privacy test gained prominence in *Campbell*, where two of the five judges preferred it to the other options – being the inherently private test and the highly offensive test.[923] Lord Nicholls saw it as a potentially lower standard than the highly offensive standard and Baroness Hale thought it was "simpler and clearer".[924] Moreham argues that the test is less likely to be subject to judicial value statements than the inherently private test.[925] Furthermore, the reasonable expectation of privacy test allows "contemporary social values" to be taken into account, so the law can adapt when values change.[926]

The test has both a subjective and an objective element.[927] Moreham argues that the subjective aspect of the test is not an enquiry into what the subject actually expected at the time of the interference, rather it is a normative enquiry about whether the claimant is "entitled to expect society, acting through the law, to step in to protect his or her privacy interests."[928] The objective check then ensures that the claimaints' expectations are reasonable. The English courts have noted that this objective test asks, "what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity."[929]

---

[923] See Chapter 4(II)(B)(1) for a discussion of the inherently private test and Chapter 6(V)(B) for a discussion of the highly offensive test.
[924] *Campbell*, above n 355, at [22] and [135].
[925] At [94]. See Moreham, above n 454.
[926] *Hosking*, above n 8, at [250].
[927] Moreham, above n 102, at 653.
[928] At 656.
[929] See for example *Murray,* above n 732, at [35].

For Barendt, the reasonable expectation of privacy test is misconceived and incoherent.[930] He argues it is artificial to ask if there was an expectation of privacy, because in many circumstances a plaintiff would not have had any actual expectations, especially if the plaintiff is a child.[931] Furthermore, he argues that the test allows freedom of expression considerations to be taken into account at the first stage, as well as the second stage, and that the test leads to uncertainty because what is reasonable shifts over time and the judiciary becomes "responsible for deciding when such a change has occurred."[932] As an alternative, Barendt suggests that the English courts should simply ask whether the claimant's "rights under ECHR Art 8 were engaged?"[933] Even better, Barendt argues, would be a non-exhaustive list of private matters set out in legislation. To preclude an onslaught of trivial claims, Barendt would have a requirement of "non-triviality" or "seriousness".[934] While there is an attractive simplicity to Barendt's argument, its reliance on categories of private matters risks becoming rigid, especially if legislation is involved.

For Moreham, the reasonable expectation of privacy test is the best option, but she argues that it can be inappropriately applied when courts focus on what "potential privacy-infringers can or usually do in the situation in question."[935] This can result in a "spiralling downward" of privacy protection as more privacy-infringing activities become normalised in society.[936] Moreham's solution is to recognise that the reasonable expectation test is an enquiry into "whether the claimant had a reasonable expectation of privacy *protection*".[937]

Moreham also argues that the application of the test is underpinned by two "previously unarticulated principles" which provide two routes for demonstrating that information or an activity are private and therefore warrant protection[938] – (1) societal attitudes to the information at issue and (2) the privacy signals given by the claimant and whether society would expect such signals to be respected.[939] These two principles work together either to

[930] Barendt, above n 886, at 96.
[931] See generally *Hosking*, above n 8; *Murray*, above n 732; and *Weller,* above n 443 for privacy cases on behalf of children.
[932] Barendt, above n 886, at 110.
[933] At 111.
[934] At 113.
[935] Moreham, above n 454, at 654.
[936] See Winkelmann, above n 342, at 18.
[937] Moreham, above n 454, at 655.
[938] Moreham, above n 454, at 651.
[939] At 651. Moreham discusses the principles in detail at 657–672.

strengthen the claimant's claim for invasion of privacy (where both elements are satisfied) or to provide an alternate grounds to find an invasion of privacy.[940]

The first principle reflects those categories of information which reasonable people usually consider private. If a matter falls into one of these categories it is likely to satisfy the reasonable expectation of privacy test.[941] Moreham identifies seven categories of usually private information. These are information relating to:[942]

> … (i) the appearance or workings of the physical body … (ii) to sexual encounters or activity; (iii) to the intimate details of one's personal relationships; (iv) to the intimacies of one's family and/or domestic life; (v) to the experience of trauma, grief or strong emotion; (vi) to the inner workings of one's mind … and (vii) to detailed patterns of one's daily life (as would be observed, for example, as a result of systematic surveillance).

The second principle requires consideration of a claimant's behaviour and the signals it provides in respect of the information at issue.[943] The sort of factors which are relevant here include: whether the claimant consented to access; whether they "courted or eschewed publicity"; the circumstances in which the information was shared; the claimant's location and how the claimant presents in such a location (for example, dress, body language and behaviour);[944] the age and specific vulnerabilities of the claimant; the way information is stored;[945] any surreptitious behaviour on the part of the defendant which means that a claimant does not even know "such privacy signals are necessary";[946] and the defendant's knowledge of the claimant's expectations or signals. Moreham argues that a defendant should only be liable if he or she knew, or should have found out, about the privacy signals.[947]

Moreham's first principle is uncontroversial. The idea that there are some generally accepted categories of private information has been seen in many instances. Nicholson J in *P v D*, for example, noted that: "I consider that information that a person has been treated at a psychiatric hospital is in the *category* of a private fact".[948] Gleeson CJ also referred to

---

[940] At 672. Moreham notes that a court needs to consider both elements, even if the first is found to exist. The privacy signals can also work in the opposite direction – to weaken a societally-recognised reasonable expectation of privacy (for example, where a person voluntarily takes their clothes off in public).
[941] At 659.
[942] At 659. The author identified these categories from English case law.
[943] At 660.
[944] At 666.
[945] At 669.
[946] At 670.
[947] At 671.
[948] *P v D*, above n 696, at [36] (emphasis added).

particular information that was "easy to identify as private".[949] Moreham's second principle reflects the subjective expectations part of the reasonable expectation test by focusing on the "socially-endorsed signals" the claimant has used to demonstrate a wish for privacy.[950] More interesting for the purposes of the present research, however, is the extent to which Moreham's principles hold true when considering once public facts.

The first consideration is whether once public facts are usually private information. Where convictions are spent, it is arguable that they should be considered as a category of usually private information. In such situations there is a clear parliamentary intent that the person should be able to treat such convictions as private. However, Moreham's analysis is less useful where the facts at issue do not fall within the first principle and the claimant's signals must be relied upon. How are courts to know whether the claimant's actions are ones that society should uphold, in the face of technology that enables the storage of enormous amounts of information, easy dissemination of information, persistent surveillance, and other people's activities that are contrary to a commitment to privacy? Assistance in answering this question may be found in the work of Winkelmann CJ.

In 2018, Winkelmann CJ gave the Sir Bruce Slane Memorial Lecture to mark the 25th anniversary of the Privacy Act 1993. As part of that lecture, the now Chief Justice discussed the reasonable expectation test. Her Honour argued that the reasonable expectation test requires courts to employ two forms of analysis. The first she described as an "empirical" analysis,[951] which ensures that the reasonable expectation test reflects the "contemporary societal values" standard described in the judgment of Tipping J in *Hosking*.[952] Winkelmann CJ proposed that the empirical analysis would:[953]

> … draw upon New Zealand's existing legal framework – case law, obligations under international law, in the field of data protection, the OECD Privacy Guidelines (2013) and the updated General Data Protection Regulation. And of course, the Privacy Act, which has done so much to shape expectations of privacy in our community.

This analysis requires consideration not just of the regulatory environment, but also of what is happening socially. However, her Honour recognised that, in considering what is happening in society, any retrograde developments in society might be incorporated into the test,

[949] *Lenah Game Meats*, above n 670, at [42].
[950] Moreham, above n 454, at 661.
[951] Winkelmann CJ, above n 342, at 19.
[952] See above n 710.
[953] Winkelmann CJ, above n 342, at 17.

resulting in a "spiralling downward of the zone of privacy."[954] For Winkelmann CJ, the risk of a "spiralling downward" of privacy results from the:[955]

> … increasing every day surveillance we are all subject to (of the public and private camera kind, and on the various phones, watches and apps we use) the modern media world (some would say, intrusive media), the culture of sharing of intimate detail on social media, and the growth of a business model in which we are the product.

Winkelmann CJ noted that while other commentators, like Moreham, had recognised this risk, their proposed solutions had not gone far enough.[956] For Winkelmann CJ, a second level of analysis was required, which she calls the "purposive check", where the courts reflect upon what zone of privacy is necessary to secure the benefits of privacy.[957] As to the benefits themselves, Winkelmann CJ discussed liberty and dignity/autonomy, but there are, no doubt, more.[958]

Winkelmann's CJ elaborations to the reasonable expectation of privacy test have been picked up by recent privacy cases in New Zealand. The Judges in both *Driver* and *Henderson v Walker* referred to Winkelmann CJ's arguments and advocated for the disclosure test to recognise a minimum standard of privacy to protect the benefits of privacy.[959] Winkelmann CJ's elaboration, and its acceptance by recent courts, is to be welcomed. Focusing on the benefits that recognition of a zone of privacy can deliver assists with determining whether society *should* protect a claimant's privacy signals, even if the information itself does not fall within a category of usually private information.

In light of the above discussion, this thesis agrees that the reasonable expectation test is to be preferred to an inherently private test or a legislated categories approach. The reasonable expectation of privacy test allows nuance and circumstances to be taken into account. It does not risk becoming rigidly applied or subject to value-based assessments. The objective check weeds out trivial claims or the claims of the overly-sensitive. What is needed, however, is greater clarity on the factors to be considered in determining when the test is met. Here the work of Moreham and Winkelmann CJ is useful. However, before moving on to discuss what

---

[954] At 17.
[955] At 18.
[956] At 19. See above n 937 for Moreham's proposed solution.
[957] Winkelmann CJ, above n 342, at 19.
[958] At 3 and 20. Winkelmann CJ herself referred to Tikanga Māori privacy values and broader community values. Thomas J in *Brooker*, above n 354, at [256]–[258] referred to the protection of one's home as a key value of privacy.
[959] See above n 733 and 742.

the greater clarity might look like, some critiques and refinements of the highly offensive test need to be considered.

B Highly Offensive

The highly offensive test is one of the more controversial elements of the disclosure tort cause of action. As noted above, several judicial statements have doubted the usefulness and validity of the test.[960] Moreham has gone further. She argues that the test should be abandoned.[961] Moreham argues that there has been a lack of principle in the way the test has been applied by the courts, leading to the test often reflecting judges' instincts, rather than any principled analysis. She believes the test leads to a narrow view of privacy which ignores the gravamen of many claims, and that the application of the reasonable expectation test has made it superfluous.[962] Moreham points to *Hosking* as an example of where the courts have established useful principles for the application of the test, but then failed to apply them, relying instead on judicial instinct. It is true that there is little analysis of why the test was not met in *Hosking*, with Gault and Blanchard JJ simply noting that they are "not convinced" a person of ordinary sensibilities would find the publication highly offensive and concluding that they "cannot see any real harm in it."[963]

Clague is another example where the reasoning is lacking. In *Clague*, despite noting that public disclosure of the information at issue would be embarrassing and distressing to the plaintiff and members of his family, the Judge found the test not to be satisfied. [964] There is no discussion about why the distress to the plaintiff and his family was not sufficient to satisfy the test. Moreham, however, reserves particular criticism for the decision in *Andrews.*[965] In particular, she questions why the plaintiff's reactions were held not sufficient to meet the standard. The plaintiffs gave evidence that they were "greatly distressed" by the screening of the broadcast, tensions were raised, the "emotional health of one of their children" was affected, and they were "forced to relive the trauma of the accident" in front of a number of

[960] See Chapter 6(III) above.
[961] Moreham, above n 712 at 1.
[962] At 14–31.
[963] *Hosking*, above n 8, at [165].
[964] Moreham, above n 712, at 14–15. It should be noted that the Judge in *Clague* did not need to make any conclusion regarding offensiveness because his earlier finding had been that the facts did not raise a reasonable expectation of privacy.
[965] Moreham, above n 712, at 20.

other people, some of whom they did not know.[966] It is hard to see how this evidence does not meet the test put forward in *Hosking*.[967]

Moreham's arguments against the test were considered by the Court of Appeal in its February 2021 Judgment in *Hyndman v Walker*. In that case, the plaintiff had asked the Court to reject the test. In addressing the argument, the Court noted that "there is a good deal of force" to the criticisms of the test.[968] However, the Court did not believe the current case was the appropriate vehicle in which to amend the test.[969]

While not taking the opportunity to evolve the disclosure tort in New Zealand, the case does leave the door open for such evolution in a more appropriate case. This position is supported by the words of Miller J who noted that:[970]

> … we consider this tort may well benefit from re-examination, and the opportunity to re-examine it very seldom arises. But it is not possible to remove the "highly offensive" requirement without reformulating the tort, and that is an exercise that courts must undertake with care having regard to the treatment accorded to privacy generally in New Zealand law and the need to balance rights of privacy against those of free expression.

Moreham has also argued that the BSA's highly offensive test is redundant. She argues that the test does "little analytical work", whereby the conclusion for something being highly offensive "follows automatically from the fact that there was an actionable intrusion or disclosure of private facts."[971] The highly fact-specific nature of the question means that decisions provide little guidance for the future and make it hard for broadcasters to know whether a broadcast will or will not be held to be offensive.[972]

Not all commentators object to the test. Beswick and Fotherby argue that the test serves an important role in ensuring that only serious and deserved interferences with privacy obtain legal protection. They argue that the test:[973]

---

[966] *Andrews*, above n 720, at [15].
[967] *Hosking*, above n 8, at [126].
[968] *Hyndman*, above n 789, at [73].
[969] At [75].
[970] At [3].
[971] Moreham, above n 725, at 15.
[972] At 15.
[973] Beswick and Fotherby, above n 20, at 263–264.

> … tells us when the affront to dignity warrants vindication in law. Separating these two considerations [offensiveness and reasonable expectation of privacy] can assist the court in reasoning toward an outcome that reconciles the privacy tort with others' competing dignitary interests. It accepts that in society not all interferences with privacy warrant legal protection.

Tobin argues that requiring a lesser level of offensiveness, like that proposed by Tipping J in *Hosking*, gives "undue weight to privacy at the expense of freedom of expression" and that the defence of legitimate public concern (discussed in the following chapter) is not sufficient to protect expression in the face of a lower offensiveness standard.[974]

In light of the above analysis, there is certainly some merit to the argument that the application of the highly offensive test has been little more than an exercise in judicial instinct, and that if a reasonable expectation of privacy has been invaded, then that invasion is likely to also be highly offensive. These conclusions strengthen the argument for abandonment of the test. In addition, if the reasonable expectation test is interpreted in line with the recommendations set out in this thesis, then that argument is even stronger. If there is a reasonable expectation of privacy that is supported by contemporary societal values and which accords with the core values promoted by privacy, then the highly offensive test is essentially folded into the reasonable expectation test. The recommendations for the reasonable expectation test, as well as the highly offensive test, are discussed in more detail next.

VI Future Directions of the Disclosure Tort

The intent of this chapter was twofold: first, to determine if once public facts could satisfy the legal test for the disclosure tort in a manner that is appropriate and consistent with the development of the tort; and second, to elucidate in what ways, if any, the tort needs to develop in order to be fit for purpose and protect once public facts in the right circumstances. As to the first aspect, it can be difficult to establish in the abstract if a legal test will cover a broad category of scenarios. Once public facts could arise in a large range of circumstances, ranging from prior criminal convictions to the existence of information in the public domain that a person would wish to not be so available. However, there are aspects of the development of the tort in New Zealand which means that such facts should not necessarily be excluded (as they generally are in the United States). What information can reasonably be expected to be private is broad and has covered facts that occurred in public, facts about

[974] Tobin, above n 386, at 103.

public officials, facts about accused or convicted persons, a taped murder confession, and facts which have had a degree of public exposure. In addition, there have been clear judicial statements recognising once public facts within the test.

As a result of the conclusion that the reasonable expectation test can, in appropriate circumstances, include once public facts, there is an argument that this thesis need not go further. However, having reviewed all the cases and relevant literature, such an argument is short-sighted. The disclosure tort is still a developing area of law and all opportunities to refine it should be welcomed. Accordingly, the present research recommends refinements to the reasonable expectation test. The refinements are not revolutionary, such as abolition of the entire test (although, removal of the highly offensive test would be a substantial change in form – although not really in substance); rather, they are enhancements that can arguably provide greater clarity both for future decision-makers and would-be publishers who want to be able to predict before publication their risk of breaching the law. The refinements align with the direction in which the tort is already travelling, but ensure that the path is clearer and less subject to some of the risks identified along the way – like retrograde developments in society being incorporated into the test.

The current test for a reasonable expectation of privacy recognises the need for a close inspection of the circumstances of the case. However, there has been little consistency about which factors need to be taken into account. This aspect of the test should recognise that these factors include the nature of the activity or information, as well as a range of factors relevant to Moreham's privacy signals, like the location of the plaintiff, plaintiff attributes (for example, whether they are a public figure, their age and actions regarding the disclosure) and plaintiff's consent. Other relevant factors are the nature and purpose of the intrusion (including how the information came into the hands of the defendant) and the effects on the claimant. These factors are not necessarily easily seen as claimant signals, although they are likely to impact on the establishment of the test. Where once public facts are at issue, these factors also include changed circumstances between the facts and publication (including whether a conviction has become spent and steps taken by the plaintiff to rehabilitate or disassociate from the information), the existence and extent of prior publicity, how readily available the information currently is, and the length of time that has passed since original publication. In terms of the latter, it is not possible to establish a specific timeframe. This will ultimately be an evaluative exercise with a range of inputs, including how all the other factors discussed here impact the length of time that has actually passed. Where the matter is a prior conviction, the Clean Slate Act timeframe will be an important input as well.

As noted above, there is still a gap between the plaintiff's signals and establishing that society should protect those signals. This gap is filled by the work of Winkelmann CJ, and the enhancements she proposed should be adopted as part of the test. Accordingly, in addition to the circumstances of the case, an empirical analysis and core values analysis (the purposive check) should be conducted to ensure that the plaintiff's expectations of privacy are reasonable and aligned with the fundamental interests and values pursued by privacy. The empirical analysis requires consideration of broader societal factors, including the attitudes to privacy discussed in Chapter 3, as well as the broader regulatory environment. For once public facts, such an empirical analysis would find a Privacy Act that includes the ability for people to request erasure of personal information, and an obligation on entities to erase information to ensure it is "accurate, up to date, complete, and not misleading".[975] The empirical analysis would identify a BSA which has historically allowed some previously public information to regain its privacy through a lapse of time. The empirical analysis would find a spent conviction legislation which allows persons convicted of an offence to be treated as having no criminal record for certain purposes if they meet the thresholds set out in the relevant law. Such analysis would also consider the international privacy landscape which allows protection for historical information which a person no longer wants to be associated with (for example, see the decision in *Google Spain* and art 17 of the GDPR).

The core values analysis considers the purpose and benefits of recognising a zone of privacy in a particular situation and ensures that the benefit is aligned to the core values supported by privacy. The benefits could be supporting liberty, rehabilitation, dignity, personhood, autonomy, sanctity of the home, intimacy, relationship-building, and community and cultural values. Calling this a 'core values' analysis or assessment, rather than the purposive check, promotes recognition that privacy supports core values and that the zones of privacy that are recognised uphold these values for the good of individuals and the wider community. Incorporation of the core values analysis also allows the highly offensive test to be abandoned, as the reasonable expectation test itself ensures that trivial claims are weeded out. Any breach of privacy which impacts a core value will naturally be offensive.

Before moving off the elements of the cause of action for the disclosure tort, there is one aspect which has to be dealt with, and that is the mental element required to establish the tort. The mental element of the tort has not been settled by the courts, largely because the

[975] Privacy Act 2020, s 22 principle 7. This empirical analysis would provide stronger support for once public facts if the amendments to the Privacy Act recommended in Chapter 9 are implemented.

predominant defendants in the tort cases are the media, where the question is unlikely to arise because, as Cheer and Todd note, such "publication is hardly ever anything but intentional".[976] However, where intention is a factor, Cheer and Todd argue that absolute liability is highly unlikely and the question will be whether intention or only negligence will be required. The High Court in *Henderson v Walker* also addressed the issue, where Thomas J agreed with Cheer and Todd that absolute liability is unlikely. His Honour said such a standard:[977]

> … would be contrary to the cautious way in which the Court of Appeal decided to develop the tort in this country. It would also put the tort out of line with the law on breach of confidence which, as I have already explained, requires a relationship of confidence and that third-party recipients have at least notice that the information is confidential.

In England, Baroness Hale in *Campbell*, noted that:[978]

> The position we have reached is that the exercise of balancing arts 8 and 10 may begin when the person publishing the information *knows or ought to know* that there is a reasonable expectation that the information in question will be kept confidential.

Moreham argues that Baroness Hales's test is appropriate, as it is easy to imagine a situation where a person discloses seemingly innocuous information, only to find out that the information is other than that.[979] However, in *NT 1 & NT 2* the Court appears to utilise a strict liability test in finding that the misuse of private information cause of action was established for NT 2. It is hard to see how the deployment of algorithms to return relevant search results could mean that Google knew or ought to know that there was a reasonable expectation of privacy in the prior conviction. However, based on the development of the tort in New Zealand to date, together with the above analysis, it is difficult to see the analysis in *NT 1 & NT 2* finding favour. Therefore, a *Google Spain* type decision would need to proceed under the Privacy Act rather than under the disclosure tort. In regard to the intention required for the tort, it is more likely that the approach of Baroness Hale would find favour and the defendant would have to know, or ought to have known, that there was a reasonable expectation of privacy.

---

[976] Cheer and Todd, above n 448, at [17.5.04].
[977] *Henderson v Walker*, above n 740, at [220].
[978] *Campbell*, above n 355, at [134] (emphasis added). Note that the phrase 'confidential' is being used here to mean private (see Warby, Speker and Hirst, above n 883, at [5.08]).
[979] Moreham, above n 102, at 648.

VII Conclusion

This chapter has considered the development of the disclosure tort in New Zealand, with a focus on the two elements of the test for establishing a prima facie cause of action – a reasonable expectation of privacy, and highly offensive publicity. The research canvassed here has considered how these elements of the tort are addressed in comparative jurisdictions and also considered critiques and clarifications. These broad investigations have had two purposes: (1) to determine if the disclosure tort can protect once public facts, or, to put it another way, is it consistent with the development of the tort to conclude that there can be a reasonable expectation of privacy in some once public facts?; and (2) to determine in what (if any) ways the disclosure tort needs to be developed in order to better protect all privacy claims, including those relating to once public facts.

What the present research has found is that the current cause of action is broad enough to protect once public facts and that such protection, in the appropriate circumstances, is consistent with the tort's developments in New Zealand. However, this conclusion does not mean that refinements of the tort are not welcome or required. The chapter ultimately envisages three ways in which the disclosure tort needs to be clarified: (1) recognition of the types of circumstances that need to be taken into account when determining if there is an expectation of privacy; (2) adoption of the empirical analysis in determining if the expectation is one which society should recognise; and (3) adoption of the core values analysis. In addition, this thesis also supports abandonment of the highly offensive test.

As noted at the start of the chapter, the prima facie claim for invasion of privacy via the disclosure tort can be defeated by the legitimate public interest defence. The defence acknowledges that the right to privacy is not absolute and that protection of privacy can conflict with other important rights and interests like freedom of expression.[980] Volokh argues that "my right to control your communication of personally identifiable information about me [privacy] – is a right to have the government stop you from speaking about me."[981]

It is feared that a right to stop people and organisations speaking in the name of privacy is the start of a slippery slope, resulting in more speech restrictions,[982] press timidity and media self-

[980] See ALRC, above n 862, at 150 for a list of interests which may compete with privacy.
[981] Eugene Volokh "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You" (2000) 52 Stan L Rev 1049 at 1050–1051.
[982] At 1014–1015.

censorship.[983] These arguments have held much sway, particularly in the United States, where, as noted above, the strength of the freedom of expression challenge has resulted in some claiming the privacy tort is dead. Freedom of expression raises particular challenges for once public facts because such facts have been or continue to be 'public' and therefore, presumptively, of public concern. It is crucial that the challenge presented by freedom of expression is addressed head-on. The next chapter, therefore, discusses the right to freedom of expression, and considers how this important right is balanced against people's ongoing desire for privacy.

[983] *Cox v Cohn*, above n 806, at 1046–1047.

7 MATTERS OF LEGITIMATE PUBLIC CONCERN: PRIVACY AND FREEDOM OF EXPRESSION

I Introduction

Freedom of expression is a treasured value that is protected by many national and international instruments. Freedom of expression is valued due to its central role in democratic self-government, individual self-fulfilment, the search for truth and as a safety-valve against community instability.[984] However, as noted above, sometimes a person's right to receive or impart information can conflict with another's wish to keep information private. This conflict plays out in many of the legal mechanisms for protecting privacy discussed above. In the disclosure tort, the defence of legitimate public concern ensures that free speech considerations are central to the provision of a remedy.[985] In the Privacy Act, s 21 requires the Privacy Commissioner to consider competing rights and interests when exercising his or her statutory functions.

This chapter considers the relationship between privacy and freedom of expression, with a focus on how the legal mechanisms for protecting privacy have managed the conflict between privacy and freedom of expression and whether that management provides any presumptive protection for free speech when the information at issue is once public facts. To achieve these outcomes, the chapter proceeds as follows. First it considers why free speech is important. Understanding this is vital when free speech comes to be weighed against privacy in any individual circumstance. Second it considers the key legal mechanisms for protecting privacy and how these mechanisms have balanced privacy and free speech. The disclosure tort is a focus of this discussion; however, the discussion also considers how other legal mechanisms manage the conflict, including the Privacy Act 2020 and the work of the BSA. Third, the chapter compares and contrasts New Zealand's approach to the disclosure tort with the approaches seen in the English and United States torts. These latter two jurisdictions represent examples at opposite ends of the privacy and free speech continuum, with the United States employing a pro-speech approach and the English using an ultimate balancing approach. Both jurisdictions have deep experience with privacy and provide the opportunity for New Zealand's approach to be assessed in a meaningful way. Fourth, the chapter draws together the research to determine that the legal mechanisms for protecting privacy in New Zealand do *not* provide any presumption in favour of free speech. What is required is a consideration of

[984] See discussion in Chapter 7(II) below.
[985] See *Hosking*, above n 8, at [130].

the particular facts at issue and whether publication of those facts is proportionate to the level of public concern in the facts. However, the analysis has determined that the application of the defence could be improved. A structured framework which builds on the jurisprudence to date, along with learnings from the BSA, English and European law, could provide much needed clarity around the shape and application of the defence, especially in difficult cases, like once public facts. Clear factors would also assist would-be disclosers in determining whether an individual decision to publish private facts is likely to satisfy the defence.

II Why Free Speech?

Freedom of expression is considered a fundamental right of all human beings.[986] The importance of the right is recognised by many major international human rights documents. The Universal Declaration of Human Rights states:[987]

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The International Covenant on Civil and Political Rights states:[988]

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Freedom of expression also has a prominent place in many regional and national documents. The ECHR states:[989]

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The Charter of Fundamental Rights of the European Union states:[990]

---

[986] Cheer, above n 392, at 951 highlights that freedom of expression includes freedom of the press.
[987] *Universal Declaration of Human Rights* GA Res 217A (1948), art 19.
[988] International Covenant on Civil and Political Rights (open for signature 16 December 1966, entered into force 23 March 1976) art 19(2) [ICCPR].
[989] ECHR, art 10(1).
[990] Charter of Fundamental Rights of the European Union, art 11.

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
> 2. The freedom and pluralism of the media shall be respected.

At a national level, one of the strongest commitments to freedom of expression is the First Amendment in the United States Constitution, which states: "Congress shall make no law … abridging the freedom of speech, or of the press".[991] In Canada, the Charter of Rights and Freedoms states that everyone has "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."[992] In New Zealand, s 14 of the NZBORA states that: "Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form."[993]

While these documents demonstrate that the right is important, they do not explain why. The White Paper presented to New Zealand's House of Representatives in 1985 arguing for the Bill of Rights (White Paper) sets out four "grand purposes" in support of freedom of expression:[994]

(1) Individual fulfilment through self-expression;
(2) Democratic self-government;
(3) To advance knowledge and reveal truth; and
(4) To achieve a more adaptable and hence a more stable community.

The individual self-fulfilment justification sees freedom of expression as integral to what it means to be human. The White Paper quoted the words of Justice Brandeis in *Whitney v California*, an opinion that has been called "arguably the most important essay ever written, on or off the bench, on the meaning of the First Amendment."[995] Justice Brandeis said that: "Those who won our independence believed that the final end of the state was to make men

[991] United States Constitution, amend 1.
[992] Canadian Charter of Rights and Freedoms, s 2(b).
[993] New Zealand Bill of Rights Act 1990 [NZBORA], s 14. The NZBORA does not operate in the same way as the United States Constitution. The NZBORA is not supreme law, and the courts cannot strike laws down as contrary to the NZBORA (see NZBORA, s 4).
[994] Geoffrey W R Palmer and Ministry of Justice *A Bill of Rights for New Zealand: A White Paper* (AJHR, Wellington, 1985) AJHR A.6, at 79.
[995] Vincent Blasi "The First Amendment and the Ideal of Civic Courage: The Brandeis Opinion in *Whitney v California*" (1988) 29 W M & Mary L Rev 653 at 668, cited by Neil M Richards "The Puzzle of Brandeis, Privacy, and Speech" (2010) 63 V and L Rev 1295 at 1297.

free to develop their faculties".[996] Emerson has described the self-fulfilment justification as follows:[997]

> … every man – in the development of his own personality – has the right to form his own beliefs and opinions. And, it also follows, that he has the right to express these beliefs and opinions. Otherwise they are of little account. For expression is an integral part of the development of ideas, of mental exploration and of the affirmation of self. The power to realize his potentiality as a human being begins at this point and must extend at least this far if the whole nature of man is not to be thwarted.

One of the central and most prominent arguments for free speech is that it is critical to democratic government. The White Paper quoted Rand J of the Canadian Supreme Court, who noted that parliamentary government was driven by public opinion in an open society, but "public opinion, in order to meet such a responsibility, demands the condition of a virtually unobstructed access to and diffusion of ideas."[998] Larson describes the theory as follows:[999]

> Informed individuals are able to vote wisely, thus governing themselves through robust and effective democracy. Under this theory, "What is important is not that everyone shall speak, but that everything worth saying shall be said." This is because the self-government value of free speech inures not to the benefit of the speaker, but of society. Speech serves to inoculate the thinking process of the community so as to safeguard it from the 'mutilation' inflicted by censorship and the suppression of disfavoured ideas.

Huscroft notes that free speech is so central to democracy "that it is has been protected by the courts even in the absence of a bill of rights."[1000] Linking free speech to democratic self-government has often led to arguments about whether the full panoply of protection for free speech applies to non-political speech. However, Larson rejects these arguments, arguing that

---

[996] *Whitney v California* (1927) 274 US 357 at 375.
[997] Thomas I Emerson "Toward a General Theory of the First Amendment" (1963) 72 Yale L J 877 at 879.
[998] *Switzman v Elbling* [1957] SCR 285 at 306.
[999] Robert G Larson III "Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten are Incompatible with Free Speech" (2013) 18 Communication and Law Policy 91 at 115–116, citing Alexander Meiklejohn *Free Speech and its Relation to Self-Government* (Lawbook Exchange, Union New Jersey, 2000).
[1000] Grant Huscroft "Freedom of Expression" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney *The New Zealand Bill of Rights* (Oxford University Press, Auckland, 2003) 308 at 310, citing the High Court of Australia cases of *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106 and *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1. See also Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis NZ Ltd, Wellington, 2015) at [13.6.13].

the foundation of the theory is the idea that it is for society, not the government, to determine when everything worth saying has been said.[1001]

In the White Paper, the truth justification was supported by the words of John Stuart Mill and Justice Oliver Wendell Holmes in *Abrams v United States*. Mill, it noted, argued that suppression of opinion was wrong because "it is only by 'the collision of adverse opinions' that truth is discovered."[1002] Greenwalt also saw truth discovery at the heart of Mill's *On Liberty*, noting that:[1003]

> Mill says that if the government suppresses communications, it may suppress ideas that are true or partly true. Moreover even if an idea is wholly false, its challenge to received understanding promotes a re-examination that vitalizes truth.

Greenwalt also notes that Mill's truth is broad and encompasses "correct judgments about issues of value as well as ordinary empirical facts and embracing knowledge conducive to a satisfactory personal life as well as facts of general social importance."[1004] The White Paper's reference to *Abrams v United States* is interesting because Justice Holmes' statement in that case is often called the 'marketplace of ideas' theory, which to some theorists is different from the search for truth justification.[1005] The marketplace of ideas theory comes from the Judge's statement that "the best test of truth is the power of the thought to get itself accepted in the competition of the market."[1006] Butler and Butler note that this rationale places faith "in the market to reach the correct conclusion [the truth] provided that the market is allowed to function uninhibited by external restrictions."[1007] Greenwalt, however, challenges the marketplace of ideas theory as a justification for free speech, arguing that the theory does not independently explain why society should accept the results of the marketplace as truth, rather than some other process, "say, the results of democratically determined suppression."[1008]

Solove argues that underlying the truth justification and marketplace of ideas theories is an assumption "that the value of truth is nearly absolute"; however, he believes that at times the

---

[1001] Larson, above n 999, at 116–117. Cynthia L Estlund "Speech on Matters of Public Concern: The Perils of an Emerging First Amendment Category" (1990) 59 Geo Wash L Rev 1 at 31 similarly argued that recognising a category of protected free speech relating to matters of public concern "inevitably charges the judiciary with the task of developing an approved list of legitimate topics of public debate, a prospect that offends basic principles of democracy and freedom of expression."
[1002] Palmer, above n 994, at 79, citing Mill, above n 343, at 116.
[1003] Kent Greenawalt "Free Speech Justifications" (1989) 89 Colum L Rev 119 at 130.
[1004] At 131.
[1005] At 153. Greenawalt treats marketplace of ideas and search for truth as two separate theories.
[1006] *Abrams v United States* (1919) 250 US 616 at 630.
[1007] Butler, above n 1000, at [13.6.3].
[1008] Greenawalt, above n 1003, at 153–154.

value of truth is minimal.[1009] Solove points to the fact that much true information is trivial and useless (for example, the number of paperclips on a desk).[1010] Others point to the fact that sometimes public disclosure can *inhibit* the truth from emerging; for example, when the media is involved, often the truth is not an objective truth, but rather "what vested interests would like the truth to be."[1011]

The final purpose referred to in the White Paper sees free speech as having a critical role as society's safety valve, helping to ensure a stable society. If there is no free speech, "ideas will be driven underground and conspiracy is encouraged."[1012] Emerson describes the theory as follows:[1013]

> … suppression of expression conceals the real problems confronting a society and diverts public attention from the critical issues. It is likely to result in neglect of the grievances which are the actual basis of the unrest, and thus prevent their correction. For it both hides the extent of opposition and hardens the position of all sides, thus making a rational compromise difficult or impossible. Further, suppression drives opposition underground, leaving those suppressed either apathetic or desperate. It thus saps the vitality of the society or makes resort to force more likely.

In addition to the justifications mentioned in the White Paper, Blasi put forward a theory based on free speech's function in checking the abuse of official power, called the "checking value" theory.[1014] Blasi's theory, which has been called both a "corollary" to the democratic self-government justification[1015] and a "sub-category of the truth-discovery" justification,[1016] is premised on the belief "that the abuse of official power is an especially serious evil" (and one far more serious than abuse of private power) and that "the general populace must be the ultimate judge of the behaviour of public officials."[1017] Greenwalt summarised the theory as follows:[1018]

> … if those in power are subject to public exposure for their wrongs …, corrective action can be taken. And if public officials know they are subject to such scrutiny, they will be must less

[1009] Solove, above n 395, at 998.
[1010] At 998–999.
[1011] Butler, above n 1000, at [13.6.7].
[1012] At [13.6.15], citing *R v Secretary of State for the Home Department, ex p Simms* [2000] 2 AC 115 (HL).
[1013] Emerson, above n 997, at 884.
[1014] Vincent Blasi "The Checking Value in First Amendment Theory" (1977) Am B Found Res J 521 at 528.
[1015] Larson, above n 999, at 118.
[1016] Greenawalt, above n 1008, at 142.
[1017] Blasi, above n 1014, at 538 and 542.
[1018] Greenawalt, above n 1008, at 142.

likely to yield to the inevitable temptation presented to those with power to act in corrupt and arbitrary ways.

This brief discussion highlights that there are many different justifications for the value of free speech.[1019] Each theory demonstrates that there are fundamental and pressing reasons why modern liberal democracies have strived to uphold free speech. An understanding of these theories is crucial when discussing how the right should be treated when it rubs up against a competing right or interest, like privacy. As noted above, the courts have established the defence of legitimate public concern as the mechanism for addressing the conflict in the disclosure tort, and it is to that mechanism that the discussion now turns.

III Legitimate Public Concern Defence in New Zealand

A Common Law

It is useful to begin a discussion of the defence by considering its development prior to *Hosking*. In *Tucker,* the Court described the gravamen of the privacy action as "unwarranted publication of intimate details of the plaintiff's private life which are outside the realm of *legitimate public concern, or curiosity*."[1020] The Court considered it arguable that the public had no legitimate interest in Mr Tucker's prior convictions. Mr Tucker was an involuntary participant in the relevant publicity and should be treated differently from a person who "presented himself to the public eye for evaluation".[1021] The case is now over 30 years old; however, Tobin has argued that the current focus on proportionality in the defence in New Zealand (which is discussed below) indicates that the decision in *Tucker* "would still be good law."[1022]

In *Bradley*, Gallen J recognised that privacy must be balanced against "the significance in a free country of freedom of expression."[1023] He referred to the *Tucker* Court's reference to "private life" and "unwarranted" publicity, noting that these two adjectives "protect against disclosure of intimate details which are outside the realm of legitimate public concern or curiosity."[1024] Gallen J also noted that just because something occurs in a public place "does not necessarily mean that it should receive widespread publicity if it does not involve a matter

[1019] Huscroft, above n 1000, at 311.
[1020] *Tucker*, above n 385, at 732 (emphasis added).
[1021] At 735.
[1022] Tobin, above n 386, at 104.
[1023] *Bradley*, above n 693, at 423.
[1024] At 423.

of public concern."[1025] However, he did not go further in developing the defence (presumably because the facts of the case did not satisfy either the private facts or highly offensive tests). In *P v D*, Nicholson J similarly recognised the need to balance privacy and free speech and established, as an element of the cause of action itself rather than as a defence, a requirement to consider the "nature and extent of legitimate public interest in having the information disclosed."[1026] In discussing whether this element was satisfied in the case at hand, the Judge considered whether the disclosed information rendered the plaintiff "unfit to carry out [the plaintiff's] occupation to an appropriate standard", or whether it impacted on the public interest in the plaintiff's "character, credibility or competence".[1027] Being satisfied with neither, the Judge held that there was minimal public interest in the private facts disclosed, despite the plaintiff being a public figure.

In *Hosking* these prior developments coalesced into the defence of legitimate public interest which is now accepted as the law of New Zealand.[1028] However, while the majority was comfortable that the defence was sufficient to ensure that privacy considerations did not unduly outweigh free speech, the minority were not so convinced. The minority's position hinged on the fact that the NZBORA does not include a right to privacy. The White Paper, which excluded such a right, noted that a right to privacy was not fully recognised in New Zealand and that its "boundaries would be uncertain and contentious."[1029] Without a right to privacy in the NZBORA, privacy can only override free speech when the requirements of s 5 of the NZBORA are met. Section 5 states that a right contained in the NZBORA can only be subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[1030] Both minority judges in *Hosking* found that a disclosure tort would not be demonstrably justified under s 5.[1031] In contrast, Gault J argued that limits on the right to freedom of expression imposed to "give effect to rights declared in international conventions to which New Zealand is a party" could not seriously be held as unjustified in a free and democratic society.[1032] Central to ensuring that the disclosure tort was a reasonable limit for the majority in *Hosking* was the defence of legitimate public concern.

[1025] At 424.
[1026] *P v D*, above n 696, at [34].
[1027] At [41].
[1028] It should be noted that while the Court's description of the defence is now settled law, the Court did not actually have to apply the defence because it found there was no reasonable expectation of privacy in the information at issue (see *Hosking*, above n 8, at [170] and [260]).
[1029] Palmer, above n 994, at [10.144]. See also *Hosking*, above n 8, at [181].
[1030] NZBORA, s 5.
[1031] *Hosking*, above n 8, at [222] and [267]. The reasons given by the minority judges for a new disclosure tort being held unjustified included the fact that the law has already carefully set out protections for privacy and because of the importance of freedom of expression.
[1032] At [114]. Gault P's quote referenced ICCPR, art 7 and the United Nations Convention on the Rights of the Child 1989 (opened for signature 20 November 1989, entered into force 2 September 1990), art 16.

In discussing the defence, Gault J recognised that proportionality was an important component, noting that: "The importance of the value of the freedom of expression therefore will be related to the extent of legitimate public concern in the information publicised."[1033] He also noted that the use of the phrase 'public concern' was deliberate, employed to "distinguish between matters of general interest or curiosity to the public, and matters which are of legitimate public concern."[1034] Here, Gault J endorsed the words of Eichelbaum J in *TV3 Network Services Ltd v Broadcasting Standards Authority*, who said that: [1035]

> … there is a difference between material that is "merely interesting" to the public and material "properly within the public interest, in the sense of being of legitimate concern to the public".

Gault J also noted that proportionality considerations applied to the relationship between the expression and the privacy interests, stating that only matters that reach the higher threshold of 'public concern' are able to outweigh the "substantial breach of privacy harm the tort presupposes."[1036]

In determining what is of public concern, Gault J preferred an approach which looked to the "community, norms and values" in existence in each particular case.[1037] To this end, he endorsed the United States approach set out in the *Restatement,* as follows:[1038]

> The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern. The limitations, in other words, are those of common decency, having due regard to the freedom of the press and its reasonable leeway to choose what it will tell the public, but also due regard to the feelings of the individual and the harm that will be done to him by the exposure.

[1033] At [132]. Tipping J, at [236]–[237] and [230], also uses the language of 'balance'.
[1034] At [133].
[1035] At [133]. *TV3 Network Services Ltd v Broadcasting Standards Authority* [1995] 2 NZLR 720 (HC) was an appeal from a decision of the BSA.
[1036] *Hosking*, above n 8, at [134].
[1037] At [135].
[1038] At [135].

For the other majority decision of Tipping J, proportionality was similarly a key feature of the defence. He noted that: [1039]

> … the nature of the information imparted may well have a bearing on the reasonableness and justifiability of the limitation in issue … . The more value to society the information imparted or the type of expression in question may possess, the heavier will be the task of showing that the limitation is reasonable and justified.

However, for Tipping J the importance of the expression should be determined by its theoretical foundations, rather than community norms. Tipping J noted that freedom of expression rested on three theoretical foundations – the marketplace of ideas, maintenance and support of democracy, and liberty. He found that there is likely to be more legitimate public concern in expression which implicates the first two than expression whose only value is theoretical support of liberty.[1040] Where the expression's justification is based solely on the latter, but causes "significant individual or public harm in concrete terms", then "the theory must give way."[1041] Tipping J did note that s 5 of the NZBORA meant freedom of expression had a "head start", because any privacy interest "must pass the threshold test …, namely reasonableness, justification and prescription by law."[1042]

The defence was next discussed in *Brown*. In that case, which involved the publication of a flyer by the Police identifying the plaintiff as a recently released paedophile, the Judge believed the publication would be of public concern, but questioned whether that public concern was legitimate. To answer that question, the Judge turned to a similar English case, *R v Chief Constable of North Wales Police: ex parte Thorpe*,[1043] where the Judge had utilised a test of "pressing need in the public interest".[1044] Adopting this test, Judge Spear considered the "combined effect of all the information contained in the flyer"[1045] and determined that it went well beyond what was of legitimate public concern or establishing a pressing need in the public interest. The Judge also noted that if the 'pressing needs' test was too high a threshold, he was satisfied that the Police went well beyond any legitimate public interest or concern. In

[1039] At [235]
[1040] At [233]–[235].
[1041] At [234].
[1042] At [234].
[1043] *R v Chief Constable of North Wales Police: ex parte Thorpe* [1999] QB 396. The Judge in *Brown*, above n 391, at [88] called it the "leading" English case on the issue.
[1044] *Brown*, above n 391, at [89].
[1045] At [92].

particular, the Judge noted that the Police could have dealt with matters in a more privacy-protective way.[1046]

In *Andrews* the Court discussed the defence, even though it did not need to because the plaintiff failed to establish that the publication was highly offensive.[1047] Allan J noted that if he had applied the defence he would have upheld it because the television show complained of had a "serious underlying purpose" which was of significant public concern (the impact of road accidents on fire fighters).[1048] The fact that there was an element of entertainment to the show did not negate this conclusion. Allan J found that the disclosure was not disproportionate to its relevance. The fact that the public interest could have been served without identifying the plaintiffs was also not relevant. Ultimately he found that because the invasion of privacy (if upheld) would have been at the lower end, the "degree of public concern needed to maintain the defence would not be high."[1049] Tobin has queried why the intimate conversation at the heart of *Andrews* was not covered by the defence. She notes that the conversation added nothing to the story and that "the work of the fire fighters was easily portrayed without disclosing the conversation, where the audience became a voyeur."[1050] Cheer argues that *Andrews* relied on United States law without recognising that its law is heavily influenced by its unique constitutional approach which provides supremacy to freedom of expression and the media.[1051] It is certainly debatable whether Allan J was correct to find that there was no "morbid and sensational prying into private lives for its own sake".[1052] It is hard to see how an intimate conversation between a married couple in a very vulnerable situation provides any insight into the work of fire and emergency services at the site of road accidents.

Consideration of whether publication of the private matter would add anything to the matters of public concern was central to the High Court's decision in *Rogers*, where the Court found that it was not of legitimate public concern to broadcast evidence of a confession that had

---

[1046] At [93]. The Judge was also influenced by expert evidence that publication might enhance the risk to the public, rather than reducing it, because public shaming can inhibit attempts to rehabilitate and increase the risk of reoffending (see at [92]).
[1047] *Andrews*, above n 720, at [72].
[1048] At [92].
[1049] At [93]. See also at [84] where Allan J noted that this proportionality was supported by the court of appeal in *Rogers* (CA), above n 705, at [86]. Allan J also pointed to "the fact that only first names were used throughout the programme, the omission of any reference to drink-driving issues, the fact that the car itself was not identifiable, the significant degree (albeit incomplete) of pixilation and the generally low-key and sensitive treatment of the plaintiffs" as reasons for the privacy interest being low (see at [94]).
[1050] Tobin, above n 386, at 104.
[1051] Ursula Cheer "The Future of Privacy: Recent Legal Developments in New Zealand" (2007) 13 Canterbury L Rev 169 at 187. Allan J in *Andrews,* above n 720 relied heavily on the United States case of *Shulman v Group W Productions* 955 P 2d 469 (Cal 1998).
[1052] *Andrews*, above n 720, at [89].

been ruled inadmissible in the plaintiff's murder trial.[1053] However, the Court of Appeal came to a different conclusion. The majority in the Court of Appeal noted that, because the privacy interest at stake was on the low end, the necessary legitimate public concern only needed to be at the low end.[1054] The public right to know about excluded evidence was an important component of ensuring that the courts were open and subject to scrutiny and, therefore, the legitimate public concern test was satisfied.[1055]

Recently, the High Court in *Henderson v Walker* discussed the defence. The High Court held that there was *no* legitimate public concern in disclosing private information like "medical documents, private emails between a husband and wife and personal photographs" to the Official Assignee."[1056] There was, however, legitimate public concern in advising the Official Assignee and the Police of potential breaches of the law, especially where the information was limited to that which was relevant to "official interests".[1057] In *Peters v Bennett*, the High Court noted that whether information is of legitimate public concern "depends on the nature of the information."[1058] In the case at hand, the information was a potential benefit overpayment being disclosed by the relevant public officials to the Ministers with portfolio responsibilities for the matter. In this circumstance, the Judge held that "it was difficult to envisage a clearer example of legitimate concern".[1059]

In 2007, Cheer argued that the "conversation about the place of public interest in the New Zealand tort has … barely begun to take place."[1060] Fifteen years later, little has changed. The subsequent case law has not developed the tort much further than what was established in *Hosking*. However, one case outside the tort has provided some much needed deeper analysis on the conflict between privacy and free speech. The case – *Brooker v Police* – involved a charge of disorderly behaviour under s 4(2)(a) of the Summary Offences Act 1981. Privacy became relevant, at least to some of the Judges, because the alleged disorderly conduct was a protest by the plaintiff outside the home of an off-duty police officer.[1061]

For McGrath J, one of the minority Judges who viewed the issue as a conflict between privacy and expression, what was needed to resolve the conflict was "structured reasoning

[1053] *Rogers* (HC), above n 722, at [76]. See also the discussion at [65]–[76]. The taped confession had been ruled inadmissible because it had been obtained in breach of the plaintiff's rights.
[1054] *Rogers* (CA), above n 705, at [86].
[1055] At [88].
[1056] *Henderson v Walker*, above n 740, at [192].
[1057] At [195] and [235].
[1058] *Peters v Bennett*, above n 744, at [264].
[1059] At [266].
[1060] Cheer, above n 1051, at 187.
[1061] *Brooker*, above n 354, at [123]. Elias CJ did not see the case as involving privacy at all (at [11]).

rather than an impressionistic process."[1062] He found this structured reasoning in the Court of Appeal case of *Gisborne Herald Co Ltd v Solicitor General*, which had addressed the conflict between freedom of expression and the right to a fair trial.[1063] In *Gisborne Herald*, the Court of Appeal considered, first, whether non-speech-infringing measures could be used to adequately address the conflict. If not, then neither right had automatic precedence and what was needed was a close assessment of the:[1064]

> … importance and impact of the particular rights in the circumstances. All relevant circumstances were to be taken into account so that all interests were given due consideration according to their importance in the particular situation.

McGrath J noted that this framework was similar to the one followed in English law which required a true balancing of the relative weight of each interest in the particular circumstances.[1065] In the case at hand, the complainant was protesting about official police action which was an important aspect of free speech. On the other side, the protest took place directly outside the police officer's home and was knowingly conducted when the officer was off-duty. As such the plaintiff's actions were highly intrusive to the officer's enjoyment of her home. When weighed against each other, the officer's privacy rights outweighed the complainant's free speech rights. For McGrath, while privacy had to be a justifiable reasonable limit on freedom of expression under s 5 of the NZBORA, he held that privacy was a value which "in the abstract, is close to being as compelling as freedom of speech", and deserved to be balanced equally.[1066]

The other minority judge, Thomas J, rejected outright the NZBORA, s 5 "framework of justification"[1067] and advocated for privacy to assume its deserved position as a recognised right. Thomas J believed the *right* to privacy should be subject to s 28 of the NZBORA, which states that existing rights are not "abrogated or restricted by reason only that the right or freedom is not included in this Bill of Rights".[1068] For Thomas J, recognition that privacy is a right not abrogated under s 28 would allow a straightforward balancing of two rights, with "equal standing."[1069] However, he noted that privacy had "not yet been judicially accorded the

---

[1062] At [132].
[1063] At [131]. *Gisborne Herald Co Ltd v Solicitor General* [1995] 3 NZLR 563 (CA).
[1064] *Brooker*, above n 354, at [131].
[1065] At [134]. See the discussion of English law in Chapter 7(IV)(D) below.
[1066] At [129].
[1067] At [231]–[232].
[1068] At [164] and [165]. Thomas J does note that if he took a s 5 approach, he would have endorsed the decision of McGrath J (at [232]). See at [214]–[225] for a discussion of why Thomas J believes privacy is an existing right that should not be abrogated under s 28.
[1069] At [209].

status of a right";[1070] therefore he sought an alternative route to avoid the s 5 justificatory framework, yet allow himself to balance privacy and free speech *equally*. He found the alternative route by viewing the case as a contest between two citizens rather than between the state and a citizen, and declaring that it would be inappropriate to consider rights and their limits under s 5. As a contest between two citizens, he argued, what was important were the *values* of privacy and free speech, and neither had paramount status.[1071] While Cheer questions the validity of Thomas J's reasoning,[1072] it is clear the Judge wanted to get to a position where he could weigh two equal rights or values. However, contrary to McGrath J, Thomas J believed that viewing the case within the s 5 justificatory framework did now allow such equal weighting. Ignoring the difference between balancing a right and a limit and a right and another right, would be a "judicial pretence."[1073] For Thomas J, when the balancing exercise is between a right and a limit, "the right tends to assume a dominant status" and "Judges will be prone to import a presumption in favour of the right."[1074]

The NZLC, however, disagrees. In discussing the two approaches – a s 5 justification or a s 28 balancing of two rights – the NZLC stated:[1075]

> While the starting points for the two approaches may seem different, it is difficult to see that in the ultimate analysis they will produce any different result, given that both approaches involve what Lord Steyn refers to as an "intense focus on the comparative importance of the specific rights being claimed in the individual case."

In conducting the actual balancing exercise on the facts of the case, Thomas J was influenced by Tipping J's analysis in *Hosking,* which linked the value of the expression to its theoretical drivers. He found that Mr Brooker's protest did not support the marketplace of ideas because he was essentially expressing a personal grievance against the police officer. He noted that a robust democracy requires the ability to protest police behaviour, but in this case Mr Brooker's chosen form of protest outside the police officer's home did not make a significant contribution to democracy[1076] Mr Brooker could have chosen to conduct his protest in another way – for example, outside a police station. Ultimately, Thomas J concluded that Mr

---

[1070] At [164].
[1071] At [212].
[1072] Cheer, above n 1051, at 196 rejects Thomas J's approach here, calling it a "sleight of hand." She notes that it was misleading to say the case was about a contest between citizen and citizen, when ultimately the case was about the application of criminal law to Mr Brooker and involved the important state interest of public order.
[1073] *Brooker*, above n 354, at [211].
[1074] At [211].
[1075] Law Commission, above n 76, at [8.14].
[1076] *Brooker*, above n 354, at [246].

Brooker's protest was of minimal public benefit and it did not "attract conspicuous value in serving any of the recognised theories or bases upon with the right to freedom of expression is based."[1077] On the other side, Mr Brooker's protest disrupted the seclusion and sanctity of the home, a "vital aspect of privacy".[1078] The value of the privacy interest at stake was, therefore, high and outweighed the value of the expressive activity.

B Conclusions on the Common Law

The New Zealand case law shows that while freedom of expression is important, it is not absolute. Privacy interests have been held to outweigh the right to freedom of expression when the matter disclosed is not of legitimate public concern. Proportionality is also a key component of the defence. The weight given to freedom of expression must be proportionate to the level of public concern in the information. The level of public concern must be proportionate to the gravity of the privacy invasion to outweigh it. Proportionality requires a weighing of the interests on both sides of the equation. However, there has been some disagreement about how the level of public concern should be determined. Gault J in *Hosking* and the Court in *Andrews* preferred the *Restatement's* approach. In contrast, Tipping J in *Hosking* and Thomas J in *Brooker* preferred an approach which considered the extent to which a particular exercise of the right of freedom of expression serves the fundamental rationales of free speech.

What is not disputed, however, is that the courts are comfortable making determinations of what is of legitimate public concern. In no case has a court resorted to simply accepting that, if the media published the matter, it was clearly of public concern. In fact Tipping J disclaimed this approach, when he stated that: "Society cannot be expected to vest unrestrained or insufficiently restrained power in the news media and others under the banner of freedom of expression."[1079]

The case law also demonstrates that categories or generalisations about information – that the information is a public record, occurred in a public place, or the person concerned is a public figure – do not appear to hold sway in determining if a matter is of legitimate public concern. What is required is a fact-specific analysis, based on the nature of the information. A fact-specific approach is good news for once public facts. It means the circumstances of each case will be considered on their merits.

[1077] At [251].
[1078] At [256] and [262].
[1079] *Hosking*, above n 8, at [231]. See also Gault J's comments at [132].

However, there does not appear to be a clear framework in which to answer the question of whether a matter is of legitimate public concern. The cases appear to simply apply the test, which runs the risk of being seen as an 'impressionistic process' or one where the most deserving party wins.[1080] The application of the defence could be improved by establishing a structured framework to guide decision-makers. The framework does not need to be a rigid checklist, but rather a list of factors to guide decision-making. Clear factors would also assist would-be disclosers in determining whether an individual decision to publish private facts is likely to satisfy the defence, especially in difficult cases, like those involving once public facts. However, before attempting to establish such a framework, the wider context of balancing privacy and freedom of expression must be considered. As discussed in Chapter 6, the BSA privacy jurisprudence has exerted some influence on the development of the disclosure tort; therefore it is useful to consider how the BSA has balanced privacy and free speech, especially in determining whether there is any presumption in favour of free speech that would exclude protection for once public facts. In addition, because once public facts have been protected under data protection statutes in other jurisdictions, and once public facts can easily come into conflict with free speech, it is also useful to consider how the Privacy Act 2020 balances free speech and privacy. Before moving on, however, a final word on the status of privacy is warranted.

Thomas J in *Brooker* raised the issue of whether it is still appropriate to consider privacy as a reasonable limit rather than a right itself. There is considerably more recognition of privacy than when the White Paper made its recommendations in 1985. Privacy interests are now recognised in two tort causes of action,[1081] the Privacy Act has been recently strengthened, the HDCA recognises that digital communications should not disclose sensitive personal information about individuals,[1082] and the BSA continues its work to provide practical privacy protection in regard to a broad range of public broadcast mediums. Furthermore, while judges do not appear to have struggled to utilise an appropriate balance of competing values under the s 5 justificatory framework, this does not mean that a presumption in favour of free speech will not creep in at some stage. Such a presumption is likely to arise where the values are relatively evenly weighted, there is a lack of understanding of the privacy values or benefits at issue, or decision-makers resort to simple generalisations about certain types of information or people. In such situations, the temptation to consciously or unconsciously bias the right

[1080] See Cheer, above n 1051, at 189.
[1081] See *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672 which establishes an intrusion upon seclusion privacy tort in New Zealand.
[1082] The Harmful Digital Communications Act 2015 [HDCA] is discussed in Chapter 8.

over the limit might be enough to tip the balance in favour of free speech. A recognition of privacy as a right would mitigate this risk.[1083] Therefore this thesis argues that privacy should be recognised as an affirmed right under the NZBORA (or even included as a right in the NZBORA).

IV Other New Zealand Approaches: Broadcasting Standards Authority, NZ Media Council and Privacy Act 2020

A Broadcasting Standards Authority

It will be remembered from Chapter 6 that the Broadcasting Act sets up a framework for considering privacy complaints against broadcasters and the Codebook sets out the privacy standards broadcasters must meet. The Codebook recognises that privacy can conflict with freedom of expression. It views freedom of expression as a fundamental freedom that, while not absolute, must be given "high value" and which may impose a cost to society.[1084] The Codebook acknowledges that a privacy complaint can be upheld only if it is a reasonable limit demonstrably justified in a free and democratic society. To surmount this hurdle, a proportionality assessment is required which weighs up the harms on both sides.[1085] The weight given to freedom of expression is measured by the level of public interest in a matter. Matters involving politics, governance or governmental accountability, the search for truth, and nurturing of "our social, cultural or intellectual growth" have high public interest.[1086] On the other side are interests in ensuring that broadcasts neither misinform society of important matters nor unfairly harm the dignity or reputation of individuals.

The privacy standard in the Codebook states:[1087]

> 10(d) It is a defence to a privacy complaint to publicly disclose matters of legitimate public interest. The level of public interest must be proportionate to the seriousness of the breach of privacy in order for the defence to apply.

[1083] See Cheer, above n 1051, at 197 who supports this view. See also Petra Butler "The Case for a Right to Privacy in the New Zealand Bill of Rights Act" (2013) 11 NZJPIL 213 who argues that privacy should be included as a right in the NZBORA.
[1084] *BSA Codebook*, above n 748, at 6.
[1085] At 6.
[1086] At 6.
[1087] At 41.

Public interest is defined as a "matter of concern to, or having the potential to affect, a significant section of the New Zealand population. It is more than something that merely interests the public."[1088] Guidance is given about the specific matters that *may* be of legitimate public interest. These are:[1089]

- criminal matters, including exposing or detecting crime
- issues of public health or safety
- matters of politics, government or public administration
- matters relating to the conduct of organisations which impact on the public
- exposing misleading claims made by individuals or organisations
- exposing seriously antisocial and harmful conduct.

The Codebook notes that the proportionality assessment must focus on the particular part of the broadcast which is claimed to breach privacy, so the public interest must be in that part not just in the broadcast as a whole.

There is much in the Codebook which reflects the disclosure tort and its jurisprudence to date. The Codebook recognises the importance of freedom of expression, but also that it is not absolute. What is required is a balancing between the underlying value of freedom of expression and the value of privacy. The Codebook also utilises a similar distinction between public concern and mere general interest, and a clear focus on proportionality. Furthermore, the BSA jurisprudence demonstrates that it is not afraid to uphold privacy over free speech in appropriate circumstances.

The BSA has upheld privacy where the footage complained of made no contribution to the wider public interest in the broadcast and was only included to "sensationalise a distasteful but unremarkable discovery, and to create the impression that … actions were somehow sinister and improper."[1090] Privacy has also won where the Authority found that the public interest could be satisfied without identifying the complainant.[1091] The Authority has found a breach of privacy where photos taken from a publicly accessible Facebook page were published to a wider audience without consent. In this case the BSA noted that "the

[1088] At 9.
[1089] At 61. These principles derive from *Balfour v Television New Zealand Ltd* 21/3/06, BSA Decision No 2005-129 at [61] where the BSA noted that the list was not exhaustive and that: "Each situation must be determined on its own particular facts; the essential element in every case is that the material being broadcast must be of importance and concern to the New Zealand public generally." This list was approved by Harrison J in *CanWest TV Works Ltd v XY* [2008] NZAR 1 at [57].
[1090] *Balfour,* above n 1089, at [63].
[1091] *SW v Television New Zealand Ltd* 18/12/2015, BSA Decision No 2015-030 at [35].

publication of content on one platform does not automatically justify further republication on another platform, to a national audience, without consideration of the standards that apply."[1092]

Even matters that are mentioned in the Codebook may not be sufficient to support the defence. In *MA v Television New Zealand Ltd*, the Police were filmed executing a search at the complainant's home and arresting him for possession of cannabis. The BSA found that the invasion of privacy in this instance was significant and therefore a high degree of public concern was required. However, the public interest in the identification of such a minor offence did not meet this standard.[1093] The Authority noted:[1094]

> The broadcaster should not simply proceed on the basis that any crime, no matter how minor, warrants an invasion of privacy. Particularly where an individual is filmed inside their private home, which we have found to be a serious intrusion, the broadcaster must ensure that a proportionately high degree of public interest justifies the broadcast of the footage.

The BSA has also considered some once public fact scenarios. In *T v Television New Zealand Ltd*, a year-old conviction for fraud was held to be of legitimate public interest to a broadcast addressing current (but different) fraud of the same student loan scheme.[1095] In contrast, in *FS v Television New Zealand Limited*, the Authority found that the re-broadcast of footage filmed three years previously had "become stale and would no longer have a live public interest."[1096]

Moreham has described the BSA's approach to the defence as "balanced and consistent with common law authority."[1097] In coming to this conclusion, Moreham noted the BSA's distinction between matters of genuine public concern and mere interest, and its use of the proportionality approach. The BSA also appears to be continuing the common law trends in regard to once public facts – no broad acceptance that public information like criminal offending is automatically a matter of public concern, no rigid exclusion for information previously published in the media, and use of the proportionality test to determine if the actual public concern in the matter outweighs the privacy invasion. Whether matters could have

---

[1092] *Rickard v Television New Zealand Ltd* 19/04/17, BSA Decision No 2016-098 at [24]. See also *IY v Mediaworks TV Ltd* 5/09/2018, BSA Decision No 2018-032 at [18].
[1093] *MA v TVNZ Ltd*, above n 758, at [50].
[1094] At [58].
[1095] *T v Television New Zealand Ltd* 1/10/98, BSA Decision No 1998-119.
[1096] *FS*, above n 442, at [35]. This decision involved the filming of an environmental health officer's inspection of the complainant's fish and chip shop, and the re-broadcast of the footage three years later (it had been broadcast earlier, but that broadcast was not complained about). The BSA held that any public interest in the food safety did not justify it being re-broadcast three years later.
[1097] Moreham, above n 760, at 19.

been dealt with in a more privacy-sensitive manner also shows some influence in determining the weight of the defence.[1098] There are, in addition, some innovations in the BSA's approach to the defence; in particular, its requirement for public concern to relate specifically to the privacy-invading matter and not just the broadcast as a whole. Moreham argued that this approach is necessary because:[1099]

> … without it a broadcaster would be free to use intrusive footage to liven up any broadcast as long as the programme as a whole dealt with a matter in the public interest and the relevant footage is tangentially related to it.

B NZ Media Council

The second body which regulates media activity and addresses the conflict between privacy and free speech is the NZ Media Council, formerly the Press Council. Unlike the BSA, which is an independent body, the Media Council is a self-regulatory body entirely funded by its industry members.[1100] The Media Council takes complaints about print media (including newspapers and magazines) and online content of broadcasters and digital sites with news content. The Media Council has released a Statement of Principles setting out how publications should operate. These are more informal and less detailed than the BSA, but do include privacy. Principle 2 states:[1101]

> Everyone is normally entitled to privacy of person, space and personal information, and these rights should be respected by publications. Nevertheless the right of privacy should not interfere with publication of significant matters of public record or public interest. Publications should exercise particular care and discretion before identifying relatives of persons convicted or accused of crime where the reference to them is not relevant to the matter reported. Those suffering from trauma or grief call for special consideration.

However, Principle 2 must be put in the context of the Media Council's overarching comments about freedom of expression, which are set out as a preamble to the Principles. The Media Council states:[1102]

> There is no more important principle in a democracy than freedom of expression. Freedom of expression and freedom of the media are inextricably bound … In dealing with complaints,

---

[1098] See *SW v Television New Zealand Ltd*, above n 1091.
[1099] Moreham, above n 760, at 20.
[1100] See Tobin, above n 748, at 247–251 for a discussion of the Press Council.
[1101] NZ Media Council "Principles" (last accessed 3 March 2021) <www.mediacouncil.org.nz>.
[1102] NZ Media Council "Principles".

> the Council will give primary consideration to freedom of expression and the public interest. Public interest is defined as involving a matter capable of affecting the people at large so that they might be legitimately interested in, or concerned about, what is going on, or what may happen to them or to others.

It is instantly noticeable that, contrary to both common law and the BSA, the Media Council starts with a presumption in favour of freedom of expression, and public interest is determined more broadly. That said, Tobin notes that, in making its decisions, the Council "has some regard to developments in the Common Law and the general jurisprudence of the BSA."[1103] This pro-speech approach likely drives the Media Council's reluctance to protect publications of matters that occur in the public or relate to public persons.[1104] However, there are limits to the Media Council's pro-speech approach. Children appear to obtain greater protection, even where their parents are public figures.[1105] Similarly, the use of photographs has garnered more protection, especially where they involve children or vulnerable persons.[1106]

There are many factors which limit the usefulness of the Media Council decisions, including the brevity of the principles and the decisions themselves, and the fact that its work is not influenced by the development of the common law. That said, it is useful to acknowledge that even in an environment where free speech is primary, the industry is prepared to recognise the need for privacy and to uphold its primacy in appropriate circumstances.

C Privacy Act 2020

The role that freedom of expression plays in the Privacy Act is markedly different from that in the tort or via the BSA or the Media Council. The Act does not provide guidance on how to resolve conflicts between privacy and competing interests like expression; rather, it is an example of the *outcome* of a prior balancing between privacy and competing interests. This *external b*alancing occurs during the making of the rules and "precedes the formulation of a rule which reconciles both interests in what is seen as the most appropriate way."[1107] The result of this external balancing is seen in various components of the Privacy Act, including the news media exemption and in various exemptions to the IPPs themselves.[1108]

[1103] Tobin, above n 748, at 248.
[1104] At 248–249.
[1105] At 251. The case reference is: *Hon Bill English v The Southland Times* Case No 2019, 2008, February 2008.
[1106] Cheer, above n 392, at 873.
[1107] Law Commission, above n 76 at [8.20]. See generally at [8.19]–[8.27].
[1108] Law Commission, above n 293, at [2.28]. See also Law Commission, above n 654, at [4.25]–[4.47] for a discussion of the news media exemption. An example of the prior balance can be seen in IPP 11, where there is an exemption for publicly available personal information. However, it should be noted that the news media

The Privacy Act also contains *internal* balancing, where the balancing is delegated by the rules themselves to those who apply or enforce the law.[1109] Section 21(a) is an example of this type of balancing, where the Privacy Commissioner must have due regard to other rights and interests when exercising his or her powers under the Act.[1110] Internal balancing is also evident in the rules regarding access to personal information, where agencies must balance the public interest in making information available against commercial interests like disclosure of trade secrets or prejudice to a person's commercial situation.[1111]

For those who comply with the Privacy Act, application of the rules themselves will generally ensure that an appropriate balance is being made between privacy and expression in each particular instance. However, a recent Canadian case has highlighted that this conclusion is not necessarily watertight. In *Information and Privacy Commissioner of Alberta v United Food and Commercial Workers, Local 401*, the Supreme Court of Canada held that Alberta's Personal Information Protection Act 2003 (PIPA), which is a provincial statute substantially similar to the federal PIPEDA,[1112] did not adequately address freedom of expression in accordance with the Canadian Charter.[1113] The case related to the publication of photographs of people who had crossed a picket line during a lawful strike. The Privacy Commissioner of Alberta initially upheld the complaint on the basis of an unlawful collection, use and disclosure of personal information. On appeal, it was held that the publication of the photos was an expressive activity, the restriction of which by the PIPA was not reasonably justified under the Charter.[1114] The Court held that in the context of the case, the PIPA was not a proportionate response to the privacy interests being pursued by the Act. The Court held that the privacy interest at issue was actually quite weak, yet it was still legislatively protected by the PIPA.[1115]

---

exemption is not a complete external balancing. In interpreting whether the exemption applies, decision bodies need to interpret the meaning of 'news entity' and 'news activities' (see Privacy Act 2020, s 8) and in doing so a level of internal balancing in occurring.

[1109] Law Commission, above n 76, at [8.22].

[1110] Privacy Act 2020, s 21(a).

[1111] Section 55.

[1112] Alberta's Personal Information Protection Act, S.A.2003, c.P-6.5. See Chris D L Hunt "The Future of Privacy: The Conflict with Free Expression" (2015) 43 Advoc Q 391 at 395.

[1113] *Information and Privacy Commissioner of Alberta v United Food and Commercial Workers, Local 401* (2013) SCR 733.

[1114] Canadian Charter of Rights and Freedoms, s 1. This section states that: "The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

[1115] *Information and Privacy Commissioner of Alberta*, above n 1113, at [26]. For a discussion of the case see Hunt, above n 1112.

The simplest way to address the constitutional challenge from the case was to exempt union expression during a strike, similar to existing journalistic expression exemptions.[1116] However, Hunt disagrees with this approach. He argues that such an exemption would not solve the structural issue of the PIPA, which he said was at the heart of the Supreme Court's decision. He stated that:[1117]

> Expressed in more general terms, the essential problem is this: *PIPA* (like other Canadian data protection statutes) appears by its structure to order *a priori* all privacy claims above most exercises of free expression, because all "personal information" is protected but all speech is not - unless it can be fitted into a discrete legislative exception (such as literary, artistic or journalistic purposes).

For Hunt, simply excluding labour speech does not solve the issue; rather, it upholds the structural problem, because such speech becomes *a priori* above privacy. Hunt's solution is to establish a new structure for analysis under the Act, "one that examines the contextual importance of each right, and permits, on a case-by-case basis, the more valuable right to prevail."[1118]

Whether the Privacy Act 2020 could withstand a similar challenge is not a question the present research needs to consider. However, the case does raise the spectre that the balance between expression and privacy might need more consideration should New Zealand adopt a right to erasure, as discussed in Chapter 5. Overseas experience of rights to erasure demonstrate that that the right operates in ways that particularly implicates expression – for example, search engines – and, if introduced, the erasure decision (in the first instance) would be made by the agency itself, not the Privacy Commissioner, so s 21 would not apply.[1119] Accordingly, the Act itself would need to expressly direct the agency to conduct a balancing exercise. This direction exists in the GDPR, where art 17(3) allows the continued processing of data subject to an erasure request where the processing is required to support freedom of expression. In framing any erasure tool in New Zealand, consideration should be given, therefore, to balancing privacy with freedom of expression. This balancing is discussed further in Chapter 9.

[1116] Hunt, above n 1112, at 400–401.
[1117] At 402.
[1118] At 403.
[1119] While there is some debate over whether the balancing required by s 21 applies to the Tribunal (see Gehan Gunasekara "Making a Difference? The Privacy Act and Employment Relationship Problems in New Zealand" (2018) 28 NZULR 25 at 31 and Roth, above n 589, at PVA14.3), the provision "does not impose any duties on the party that is named as the defendant" (see *O'Neill v Health and Disability Commissioner* (12 February 2003) HRRT 45/02).

V Legitimate Public Concern in the United States

In the United States the disclosure tort can only be established if the private matter "is not of legitimate concern of the public."[1120] The *Restatement* states the following about the test:[1121]

> The common law has long recognized that the public has a proper interest in learning about many matters. When the subject-matter of the publicity is of legitimate public concern, there is no invasion of privacy. This has now become a rule not just of the common law of torts, but of the Federal Constitution as well.

The absence of legitimate public concern is part of the test for establishing the cause of action, rather than being a defence. Therefore, it is for the plaintiff to prove an absence of legitimate public concern rather than the defendant proving such public concern.[1122] To determine what is of legitimate public concern – or newsworthy, as it is also called – the courts have utilised a number of tests, although all have resulted in limited practical protection for privacy.[1123] Solove has identified three such tests, as follows:[1124]

> (1) deferring to the media; (2) focusing on the status of the individual, e.g. whether she is a public or private figure; and (3) examining the nature of the information, e.g. whether it relates to public affairs or matters typically considered private, such as sex and health.

The "deferring to the media" (or "leave-it-to-the-press")[1125] test does what is says on the box – it contends that anything printed by the media is newsworthy because the media's role is to provide the public with the information the public wants. The *Restatement* alludes to this approach when it states:[1126]

> Included within the scope of legitimate public concern are matters of the kind customarily regarded as "news." To a considerable extent, in accordance with the mores of the community, the publishers and broadcasters have themselves defined the term … .

[1120] *Restatement*, above n 210, at § 652D.
[1121] At § 652D, cmt d.
[1122] Penk, above n 834, at 146.
[1123] Jaime A Madell "The Poster's Plight: Bringing the Public Disclosure Tort Online" (2011) 66 N Y U Ann Surv Am L 895 at 917.
[1124] Solove, above n 395, at 1001.
[1125] At 1001. See also Diane L Zimmerman "Requiem for a Heavyweight: A Farewell to Warren and Brandeis' Privacy Tort" 68 Cornell L Rev 291 at 353.
[1126] *Restatement,* above n 210, at § 652D cmt g.

Solove, however, rejects this approach. He argues that media does not just respond to what the public wants, it shapes it. Furthermore, determining what is of public concern is such an important decision, it should not be left to just one body.[1127] Others highlight that the approach renders the tort protection meaningless against media defendants, who are often the main invaders of privacy.[1128]

Focusing on the status of the person claiming the invasion has led to some clear outcomes. There is no privacy for persons who voluntarily assume a public role, at least in relation to their conduct and activities in their capacity as a public figure. This rule generally applies whether the person is a public official, celebrity or other famous or well known person.[1129] It is also arguable that the legitimate interest of the public in the person may result in the person loosing privacy in relation "to matters that would otherwise be private."[1130] Those associated with public figures also lose a certain amount of privacy.[1131] Involuntary public figures may also have limited privacy, especially in regard to the conduct or incident that brought them fame in the first place. In *Smith v National Broadcasting Co*, making a false report to the Police regarding the escape of a black panther meant that the plaintiff had become "stamped with the imprint of public notoriety and renounced his right to privacy insofar as this particular incident was concerned".[1132]

The passage of time does not negate newsworthiness. In *Sidis* the Court held that the history and fate of Mr Sidis were of public concern as they answered the question of whether or not he had fulfilled his early promise.[1133] Similarly, in *O'Hilderbrandt v Columbia Broadcasting System Inc*, the passage of almost 50 years since the plaintiff had relinquished her career as a film actress and retired from public view did not mean she was not a person in whom there was some public interest.[1134]

[1127] Solove, above n 395, at 1001–1008.
[1128] Jurata, above n 825, at 505–506.
[1129] *Restatement,* above n 210, at § 652D cmt e.
[1130] At § 652D cmt e. See *Rawlins v Hutchinson Publishing Co* 543 P 2d 988 (Kan 1975) at 996 where the publication of information about a police officer's alleged misconduct in office 10 years previously did not become private. See also *Werner v Times-Mirror Co* 193 Cal App 2d 111 (1961), where the plaintiff was held to have relinquished all privacy to reported matters from 30 years previously when the plaintiff had been a "public personage".
[1131] See *Carlisle v Fawcett Publications Inc* 201 Cal App 2d 733 (1962) at 746 where the former husband of a well known actress had no right of privacy to the fact of their very short marriage and annulment 18 years previously. In dealing with the lapse of time, the Court noted that if all the necessary elements are present to allow publication then "mere lapse of time does not prohibit publication."
[1132] *Smith v National Broadcasting Co* 292 P 2d 600 (Cal App 1956) at 603.
[1133] *Sidis*, above n 11, at 809.
[1134] *O'Hilderbrandt v Columbia Broadcasting System Inc* 40 Cal App 3d 323 (1974) at 329.

Tests which focus on the nature of information have generally found that information on the public record or information that is otherwise of a public nature is not protected and can be republished at will. However, some particularly private matters have been held not to be newsworthy. The *Restatement* draws the line between the "giving of information to which the public is entitled" and that which is a "morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern."[1135] This line is to be determined in accordance with the "customs and conventions of the community".[1136] However, the *Restatement* states that the line should reflect:[1137]

> … common decency, having due regard to the freedom of the press and its reasonable leeway to choose what it will tell the public, but also due regard to the feelings of the individual and the harm that will be done to him by the exposure.

Solove argues that this distinction between free speech on public and private matters is appropriate and constitutional. He points to *Dun & Bradstreet Inc v Greenmoss Builders Inc,* where a plurality of the Supreme Court, in a defamation case, noted that: "We have long recognized that not all speech is of equal importance" and that: "It is speech on 'matters of public concern' that is 'at the heart of the First Amendment's protection.'"[1138] In contrast, private speech, the Court states:[1139]

> … [poses] no threat to the free and robust debate of public issues; there is no potential interference with a meaningful dialogue of ideas concerning self-government; and there is no threat of liability causing a reaction of self-censorship by the press.

Solove argues that privacy interests do not engage most predominant theories of free speech and, in fact, can assist in advancing the aims of those theories.[1140] He argues that privacy allows for the incubation of ideas, allowing the ideas to be refined before being exposed to the world. Privacy can also enhance democracy by encouraging conversations and speech that might not happen if nothing were private or anonymous.[1141] Roessler similarly argues that

---

[1135] *Restatement,* above n 210, at § 652D cmt h.
[1136] At § 652D cmt h.
[1137] At § 652D cmt h.
[1138] *Dun & Bradstreet Inc v Greenmoss Builders Inc* 472 US 749 (1985) at 758–759. Solove, above n 395, at 987 argues that this case should have wider application than just the law of defamation.
[1139] *Dun & Bradstreet*, above n 1138, at 760. It should be noted that the plurality were not advocating for no First Amendment protection for private speech; rather "less stringent" protection. In the case itself, the information – a false credit report issued to a small number of subscribers – was held by the plurality to be private speech.
[1140] Solove, above n 395, at 993.
[1141] At 993–994.

without some protection of privacy "citizens cannot make use of their democratic liberties".[1142] She argues that: "When one cannot be sure that one is not being observed and controlled, one can no longer engage in open and autonomous critical debate with others."[1143]

However, not all agree. The dissent in *Dun & Bradstreet* argued that private speech has the same degree of First Amendment protection as public speech. Justice Brennan reasoned that:[1144]

> … the choices we make when we step into the voting booth may well be the products of what we have learned from the myriad of daily economic and social phenomenon that surround us.

Volokh also believes there is constitutional value in private speech. He argues that private speech on what he calls "daily life matters":[1145]

> … indirectly, but deeply affects the way we view the world, deal with others, evaluate their moral claims on us, and even vote; and its effect is probably greater than that of most of the paintings we see or the editorials we read.

He also argues that it is simply "not the government's job to decide what subjects speakers and listeners should concern themselves with."[1146]

In addition to the three tests identified by Solove, other have been identified. In California, a test that focused on: (1) the social use of the published facts; (2) the extent of the intrusion into allegedly private affairs; and (3) the extent to which the plaintiff consented to a position of public fame found support for a period of time.[1147] However, it has been argued that this test has now been superseded by the "logical-nexus" test, which looks for "a logical relationship between the plaintiff and a matter of legitimate public concern."[1148] The logical nexus test has generally been applied in cases involving private people who become caught up in events of public interest. The test was used in *Shulman v Group W Productions*, which involved the filming and broadcast of the aftermath of a serious road accident where the plaintiff was left a paraplegic. The plaintiff had been filmed at the scene and in a rescue

---

[1142] Beate Roessler "Privacy as a Human Right" (2017) Proceedings of the Aristotelian Society, Vol CXVII, Part 2 187 at 202.
[1143] At 203.
[1144] *Dun & Bradstreet*, above n 1138, at 788.
[1145] Volokh, above n 981, at 1093.
[1146] At 1089. See also Estlund, above n 1001.
[1147] See *Kapellas v Koffman* 459 P 2d 912 (Cal 1969); *Diaz v Oakland Tribune Inc* 139 Cal App 3d 118 (1983); and *Briscoe*, above n 9.
[1148] Jurata, above n 825, at 508.

helicopter, and her conversations with the attending nurse, along with some medical information, had been broadcast in a reality television show. Employing the logical nexus test, the Supreme Court of California rejected an argument that broadcasting the plaintiff's medical facts and clear distress was not necessary. It also did not matter that the broadcast could have been edited to remove these parts. The information was relevant to the broadcast as a whole and therefore of legitimate public concern. The Court stated:[1149]

> The challenged material was thus substantially relevant to the newsworthy subject matter of the broadcast and did not constitute a "morbid and sensational prying into private lives for its own sake." Nor can we say the broadcast material was so lurid and sensational in emotional tone, or so intensely personal in content, as to make its intrusiveness disproportionate to its relevance.

The potential breadth of the logical nexus test is visible in *Shulman*. Similarly, in *Howard v Des Moines Register & Tribune Co*, the test was used to hold that the disclosure of a minor's involuntarily sterilisation was not a breach of privacy because it "offered a personalized frame of reference to which the reader could relate, fostering perception and understanding."[1150] If identification of the plaintiff in relation to such highly sensitive and intimate information as seen in *Des Moines* is held to be relevant to the overall public interest in a broadcast, it is difficult to see what would not satisfy the logical nexus test.

The privilege which is given to the media and the breadth of what is considered of legitimate public concern reflects the United States' strong commitment to the First Amendment. So strong is this commitment that it has been argued that there should be "no abridgment of the rights of free speech".[1151] These absolutists argue that any limit on free speech is unconstitutional and privacy protections like those seen in the disclosure tort are "difficult to defend."[1152] An absolutist vision would require disclosure of personal information to be classified as action rather than speech in order to gain protection. However, such approaches can result in illogical distinctions that often cloak "the real normative reasons for why society wants to permit greater regulation of certain communicative activity."[1153]

While the United States approach is useful, because it provides a considerably larger pool of jurisprudence than New Zealand and its cases have exerted influence on the development of

[1149] *Shulman,* above n 1051, at 488. Shulman was referred to by the Judge in *Andrews*, above n 720.
[1150] *Howard v Des Moines Register & Tribune Co* 283 NW 2d 289 (Iowa1979) at 303.
[1151] *Konigsberg v State Bar of California* 366 US 36 (1961) at 61. See also Solove, above n 395, at 978.
[1152] Solove, above n 395, at 978. See also Jurata, above n 825, at 503–504 who discussed this absolutist approach and noted that a few jurisdictions in the United States refuse to uphold the existence of the disclosure tort.
[1153] Solove, above n 395, at 981. For the full discussion of Solove's argument see at 978–981.

the tort in New Zealand, it must be recognised that the tort operates in a substantially different constitutional environment to New Zealand. The predominance given to the First Amendment in the United States is not reflected in New Zealand, where the courts have been clear that while free speech is important it is not absolute. Furthermore, the New Zealand courts have seen past the empty rhetoric in the United States disclosure tort, recognising that the tort proclaims more than it actually provides.[1154]

VI The Ultimate Balancing Test: Privacy and Free Speech in English Law

The second part of the English misuse of private information tort requires a balancing of the ECHR's art 8 right to privacy and art 10 right to freedom of expression.[1155] The balancing requires consideration of four factors. These factors were articulated by Lord Steyn in *Re S (a child)* as follows:[1156]

> First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each. For convenience I will call this the ultimate balancing test.

The "intense focus" required by the test has resulted in the courts rejecting the general approach seen in the United States. For example, it has been stated that:[1157]

> This modern approach of applying an "intense focus" is thus obviously incompatible with making broad generalisations of the kind to which the media often resorted in the past such as, for example, "Public figures must expect to have less privacy" … Some facts of this kind may have a legitimate role to play when the "ultimate balancing exercise" comes to be carried out, but generalisations can never be determinative.

The proportionality test requires consideration of whether the extent of the privacy interest justifies the curtailment of the right to freedom of expression *and* whether the extent of the public interest in the expressive activity is sufficient to justify the invasion of privacy. It is a

---

[1154] *Hosking*, above n 8, at [76].
[1155] *Murray*, above n 732, at [35]–[40]. See also *Campbell,* above n 355, at [21]; *Mosley*, above n 886, at [10]; and Barendt, above n 886, at 102.
[1156] *Re S (a child)* [2004] UKHL 47 at [17].
[1157] *Mosley*, above n 886, at [12].

"parallel analysis".[1158] Prior to *Re S*, Sedley LJ described the proportionality test as the "metwand" that the ECtHR had adopted for "deciding a variety of Convention issues including … what is and is not necessary in a democratic society."[1159] The proportionality test generally considers if an interference corresponds "to a 'pressing social need', that the reasons given by the national authorities to justify it are relevant and sufficient and that it was proportionate to the legitimate aim pursued."[1160]

In cases where privacy comes into conflict with freedom of expression, the focus has been on the "proportionate" aspect of the above criteria, which has come to be seen as a "fair balance" test.[1161] In *Von Hannover v Germany* the fair balance test required consideration of whether the information published contributed to a debate of general interest. In that case, the Court noted that:[1162]

> … a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of "watchdog" in a democracy by contributing to "impart[ing] information and ideas on matters of public interest, it does not do so in the latter case."

In this case, the Princess did not exercise any official function on behalf of the state, so the publication of articles and photos about her everyday activities were firmly in the latter category.[1163] It did not matter that the Princess was a "figure of contemporary society '*par excellence*'", she still had a right not to have details of her private life photographed at any time and widely distributed.[1164]

[1158] Gavin Phillipson "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act" (2003) 66 MLR 726 at 752.
[1159] *London Regional Transport v The Mayor of London* [2001] EWCA Civ 1491, [2001] All ER (D) 80 (Aug) at [57]. ECHR, art 10(2) states that the right to freedom of expression "may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society". Similarly, ECHR, art 8(2) states that: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society".
[1160] *Case of National Federation of Sportspersons' Associations and Unions (FNASS) and Others v France* ECHR 48151/11 and 77769/13 18 April 2018, at [167].
[1161] See *Von Hannover*, above n 897, at [57] and *Axel Springer AG v Germany* (2012) 55 EHHR 6, at [84]. See also Kristina Trykhlib "The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights" (2020) EU and Comparative Law Issues and Challenges Series 128 at 138.
[1162] *Von Hannover*, above n 897, at [63].
[1163] At [65] and [76].
[1164] At [74]. The concept of a "figure of contemporary society '*par excellence*'" was used by the German Federal Court of Justice to balance freedom of the press and the right to respect of private life. See Rainer Grote "The ECHR's Rulings in *Von Hannover v Germany (No 2)* and *Axel Springer AG v Germany*: Rebalancing Freedom of the Press with the Respect for Privacy" 55 German Y B Int'l L 639 at 640.

In the second case involving Princess Caroline – *Von Hannover v Germany (No 2)* – the test was broadened to include a range of factors to determine where the fair balance resided. The Court held that the following matters must be considered: (1) whether the publication constitutes a contribution to a debate of general interest; (2) how well known is the person concerned and what is the subject of the report; (3) the prior conduct of the person concerned; (4) the content, form and consequences of the publication; and (5) the circumstances in which the photos were taken.[1165]

The *Von Hannover (No 2)* balancing test was also reiterated in *Axel Springer AG v Germany*, which involved the publication of articles relating to the arrest of an actor for possession of illegal drugs at the Munich beer festival. In determing where the fair balance rested, the Court noted that matters of criminal justice were in the public interest. The Court held:[1166]

> The public do, in principle, have an interest in being informed – and in being able to inform themselves – about criminal proceedings, whilst strictly observing the presumption of innocence … That interest will vary in degree, however, as it may evolve during the course of the proceedings – from the time of the arrest – according to a number of different factors, such as the degree to which the person concerned is known, the circumstances of the case and any further developments arising during the proceedings.

In the case, the fact that the actor was in a popular television show and that the arrest occurred at a public event contributed to the public interest in the matter.[1167] Furthermore, the fact that the actor had previously engaged with media about his personal life meant he had reduced expectations of protection for his private life.[1168] All these factors ultimately meant that the right to publish outweighed any rights to privacy the applicant had.

The fair balance critieria of *Von Hannover (No 2)* and *Axel Springer* was also employed by the ECtHR in *ML and WW*. In that case, the Court had to consider whether the publication of a past criminal conviction warranted protection under art 8 of the ECHR. The applicants had been sentenced to life imprisonment for murder in 1993 and were released over 20 years later. The case involved publications, including publications in media archives, that remained publicly accessible after the applicants were released from prison. In applying the fair balance criteria, the seriousness of the crime, its high profile, the actions of the applicants in creating

---

[1165] *Von Hannover v Germany (No 2)*, above n 417, at [108]–[113]. The Court found against Princess Caroline in this case.
[1166] *Axel Springer AG v Germany*, above n 1161, at [96].
[1167] At [99].
[1168] At [101].

their media profile, and the content of the media reports were the factors that most influenced the Court. The seriousness of the crime and its infamy meant that the public interest in the case had not diminished by the passage of years since publication.[1169] As recently as three years before their release, the applicants had engaged with the media in order to try have their cases re-opened. Furthermore, the Court noted that the use of the media by the applicants for their own purposes led to them having a reduced expecation of privacy in the publications.[1170] In regards to the content of the media reports, the Court noted that they were objective, accurate and limited in nature.[1171] The Court also accepted a chilling effect argument – that if the right to privacy was accepted, the media would have to review the lawfulness of informtion in its archives and balance competing interests, and as a result "the press might refrain from keeping reports in its online archives or that it would omit individualised elements in reports likely to be the subject of such a request."[1172]

While the decision in this case found against the applicants, it is not unsurprising. The criminal convictions were for a serious offence and related to a high profile case (the murder of a popular actor), the convictions had not become spent and the plaintiffs had courted the media for their own purposes.[1173] The fact that the applicants had made no attempt to contact the search engines meant the Court did not look favourably on the applicants argument about the amplifying effect of the Internet.[1174] On this point, Tomlinson and Wills argue that the applicants may have had more success against a search engine:[1175]

> The court may have taken a different view if, instead of seeking anonymisation of media archives, the applicants had sought search engine "delisting". Given the art 10 rights at play when challenging a primary publisher, a convicted person's right to be forgotten—whether under data protection law or art 8—is much more powerful when against search engine operators or internet platforms.

Following *ML and WW*, the ECtHR considered the issue of prior convictions again in *Hurbain*.[1176] The facts of the case were discussed in Chapter 4, but ultimately considered whether the continued publication of information regarding an offender's spent conviction

[1169] *ML and WW*, above n 917, at [105].
[1170] At [109].
[1171] At [112].
[1172] At [104].
[1173] Hugh Tomlinson and Aidan Wills "ML and WW v Germany—Article 8 Right to be Forgotten and the Media" (2018) Ent LR 235 at 235.
[1174] ML and WW, above n 917, at [114].
[1175] Tomlinson and Wills, above n 1173, at 232.
[1176] *Hurbain,* above n 468.

was a breach of art 8. The Court applied the same balancing exercise to determine if the interference was necessary but noted that the relevance of some of the *Axel Springer* criteria may change with the passage of time.[1177] In particular, how well known a person is may decline with the passage of time. Accordingly, while a person cannot use art 8 to "complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence",[1178] the Court held that:[1179]

> …this does not mean that a person who has in the past been the subject of a criminal conviction can never exercise the right to be forgotten, otherwise that right would be void of its substance. The Court considers that after a certain time has elapsed, a convicted person may have an interest in no longer being confronted with his act, with a view to his reintegration into society.

The Court also noted the different contributions of archived information and initial publications to debates of general interest, with the former contributing to "historical research, teaching, and contextualising current events".[1180] However, in this instance the naming of a person who was not a public figure in connection with an old conviction did not contribute to a debate of general interest.

Phillipson argues that *Von Hannover (No 2)* and *Axel Springer* demonstrate a trend "tilting the balance quite strongly in favour of press freedom" in English and European law.[1181] While still not as weighted toward free speech as the United States, he argues that in England and Europe "privacy is starting to lose its fight with the press".[1182] Phillipson points to a range of factors influencing this trend, including growing acceptance of the argument that the economic survival of newspapers requires them to print stories that will sell irrespective of the public interest in the story. Phillipson also argues that courts are increasingly accepting arguments that public figures have reduced expectations of privacy and a widening of *who* is a public figure, as well as accepting that persons who court publicity cannot complain about ongoing intrusive publicity.[1183] Furthermore, he also points to increased acceptance of the

---

[1177] At [94] and [104].
[1178] *Axel Springer AG v Germany*, above n 1161, at [83].
[1179] *Hurbain*, above n 468, at [109].
[1180] At [105].
[1181] Gavin Phillipson "Press Freedom, the Public Interest and Privacy" in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 136 at 137. See also Elspeth Reid "Rebalancing Privacy and Freedom of Expression" (16) Edin L R 253 at 256 who, like Phillipson, sees a "perceptible shift towards freedom of expression" in *Von Hannover v Germany (No 2)* and *Axel Springer AG v Germany*.
[1182] Phillipson, above n 1181, at 137.
[1183] At 150.

'role model' argument, whereby it is in the public interest to report a role model's bad behaviour, and acceptance of the belief that people need to be free to criticise "the conduct of other members of society as being socially harmful, or wrong" as a way to develop public opinion and standards.[1184]

Whether Phillipson's argument is correct will only be determined as further cases are decided in England and Europe. Certainly, in *PJS v News Group Newspapers Ltd*, Lord Mance of the Supreme Court noted that "freedom to criticise" cannot be a "pretext for invasion of privacy by disclosure of alleged sexual infidelity which is of no real public interest in a legal sense."[1185] In that case, it did not matter that the plaintiff and his partner were both well known public figures. *PJS* is also useful because it finds that there is an arguable case for invasion of privacy despite the fact that the information was already publicly available on the internet. What was relevant was the considerably more intrusive publicity that would arise from extensive unrestricted mainstream publication.[1186] In *Weller v Associated Newspapers*, the application of the *Von Hannover (No 2)* criteria resulted in a finding of breach of privacy for the publication of photos of the children of a public figure pursuing everyday activities on the streets of Los Angeles.[1187]

The English courts have also held that the ECHR balancing exercise applies to the data protection environment, and in particular, when the decision in *Google Spain* is applied. In *NT 1 & NT 2*, Justice Warby noted that the *Re S* balancing exercise is essentially the same as the balancing exercise required by the decision in *Google Spain*.[1188] In *Google Spain*, the ECJ held that the interests to be weighed against the fundamental rights of the data subject were the legitimate economic interests of Google *and* the interests in freedom of information.[1189] The *Google Spain* balancing exercise was set out in the decision itself and elaborated in the Article 29 Data Protection Working Group Guidelines. In the decision, the Court noted that the balance may depend upon:[1190]

> … the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

[1184] At 158.
[1185] *PJS*, above n 906, at [21].
[1186] At [35].
[1187] *Weller,* above n 443.
[1188] *NT 1 & NT 2*, above n 361, at [115] and [132].
[1189] *Google Spain*, above n 5, at [81]. See also *NT 1 & NT 2*, above n 361, at [134].
[1190] *Google Spain*, above n 5, at [81].

The Article 29 Data Protection Working Group Guidelines set out a broader suite of criteria for the balancing, which includes: whether or not the person concerned is a public figure; their age; whether or not the data are accurate, relevant or excessive; whether or not the data's sensitive or up to date; whether or not the processing causes prejudice to the data subject or puts them at risk; the context of the data's publication (including consent); and whether or not the data relates to a criminal offence.[1191]

It is worthwhile considering some of these criteria in detail, especially as they relate to once public facts. The Article 29 Data Protection Working Group Guidelines note that determining whether or not a person is a public figure or involved in public life can be contentious. However, politicians, senior public officials, business-people and members of regulated professions are generally considered to have a role in public life. A "good rule of thumb", the Guidelines state is to determine whether "the public having access to the particular information … would protect them against improper public or professional conduct."[1192] Furthermore, public figures are generally people who "have a degree of media exposure".[1193] The Guidelines state that there is an argument that the public should be able to find "information relevant to their public roles and activities",[1194] but that there is some information about public figures which remains private and should not generally appear in search results, including information relating to their health or family members.[1195] Justice Warby in *NT 1 & NT 2* noted that the passage of time was also relevant in assessing the extent to which the plaintiffs were public figures. In particular, his Honour noted that the length of time since the convictions weakened the argument that the public needed to know the information to guard against impropriety.[1196]

In determining whether or not data are relevant or excessive, the age of the information is a factor, so that "information that was published a long time ago, e.g. 15 years ago, might be less relevant than information that was published one year ago."[1197] In *Google Spain*, the fact that the information at issue was 16 years old was a key factor in determining that it was no longer relevant. Passage of time is also a factor when determining whether or not the data processing is causing prejudice. The Guidelines note that:[1198]

[1191] Article 29 Data Protection Working Party Guidelines, above n 394.
[1192] At 13.
[1193] At 13.
[1194] At 13
[1195] At 14.
[1196] *NT 1 & NT 2*, above n 361, at [138].
[1197] Article 29 Data Protection Working Party Guidelines, above n 394, at 15–16.
[1198] At 18.

> The data might have a disproportionately negative impact on the data subject where a search result relates to a trivial or foolish misdemeanour which is no longer – or may never have been – the subject of public debate and where there is no wider public interest in the availability of the information.

The last criterion in the Article 29 Data Protection Working Group Guidelines addresses situations where the information at issue is a criminal offence. The Guidelines note that different member states will follow their own rules and approaches, and that:[1199]

> DPAs [data protection authorities] are more likely to consider the de-listing of search results relating to relatively minor offences that happened a long time ago, whilst being less likely to consider the de-listing of results relating to more serious ones that happened more recently.

The last criterion of the Article 29 Data Protection Working Group Guidelines weighed heavy in *NT 1 & NT 2*, where Justice Warby called it the "single most important criterion in the present case."[1200] The Judge noted that the plaintiff's convictions were spent under the United Kingdom's Rehabilitation of Offenders Act. However, the existence of a spent conviction was not determinative and it did not make privacy a "preponderant weight"; rather, the spent conviction was a "weighty factor" in the balance.[1201] For NT 1 the balance ultimately found that free speech outweighed privacy, despite the spent conviction. The Judge reduced the weight given to the spent conviction because, when convicted, NT 1 would not have qualified for a spent conviction and he only did so at the time he brought his case against Google because of a recent law change. The Judge also noted that if NT 1's sentence had been any longer it could not be spent at all. The Judge concluded that these factors meant that NT 1's conviction was only spent "at the margins."[1202] However, this argument is not convincing. Convictions are either spent or not. If they are spent, then the focus should be on how the other factors are weighted against that factor, rather than arguments that convictions are only *just* spent. Certainly, the other factors the Judge pointed to in the overall assessment could ultimately have assisted to weigh the balance in favour of the ongoing public interest in the expression, without the semantic gymnastics regarding the spent convictions. The other relevant factors in the decision regarding NT 1 included that the conviction related to dishonesty, that the plaintiff's career since leaving prison made the prior information relevant

[1199] At 20.
[1200] *NT 1 & NT 2*, above n 361, at [161].
[1201] At [166(2)].
[1202] At [170].

to current assessments of his honesty, and that he could not demonstrate a strong interference with his private life.

In contrast, NT 2's spent conviction in *NT 1 & NT 2* was given more weight in the overall balancing exercise. NT 2's previous conviction was always going to become spent, it did not relate to dishonest activities and it had no relevance to his current business practices. These circumstances, along with the presence of young children which strengthened his argument for interference with his family life, meant that NT 2's right to privacy was held to outweigh interests in free speech.[1203]

Returning to the objectives of this chapter, it will be remembered that the intent was to determine how the legal mechanisms for protecting privacy have managed the conflict between privacy and free speech and whether that management provides any presumptive protection for free speech, when the information at issue is once public facts. Where the disclosure tort is considered, the present research demonstrates that the New Zealand approach to the tort establishes no presumption in favour of free speech or against once public facts. What is required is a close analysis of the particular circumstances and a weighing of the respective interests to determine if the level of legitimate public concern in a disclosure is proportionate to the gravity of the invasion of privacy. Generalisations and broad categories are not determinative. The present research has also demonstrated that the balance between privacy and free speech operates differently under the Privacy Act, and that the Act is in fact the outcome of a prior, external balancing between the two interests, although in certain circumstances further balancing is required when decisions regarding the privacy principles are made. However, this discussion on the Privacy Act has determined that the operation of a strengthened erasure tool needs to ensure that free speech considerations are factored into assessments of whether erasure is required. This matter will be dealt with by the package of amendments set out in Chapter 9.

The New Zealand approach puts it closer to the approach in English and European law than the law of the United States, where a broad category-focused, pro-speech approach is favoured. The most obvious example of this conclusion is New Zealand's clear endorsement of the proportionality principle and a focus on the particular circumstances of the case. However, what has been identified from the research in this chapter is that the operation of the legitimate public concern defence under the disclosure tort in New Zealand could be improved by the establishment of a structured framework for using the defence. Such a

[1203] At [222].

framework will assist all cases, but be of particular assistance in difficult cases, like once public facts, where there is a risk that the s 5 NZBORA justificatory framework might import an unconscious bias in favour of free speech. Furthermore, the discussion of the international perspective highlights that the framework should take inspiration from English law rather than United States law. A proposed framework is described next.

VII The Proportionality Framework

This thesis argues that in order to determine whether or not the defence of legitimate public concern in the disclosure tort has been established, a structured and principled framework is needed to guide decision making. This framework should reflect the central role of proportionality in the New Zealand jurisprudence. The framework should not be a rigid checklist, but rather a list of factors to be considered to ensure that a principled weighing of the competing interests occurs. The framework is described below, with a diagrammatic representation provided in Chapter 9.

The first aspects of the proportionality framework proposed here is a determination of the particular public concern in the expressive matter and the weight to be given to that concern. It refers to the first type of proportionality discussed in s III(A) above. This thesis argues that the broad approach used by Tipping and Thomas JJ in *Hosking* and *Brooker,* respectively, provides an appropriate starting point. Their approach identifies the public interest pursued by the expressive activity and recognises that there is significant public interest in information which implicates certain types of speech. Speech that directly supports democracy will have a high value. Speech that supports the marketplace of ideas and the safety valve theories will also have a high value. However, it is also arguable that it is unlikely that restricting the disclosure of *private* information (or information in which there is a reasonable expectation of privacy) restricts in any meaningful way the broader market for ideas or speech as society's safety valve.[1204] However, this will depend on the value of the particular speech at issue.

There can be free speech value in once public facts, especially where the facts relate to criminal convictions and the public have a right to be informed about the proceedings of the criminal justice system.[1205] Where the once public facts relate to people who are public figures, then there may be increased free speech value in the information, as the information may contribute to a debate of general interest. Furthermore, the truth justification for free

[1204] See *Hosking*, above n 8, at [233].
[1205] See above n 392 for a discussion of open justice.

speech means that there is potentially value in all factual information, even old information.[1206] However, where the value of speech solely rests on this truth justification (or a person's liberty of action as an expression of self) then the weight given to such speech should be open to increased challenge, especially where there is no other concrete public benefit to the speech, for example, preventing harm to society.

The factors that will be relevant in making the assessment of the value of the speech include whether the matter contributes to a debate of general interest, how well known the person is, their prior conduct, the content, form and consequences of publication and whether the publication went further than necessary to meet its purposes. The age of the information will also be relevant. A person who used to be a public figure might no longer be considered one after a number of years, the passage of time may have made information out of date or irrelevant, or historical information might no longer contribute to a debate of current interest. Furthermore, even if it is determined that information is necessary for historical record, it may not be necessary to publish a person's identifying information.

The next requirement of the framework is determining the weight to be given to the privacy interest at issue. This aspect should, theoretically, be performed by the reasonable expectation of privacy test. In *Campbell*, Baroness Hale noted that, similar to freedom of expression, where there are different classes of speech, there are also "different types of private information, some of which are more deserving of protection in a democratic society than others."[1207] Warby, Speker and Hirst refer to a "hierarchy of privacy interests" and note that the more intimate or "the closer it lies to the 'core' values protected by Article 8, the greater the weight which the court will accord to the information when conducting the balancing exercise."[1208] In New Zealand, the core values assessment would similarly ensure that appropriate weight to matters which engage the core values of privacy.

The final aspect of the framework is the actual weighing to be made between the respective interests identified in the assessments described above. In the case of *Richard v British Broadcasting Corporation*, the English Court of Appeal noted that this exercise was "an overall evaluative exercise which is not a precise scientific measuring one".[1209] The weighing exercise is the second type of proportionality assessment discussed in s III(B) above, which

[1206] See above n 1004 for a discussion of the truth justification for free speech.
[1207] *Campbell*, above n 355, at [148].
[1208] Warby, Speker and Hirst, above n 883, at [5.130].
[1209] *Richard*, above n 902, at [315].

recognises that a low value speech interest cannot outweigh a high value privacy interest, and vice versa.

VIII Conclusion

This chapter has investigated the fundamental conflict between privacy and free speech that commonly arises when the law attempts to protect privacy interests. In the disclosure tort, the conflict is addressed via the defence of legitimate public concern, which seeks to ensure that privacy is a reasonable limit on freedom of expression that is demonstrably justified in a free and democratic society. In considering the disclosure tort, the research has sought to understand whether the right to freedom of expression imposes any presumption against protection for once public facts. What has been found, however, is that the New Zealand courts have rejected a focus on generalisations and categories of information, preferring instead a close analysis of the particular circumstances and a weighing of the respective interests on the basis of proportionality. This nuanced approach is good news for once public facts.

However, it has also been identified that improvements could be made to the legitimate public concern defence. It is argued that the defence would benefit from a structured and principled approach being employed when determining if a matter is of legitimate public concern. Such an approach will assist all cases, but be of particular assistance in difficult cases, like once public facts, where there is a risk that s 5 of the NZBORA might import an unconscious bias in favour of expression. Furthermore, the discussion of the international perspective highlights that the framework should take inspiration from English law rather than United States law.

The chapter has proposed the use of a principled proportionality framework to improve the operation of the defence. This framework requires consideration of four factors when determining if the defence has been established: (1) the particular public concern in the expressive matter and how that concern aligns with the predominant rationales for free speech; (2) the weight to be given to that concern, which recognises that different types of speech have different values, as well as identifying other factors that influence the public concern like whether the person is a public figure, their prior conduct, the age and relevance of the information and the consequences of publication; (3) the weight to be given to the privacy interest, which is an output of the reasonable expectation of privacy test; and (4) a

weighing of the respective interests to determine which has the most weight and which should be given priority in the particular circumstances of the case.

In considering the conflict between privacy and free speech, the research in this chapter also considered how the Privacy Act 2020 addresses the conflict. What has been identified is that the balance between privacy and free speech operates differently under the Act and that the Act is predominantly the outcome of a prior, external balancing between the two interests. However, it is also noted that an internal balancing of privacy and free speech is required when certain decisions are made under the Act, but that no such balancing is required under existing erasure mechanisms in the Act. Therefore, if the erasure mechanisms are strengthened as recommended in Chapter 5, then agencies must be directed to balance privacy and free speech when making erasure decisions, to ensure that s 5 of the NZBORA is upheld. Accordingly, it is recommended that the new erasure IPP includes such a direction. The specific wording of the direction is set out in the package of amendments for the Privacy Act proposed in Chapter 9.

8 HARMFUL DIGITAL COMMUNICATIONS ACT 2015

I Introduction

The HDCA was enacted in response to widespread concern about the potential harms caused by text messages, social media posts, videos and a range of other digital communication formats. These harms, like truancy, educational failure, depression, self-harm, and suicide,[1210] are increasingly prevalent in society. Independent research conducted on behalf of the NZLC found that one in 10 New Zealanders has some personal experience of harmful communications on the internet and that this rate increased to 22 per cent for those aged 18-29, who are also the heaviest users of social media.[1211] In addition, in February 2021, Netsafe released survey results which determined that 11 per cent of adults admitted to sending or sharing at least one type of potentially harmful digital communication, with nearly 80 per cent of that group saying they had done it more than once.[1212]

The HDCA establishes a range of communication principles (CPs) that apply to digital communications. One of the principles is that digital communications should not disclose sensitive personal information. This principle, along with the raft of remedies available in the Act, has led some commentators to argue that the Act provides New Zealand with a form of RTBF.[1213] This chapter investigates those claims. To achieve this, the chapter provides an overview of the HDCA, before investigating the parts of the Act that affect its use as a mechanism to protect once public facts. The chapter then considers the extent to which the Act provides a RTBF akin to either the delisting mechanism from the decision in *Google Spain* or a right to erasure from data protection statutes. What the chapter determines is that the specific drafting of the privacy CP, along with its clear links with the Privacy Act 2020 and the disclosure tort, mean that it could be used as a limited form of RTBF. However, it cannot be used to delist search results and its jurisdictional constraints may hamper its use against other proponents of ubiquitous technology, like Facebook, Twitter and YouTube.

Ultimately, this chapter recommends that the operation of the HDCA should be closely monitored to determine its level of use and effectiveness as an erasure tool, and that two amendments are made to the provisions of the Act to increase its immediate efficacy.

[1210] Law Commission, above n 653, at [1.6].
[1211] At [2.92].
[1212] Netsafe "Revealed: Who sends harmful digital communications – and why" (press release, 9 February 2021).
[1213] See Russell McVeagh "InfoRM Privacy Update" (15 March 2018) Russell McVeagh <www.russellmcveagh.com>.

II The Requirements of the Harmful Digital Communications Act 2015

The HDCA establishes civil and criminal protections against digital communications that cause harm.[1214] The civil process commences with a complaint to an approved agency established under the Act (currently Netsafe).[1215] Netsafe assesses and investigates the complaint and can use "advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints".[1216] In performing its role, Netsafe must take account of the 10 CPs set out in the Act. These include CP 1, which states that: "A digital communication should not disclose sensitive personal facts about an individual."[1217]

Once a complaint has been made and Netsafe has had the opportunity to assess it and decide what action to take, a complainant may make an application to the district court. The district court has the power to issue a range of remedial orders, including ordering a defendant to take down or disable material, stop conduct, publish a correction, or publish an apology.[1218] The district court can also make orders against online content hosts, which are defined as:[1219]

> … the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user.

The orders against online content hosts can require the hosts to take down or disable public access to material, identify the author of anonymous posts, publish a correction, or give a person a right of reply.[1220]

The district court can only grant an order under the Act if it is satisfied that there has been a serious breach, threatened serious breach or repeated breach of one or more CPs and the breach has caused or is likely to cause harm to a person.[1221] When deciding whether or not to grant an order, the court must consider the following factors:[1222]

[1214] See HDCA, s 4 for a definition of 'digital communications'.
[1215] Harmful Digital Communications (Appointment of Approved Agency) Order 2016, cl 3.
[1216] HDCA, s 8(1)(c).
[1217] Section 6(2).
[1218] Section 19(1).
[1219] Section 4.
[1220] Section 19(2). Under s 19(3), the district court can also order an IAPA to identify an anonymous poster and made a declaration that a post breaches the communication principles. An IAPA is an internet protocol address provider, and is defined in the Copyright Act 1994, s 122A(1).
[1221] Section 12(2).
[1222] Section 19(5).

(a) the content of the communication and the level of harm caused or likely to be caused by it:
(b) the purpose of the communicator, in particular whether the communication was intended to cause harm:
(c) the occasion, context, and subject matter of the communication:
(d) the extent to which the communication has spread beyond the original parties to the communication:
(e) the age and vulnerability of the affected individual:
(f) the truth or falsity of the statement:
(g) whether the communication is in the public interest:
(h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused:
(i) the conduct of the affected individual or complainant:
(j) the technical and operational practicalities, and the costs, of an order:
(k) the appropriate individual or other person who should be subject to the order.

The Act establishes two offences – non-compliance with a district court order,[1223] and causing harm by posting digital communications. The latter offence requires: (1) posting of a digital communication with the intention that it causes harm to a victim; (2) that the posting would cause harm to an ordinary reasonable person in the position of the victim; and (3) that the posting actually causes harm to the victim.[1224]

Harm, therefore, is an integral element of both the civil and criminal protections. Harm is defined in the Act as "serious emotional distress".[1225] When determining whether a post would cause harm in regard to the offence, the court can take into account any relevant factors, including:[1226]

(a) the extremity of the language used:
(b) the age and characteristics of the victim:
(c) whether the digital communication was anonymous:
(d) whether the digital communication was repeated:
(e) the extent of circulation of the digital communication:
(f) whether the digital communication is true or false:
(g) the context in which the digital communication appeared.

[1223] Section 21(1).
[1224] Section 22(1).
[1225] Section 4.
[1226] Section 22(2).

In *Police v B*, the High Court held that harm under the Act was more than minor harm, but less than "mental injury" or an "identifiable psychological or psychiatric condition."[1227] In that case, the High Court had to consider whether the publication of suggestive photos of the complainant in various states of undress, accompanied by links to pornographic websites, caused the requisite harm. The Judge in the District Court had found that serious harm was not established. However, Downs J in the High Court disagreed. Downs J stated that whether the harm standard had been achieved was part fact, part value judgement, where: [1228]

> … consideration should be given to obvious factors such as the nature of the emotional distress; its intensity; duration; manifestation; and context, including whether a reasonable person in the complainant's position would have suffered serious emotional distress.

Considering the totality of the evidence, Downs J found the evidence established "various forms of emotional distress including frustration, anger, anxiety and humiliation", that the emotions were "reasonably intense",[1229] that they continued for a long time, and had an apparent physical manifestation in the complainant's incapacity to work for a period of time.

III Does the Harmful Digital Communications Act 2015 Apply to Once Public Facts?

The HDCA will only provide a remedy for once public facts if they fall within the ambit of CP 1. The cornerstone of CP 1 is 'sensitive personal facts'. However, the phrase is not defined in the Act. The NZLC has stated that CP 1 derives from "the tort of invasion of privacy; from information privacy principle 11 in the Privacy Act; and from the intimate filming provisions of the Crimes Act."[1230] It is useful to consider the first two of those sources to see if they can shed light on how to interpret the phrase.[1231]

Starting with the Privacy Act 2020, it must be noted that the Privacy Act does not establish a sub-set of personal information that is labelled 'sensitive'. The Privacy Act and IPP 11 apply to all information about an identifiable individual, whether sensitive or not.[1232] Accordingly, if CP 1 is interpreted as *identical* to IP 11, then the sensitive qualification is redundant. However, Parliament has chosen to qualify personal information with the label 'sensitive', so

[1227] *Police v B* [2017] NZHC 526, [2017] 3 NZLR 203 at [22].
[1228] At [24].
[1229] At [38].
[1230] Law Commission, above n 653, at [5.66]. See the Crimes Act 1961, s 216J.
[1231] Intimate filming would involve "sensitive" personal information.
[1232] Privacy Act 2020, s 7(1).

it is arguable that an interpretation that ignores that qualification is wrong.[1233] So how is 'sensitive personal information' to be interpreted? In determining if there has been serious harm caused by a privacy breach, the Privacy Act requires agencies to consider "whether the personal information is sensitive in nature".[1234] The Act provides no further guidance on when personal information is sensitive; however, the Office of the Privacy Commissioner (OPC) has noted that:[1235]

> Sensitive information is typically personal information about someone's health, unique identifiers (e.g. passport or driver's licence number), genetic or ethnic background, political or religious beliefs, sex life or sexual orientation. Financial information, union affiliation or criminal history may also be considered sensitive.

The GDPR uses the phrase "special categories of personal data" to establish more stringent requirements for sensitive information.[1236] This information includes information about racial identity, political opinion, religious beliefs, trade union membership, health data, and sex life and sexual orientation.[1237] In Australia, the Privacy Act 1998 defines 'sensitive' personal information similarly to the GDPR's special categories, but also includes information on a criminal record.[1238] Leveraging these interpretations, sensitive personal information for the purposes of CP 1 would be inherently private and intimate information, together with potentially broader information like that relating to criminal convictions.

One way that IPP 11 itself might be useful for interpreting CP 1 is in addressing the issue of whether the previously public nature of the information would *disqualify* it from being considered sensitive. IPP 11 establishes a range of exemptions to the general non-disclosure rule it establishes.[1239] The exemption which provides the most difficulties for once public facts is IPP 11(1)(d), which excludes information that is publicly available. However, as discussed in Chapter 5, the HDCA itself amended that exemption so it does not apply when it would be *unfair* or *unreasonable* to disclose the publicly available information. If CP 1 is to be considered consistently with IPP 11, then it is arguable that just because the information is publicly accessible, does not exclude it from CP 1, if its redisclosure or continued disclosure is unfair or unreasonable. While unfairness or unreasonability will depend on individual

[1233] See Interpretation Act 1999, s 5(1) which states that: "The meaning of an enactment must be ascertained from its text and in the light of its purpose."
[1234] Privacy Act 2020, s 113(b).
[1235] Office of the Privacy Commissioner "Privacy breach self-assessment" <www.privacy.org.nz>.
[1236] GDPR, art 9.
[1237] Article 9.
[1238] Privacy Act 1998 (Cth), s 6.
[1239] Privacy Act 2020, s 22 principle 11(1)(a)–(i).

circumstances, the NZLC has previously stated that in some instances an historical conviction "may now be so far in the past that it would be *unreasonable* to revive it."[1240] The NZLC has also recognised that in some instances that information "is of such sensitivity that the subject of it can *reasonably* expect that even if it has been widely published previously it will nevertheless not be published again."[1241] These statements provide support for the conclusion that just because information has been publicly available does not necessarily disqualify it from protection under CP 1.

The disclosure tort was also an inspiration for CP 1. As noted earlier, the disclosure tort is pegged to matters where there is a reasonable expectation of privacy and publication is highly offensive to a reasonable person. Like the Privacy Act, the tort does not address sensitive information. While some inherently private information – like the sensitive standards described above – has been held to clearly meet the reasonable expectation standard, it is also well accepted that the scope of the standard is wider. If CP 1 is to be interpreted in light of the disclosure tort, then what is sensitive personal information can be seen as another way to describe information for which there is a reasonable expectation of privacy and where its disclosure is highly offensive to a reasonable person. The disclosure tort test has been found to be broad enough to potentially allow protection for the publication of once public facts.[1242] Accordingly, if CP 1 is interpreted consistent with the tort, then there is room for protection of once public facts in appropriate circumstances.

Consideration of whether or not CP 1 can protect once public facts is not, however, limited to theory. There has been one such case decided under the HDCA. The case – *Wensor v Stuff* – was an application for an order that Stuff remove or disable access to an article posted on its website. The article had been posted in 2008 but was still available nine years later. The article reported the complainant's conviction in Australia for sexual assault and his sentencing to a suspended term of 12 months imprisonment. The complainant complained to Netsafe. Netsafe determined there was a breach of CP 1 and that there was a likelihood of harm by emotional distress as a result of the publication.[1243] However, Netsafe was unable to resolve the complaint. The complainant took the case to the district court. The Court found that Netsafe had determined that there was only a "simple" breach of one CP.[1244] As a result, the Court found that the s 12(2)(a) threshold had not been met. However, in discussing the

[1240] Law Commission, above n 655, at [6.40] (emphasis added).
[1241] At [6.40].
[1242] See discussion in Chapter 6 above.
[1243] *Wensor v Stuff* [2017] NZDC 979 at [4].
[1244] At [6].

breach, Judge Spear held that the article at issue "unquestionably" disclosed sensitive personal facts.[1245]

The above analysis provides a reasonable basis for the argument that once public facts may be able to obtain protection via CP 1 in appropriate circumstances. However, there are several other requirements in the HDCA which must be satisfied for an application to result in a remedy. The first is s 12(2)(a), which was the downfall for the plaintiff in *Wensor*. Section 12(2)(a) requires a serious or repeated breach. Repeated breaches are relatively easy to identify and will point towards a systemic issue regarding the posting of harmful content. The serious standard, however, is harder to determine. In *Wensor*, Judge Spear provided no analysis regarding why the breach was not serious, simply stating that: "I am not satisfied that the threshold step required [by] s 12(2) has been reached."[1246]

The NZLC's recommendation on this part of the HDCA noted that:[1247]

> Only particularly serious cases should come to the tribunal. Complainants should have to demonstrate two things:
> (a) that they have attempted to resolve the matter through other avenues; and
> (b) that the communication complained about has caused, or is likely to cause, significant harm, including significant emotional distress.

While the Commission was clear that only serious cases should go to court, it links seriousness to two aspects – the complainant has utilised a self-help remedy and the communication has caused significant harm. The Act, however, has split seriousness into three aspects – pursuing a self-help remedy (s12(1)), seriousness (s12(2)(a)), and harm (s12(2)(b)). However, because harm is defined in the Act as "serious emotional distress", it must be asked if a digital communication that causes serious emotional harm should ever not be considered serious enough to meet the s12(2) threshold. Put another way, in the context of what the HDCA is trying to achieve, what level of seriousness is there over and above "serious emotional distress"?

The factors which the courts are required to consider under s 19(5) when deciding whether or not to make an order under the Act also potentially make the s 12(2)(a) threshold redundant.

[1245] At [11]. While it could be argued that the 'sensitive' part of the article was the nature of the offending, the whole thrust of the article was about the conviction and the plaintiff's sentence. To say only one aspect of the article was 'sensitive' would be to carve up the article in an unhelpful way, something the Judge did not do.
[1246] At [7].
[1247] Law Commission, above n 653, at 135.

These factors cover a broad range of matters, like the content, context and purpose of the communication, level of harm, the extent to which the communication has spread, the age or vulnerability of the affected person, the conduct of both parties, whether the communication is true or false, the public interest in the communication, and the practicalities and cost associated with an order. Again, it is difficult to see how the serious threshold requires consideration of any matter which could not be dealt with under these factors. It is, therefore, arguable that the s 12(2)(a) should be removed because it is redundant.

A remedy under the HDCA will also only result if there is serious emotional distress, and this requirement might provide a stumbling block for once public facts. Karlsen has queried whether the harm suffered by the plaintiff in *Google Spain* or Lindsey Stone,[1248] would meet the threshold.[1249] However, Karlsen's article was published before *Police v B*, where the threshold was clarified. Using the standard from *Police v B*, it is hard to see how Lindsey Stone did not suffer serious emotional distress. She lost her job, she became depressed, she suffered insomnia, and she became a virtual recluse for a year. However, these were the immediate effects. A once public facts case would need to prove serious emotional distress from the continued availability or republication of the information. The harms that can result from once public facts were discussed in Chapter 4. However, at the serious end of these harms, it is at least arguable that they would satisfy the harm definition of the HDCA.[1250]

The final two parts of the HDCA that need to be considered for a once public facts case are the clear statutory direction for decision bodies under the Act to consider the rights and freedoms protected by the NZBORA, and the factors the court must consider under s 19(5) when granting an order. The first reflects the fact that regulating communications can conflict with important and protected rights, like freedom of expression. Section s 6(2) of the Act requires Netsafe and the courts to "act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990".[1251] Section 19(6) requires the district court to act consistently with the NZBORA when making any order. Furthermore, s 19(5)(g) requires the district court to consider whether there is any public interest in the communication for which an order is requested. The s 19(5)(g) obligation is reminiscent of the language of the

[1248] See above n 530 for a discussion of Lindsey Stone.
[1249] Meredith Karlsen "Forget Me, Forget Me Not: A 'Right to Be Forgotten' in New Zealand's Information Society" (2016) NZ L Rev 507 at 533. Using *Google Spain* to support this argument is difficult because harm was not required for an action under Directive 95/46/EC, so harm was not pleaded in the case.
[1250] See Gollogly, above n 379, at 143. Gollogly argues that a case like *Tucker*, where there was a real threat to health and life from the disclosure of once public facts, is likely to meet the harm standard of the Act.
[1251] HDCA, s 6(2).

legitimate public concern defence to the disclosure tort. The NZLC clearly recognised the link between this section and the disclosure tort when it stated:[1252]

> Such a qualification is present in the common law in relation to invasion of privacy and breach of confidence, and also appears in the official information legislation as an override of the grounds on which information might otherwise be withheld. In our present context, even though a communication might hurt an individual, a countervailing public interest in the subject matter might sometimes be strong enough to outweigh the interests of the complainant. This might possibly be the case if the communication was part of a vigorous debate about a political matter, or a high profile crime, accident or natural disaster.

Acting consistently with the NZBORA requires consideration of the need to ensure any limit on the rights and freedoms in the NZBORA are reasonable and demonstrably justified in a free and democratic society.[1253] Where CP 1 conflicts with free speech, the fact that the same issue has been addressed in the disclosure tort means that it is logical for the balance worked out under the tort to influence similar considerations under the HDCA. The disclosure tort jurisprudence was extensively discussed in Chapter 7, and it is not intended to re-visit it here. What is important is that the defence of legitimate public concern requires a matter of genuine public *concern*, not just general interest and curiosity. The value to be attributed to free speech must be proportionate to the public concern, and the public concern needs to be proportionate to the gravity of the invasion of privacy.

The clash between privacy and freedom of expression was considered in *Wensor*, where Judge Spear noted that, absent any relevant suppression orders, accurate reporting of court proceedings by media "has long been held to be a justifiable form of expression that the Courts must respect."[1254] Furthermore, despite the complainant's argument that continued availability of the article for over 10 years was "unfair and … causing difficulties for him as he seeks to obtain good employment", the Judge concluded that:[1255]

> … the Harmful Digital Communications Act 2015 was surely never designed or intended to provide an effective, albeit de facto, means to restrict access to news media reports on Court proceedings no matter how long ago they occurred.

[1252] Law Commission, above n 653, at [5.81].
[1253] NZBORA, s 5.
[1254] *Wensor,* above n 1243, at [11].
[1255] At [12].

While Judge Spear was essentially concluding that free speech outweighed the privacy interest, it is arguable this statement went too far. To claim the Act was never designed or intended to achieve the stated outcome misses the point that the Act *was* designed to protect against privacy invasions that are also digital communication harms. A number of submitters on the Harmful Digital Communications Bill wanted CP 1 removed, arguing it duplicated the Privacy Act.[1256] The NZLC disagreed. While the NZLC was cognisant of the overlap and the potential for there to be a disconnect between the two Acts, the NZLC acknowledged that: "Privacy invasions are a small subset of internet harms" and preferred to allow complainants a choice of forum.[1257] Furthermore, a simple conclusion that news reports of past crimes essentially trump privacy concerns, as made by the Judge in *Wensor*, does not provide sufficient weighting to the proportionality assessment which is central to the privacy and free speech balancing in the disclosure tort.

The factors in s 19(5) which a court must consider when deciding to make an order encompass a range of matters which establish the context of the communication. However, there are factors which might pull either for or against once public facts.[1258] Factors which might pull against once public facts include the cost and practicalities of making an order. These factors might require consideration of whether the information has spread so far that it is worthless to try and remove the information[1259] or where the cost or effort associated with take down is disproportionate to the harm. Consideration of public interest in the information may also operate against once public facts, as discussed above. Factors which might pull in the other direction include the complainant's conduct, age or vulnerability. Gollogly argues that considering the complainant's conduct may allow a reformed criminal to provide evidence to support their rehabilitation.[1260] Furthermore, if the complainant is vulnerable – like in *Tucker* – or where the historical fact involved a minor who did not fully appreciate the long-term consequences of their actions, these factors might strengthen the arguments in favour of privacy.

The HDCA, therefore, can technically protect once public facts, provided that the relevant facts are sensitive and the publication of them causes serious emotional harm. However, there are factors which might count against protection, including the range of factors that a court must consider before issuing an order right, and freedom of expression. However, if the

[1256] See, for example, Google New Zealand "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013".
[1257] Law Commission, above n 653, at [5.96].
[1258] See above n 1222 for the wording of s 19(5).
[1259] Gollogly, above n 379, at 143. See also Harvey, above n 1, at 341.
[1260] Gollogly, above n 379, at 143.

district court were to employ a structured analysis for the balancing of freedom of expression and privacy, similar to the analysis of the legitimate public concern defence in the disclosure tort, then this would ensure that freedom of expression only overrode CP 1 in appropriate circumstances.

IV The Harmful Digital Communications Act 2015 as a Right to be Forgotten

As noted above, some commentators have argued that the HDCA is akin to a RTBF. Harvey has argued that the HDCA potentially provides a RTBF that is "of considerably greater potency" than seen in *Google Spain*.[1261] Harvey's argument presumably rests on the basis that the take down notice remedy applies to the publisher of the content and applies without it being pegged to the irrelevancy or excessiveness of the information (although the personal information does have to be sensitive and cause harm). Furthermore, the Act has been used to erase content. Netsafe has advised that since it began its role under the Act, it has received over 900 complaints in regard to CP 1. In response to these complaints, over 300 items of content have been taken down or deleted.[1262]

It appears, however, that whatever RTBF the HDCA does provide, it is not one akin to the decision in *Google Spain*. For the HDCA to provide an outcome akin to *Google Spain*, a search engine must be an entity against which the district court can grant an order. As noted above, the district court can grant orders against a content publisher and an online content host. A search engine is generally not the publisher, so it must be classified as an online content host to have an order issued against it. Some have argued that a search engine will fall into this definition.[1263] However, somewhat unsurprisingly, Google itself has argued that it is not an online content host, and the High Court agreed.

In *V v Google*, Clark J stated that: "Google does not come within the definition of 'online content host.'"[1264] The reason for this conclusion was supplied by Google itself. Google argued that:[1265]

[1261] Harvey, above n 1, at 340.
[1262] This data was provided by Netsafe on 30 September 2020 (obtained under Official Information Act request to Netsafe).
[1263] Stephanie Frances Panzic "Legislating for E- Manners: Deficiencies and Unintended Consequences of the Harmful Digital Communications Act" (2015) 21 Auckland U L Rev 225 at 237.
[1264] *V v Google* [2019] NZHC 488 at [31].
[1265] At [35] (emphasis added). See also David Harvey *Internet.law.nz: Selected Issues* (4th ed, LexisNexis, Wellington, 2015) at [4.221] who doubted the Google would qualify as an online content host.

> … a search engine is not the Web itself but merely a way of locating material on the Web. The companies who make the search engines available to users have no ability to control or limit what is on the Web. Those companies do not provide the content on the Web. Thus, the Google search engine does not *control* the websites and web pages accessible on the Web and nor does it have the ability to control the removal of content on those third-party websites.

Accordingly, the HDCA could not be used to achieve a delisting or delinking solution as occurred in *Google Spain*. However, other platforms, like Facebook, Twitter and YouTube, are likely to meet the definition of an online content host and therefore will be subject to the Act.

The use of the HDCA as an erasure tool that can be deployed against the likes of Facebook, Twitter and YouTube is hampered by two components of the Act. The first is the safe harbour mechanism which protects online content hosts from civil and criminal liability provided they make available an easily accessible complaints mechanism which complies with the Act.[1266] This mechanism requires the online content host to notify content authors of complaints received and sets out requirements based on whether the authors respond to the notifications and how they respond. For example, complained-of content may not have to be removed if the author does not consent to the removal; but, where the online content host cannot contact the author, then the content host must take down or disable access to the complained-of content.[1267]

The second component of the Act which may affect its use against multinational internet companies is its jurisdictional reach. In *V v Google*, Google argued that the Act was not applicable to an overseas organisation that was registered in the United States. Google argued that while Google New Zealand was a subsidiary, it was a separate legal entity and had "no control over, nor involvement in, the operation of the Google search engine."[1268] However, while the argument was raised, the Judge did not have to making any findings regarding it because on the facts of the case an order was not warranted. Harvey has also argued that being domestic New Zealand legislation, the Act does not apply to "individuals or content hosts who are located in other jurisdictions."[1269]

[1266] HDCA, s 23–25.
[1267] Section 24(2).
[1268] *V v Google*, above 1264, at [21].
[1269] Harvey, above n 1265, at [4.265].

Before the Privacy Act 2020 came into force, jurisdictional issues existed with the Privacy Act 1993.[1270] Some claimed it did not apply to overseas-based organisations that collected personal information from New Zealanders.[1271] Toy argued to the contrary. Toy's argument was that the Privacy Act 1993 should be treated consistently with the tort of defamation because both "incorporate the right to prevent the communication of information".[1272] Defamation holds that "the tort will be committed where the damage to reputation occurs".[1273] Accordingly, Toy argued that the Privacy Act should also apply where the consequences of conduct are felt, for example, where information is collected in comprehensible form.[1274]

The present research argues that Toy's logic should apply to the HDCA; that the Act should apply where the consequences of harmful digital communications occur, not where an organisation locates its server. However, rather than relying on jurisdictional arguments, the issue should be clarified by amendment to the HDCA so that its jurisdictional provision mirrors that in the Privacy Act 2020.[1275] This will assist in ensuring that multinational organisations who run platforms where much digital communication harm occurs cannot evade the requirements of the Act.

V Conclusion

The HDCA clearly includes privacy matters within its ambit. The risk of overlap with the Privacy Act was highlighted when the law was proposed, but the preference was to allow complainants to have a choice of forum. There are, however, constraints to the HDCA's ability to protect privacy. The information at issue has to be sensitive, it has to cause serious emotional distress, the breach has to be serious or repeated, and the court has a broad range of factors it must consider before it can order relief, including the right to freedom of expression. In addition, the Act cannot be used against search engines and online content hosts can mitigate the effects of the Act by complying with the safe harbour provisions. Furthermore, the Act is most commonly viewed or positioned as a mechanism for addressing cyberbullying

[1270] See Privacy Foundation "Submission to the Justice Committee on the Privacy Bill 2018" at [23]. These jurisdictional issues have been laid to rest by the Privacy Act 2020. See Chapter 5(III)(B)(1) for a discussion of the extra-territorial effect of the Privacy Act 2020.
[1271] Law Commission, above n 292, at [14.30].
[1272] Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24 NZULR 222 at 233.
[1273] At 233.
[1274] At 233.
[1275] See Privacy Act 2020, s 4(1)(b).

or online harassment and revenge porn, so it might not necessarily be the choice of forum for those who are suffering from the effects of once public facts.[1276]

However, where those hurdles can be surmounted the HDCA does provide an erasure remedy and one that can be used against the media. The ability to bring an action against the media is important because the exemption in the Privacy Act 2020 for news activities means the Privacy Act cannot be used where once public facts are published as part of such activities.[1277] Furthermore, the HDCA's simplified court procedure, which is designed to be user-friendly, cost-effective and used without professional legal support,[1278] provides a more *accessible* remedy than the disclosure tort.

However, the above analysis has determined that there are parts of the HDCA that would benefit from amendment. First, the requirement under s 12(2)(a) to have a serious or repeated breach appears redundant considering the harm requirement of the Act and the s 19(5) factors the court must consider before granting a remedy. Second, the jurisdictional reach of the Act should be clarified so that the HDCA mirrors the wording of the Privacy Act 2020. Whether any further amendments are required to the HDCA should be a 'wait and see' exercise. The Act is relatively new, and both the extent to which it will be used as a right to erasure and the overall effectiveness of its use in this manner remains to be seen.

[1276] See Ministry of Justice "Harmful Digital Communications" < www.justice.govt.nz>, which states: "Cyberbullying and other modern forms of harassment and intimidation can have a devastating impact on people, especially children and teenagers."
[1277] See Privacy Act 2020, s 8.
[1278] See Taryn Gudmanz "Harmful Digital Communications" (2019) 927 Law Talk 46. The application to the District Court is made via an e-form and there is no filing fee.

9 A PACKAGE OF AMENDMENTS TO PROTECT ONCE PUBLIC FACTS

I Introduction

From the earliest development of privacy theory there has been a recognition that privacy can protect once public facts. This recognition reflects the fact that valid privacy interests are engaged with the publication of once public facts. These interests align with the core values that broader privacy protection engages, like liberty, dignity and autonomy. Furthermore, real harm can be caused by publication of once public facts. The public component of these facts can hinder protection in some circumstances. However, the issue is mitigated by increasing recognition that there is a place for privacy in public, and that sometimes the right to freedom of expression must be constrained where the expression serves no valid societal ends.

The previous chapters investigated the scope of existing legal mechanisms to protect once public facts and identified shortfalls in those mechanisms. To address these shortfalls, and ensure a consistent and robust development of privacy law in New Zealand, this chapter proposes a package of amendments to the legal mechanisms discussed herein to enable appropriate privacy protection for once public facts. The package of amendments takes a 'whole-of-law' approach, recognising that what is required is a suite of protective measures which can be deployed in the most appropriate circumstances. Tort protection is required because the Privacy Act excludes some news media activities from its ambit, yet the media's reach, accessibility and need to provide a continual stream of news for the community, means that it is one of the most common defendants in privacy cases. However, a court case is a costly and time-consuming endeavour. Against the media, therefore, the HDCA might provide a low-cost, user-friendly option. For those entities subject to the Privacy Act, that Act also provides a user-friendly and accessible way to address inappropriate use of personal information. In some areas the recommended changes are not solely focused on once public facts, but rather reflect refinements that will benefit all potential claimants because they are directed at ensuring a clear, robust, principled and structured approach to the law. The amendments take privacy law to the next level of its evolution as an important and valued mechanism in New Zealand.

A 'whole-of-law' approach also requires consideration of law reform which is ultimately outside the ambit of this thesis. The intent here is to lay weight behind other calls for changes

in these areas.[1279] It is the position of this thesis that serious consideration needs to be given to recognising privacy as a human right – preferably as a new right under the NZBORA, but at a minimum via judicial recognition of its elevated status. This thesis also argues that the Clean Slate Act needs to be revisited. The rules are narrow and fail to recognise that there are some prison sentences that are perhaps worthy of protecting against disclosure. A broadened Clean Slate Act would ensure a deeper societal commitment to rehabilitation, liberty and self-determination. The graduated approach to spent convictions seen in the United Kingdom deserves close investigation, although whether the specific time frames for convictions becoming spent reflect the societal expectations of New Zealanders is an issue that would need to be addressed.

II The Package of Amendments

A The Privacy Act 2020

It is recommended that the Privacy Act 2020 is amended as described below.

1. The concepts of erasure and deletion should be removed from the definition of "correct". IPP 7 thus becomes a tool focused on correction of information, and a new IPP, focused solely on erasure, should be included in the Privacy Act.

2. The new erasure IPP needs to address the specific items identified in paras (3)–(6) below. The erasure procedure should be subject to operational provisions similar to subpart 2 of Part 4 of the Privacy Act, with appropriate amendments. Section 69(3) also needs to apply to the erasure right, allowing people to bring complaints to the Privacy Commissioner where an agency has refused an erasure request.

3. The grounds for erasure should be wider than accuracy and data quality. Accurate information can cause continuing harm where its use is excessive and irrelevant in regard to the purposes for which it is being used. Furthermore, there needs to be an ability for people to have their data erased where circumstances change and their individual interests outweigh the interests of the agency.

[1279] See Butler, above n 1083. See also, for example, New Zealand Law Society "Review of Clean Slate legislation needed, says NZLS" (20 July 2016) NZLS <www.lawsociety.org.nz>.

4. The circumstances in which an erasure tool could operate are numerous. Once public facts could be held by media archives, they could be part of public records like court records, or they could be historical social media posts. The facts could be 3 years old or 25 years old.[1280] What is required, therefore, is clarity regarding the considerations for determining whether information is irrelevant, inadequate or excessive. This clarity can be drawn from various sources. The proportionality assessments conducted under the disclosure tort in England and by the ECtHR are one such source. Guidance can also be obtained from other sources, like the Article 29 Data Protection Working Group Guidelines.[1281] This information will also be relevant for determining when the individual's privacy interests outweigh the agency's interests. The OPC should issue specific guidance on these matters.

5. Under IPP 9 organisations are allowed to hold information for exceptionally long periods of time. As a result, people should be able to request agencies erase their information where IPP 9 is being breached. This makes the purpose expiry of IPP 9 a point at which people can exercise direct control over their data and force agencies to be directly accountable for justifying the length of time it holds personal information. Furthermore, any breach of the IPPs by an agency which directly affects a person's personal information (for example, a notifiable breach) should also be a ground for erasure.[1282]

6. While children are clearly a special case, this thesis argues that the proposed new IPP appropriately addresses the issues of children. In particular, the right to have data erased that is out of date and excessive should be able to deal with data provided by children where they were not fully aware of the consequences and risks of data-sharing. The issue of children's particular vulnerability, however, should be supplemented by specific guidance from the OPC.[1283]

7. The reasonable steps of IPP 7 should not be included in the erasure IPP. Agencies that hold personal information assume responsibility for the data. An agency should not be able to abdicate responsibility merely because the way it has established its business processes makes erasure unreasonable or impractical. However, in recognition of the fact that in some instances erasure steps may impose a cost that is disproportionate, the IPP proposes including the ability for agencies to utilise a form of obscurity where full erasure is not practicable, provided that such solution is agreeable to the person seeking erasure.

[1280] See *FS v Television New Zealand Ltd*, above n 442 and *Sidis*, above n 11.
[1281] See the discussion at n 1191.
[1282] See Privacy Act 2020, s 115.
[1283] This recommendation was also made by the Ministry of Justice, above n 622, at [125].

8. To ensure the erasure tool is consistent with s 5 of the NZBORA, it is recommended that it does not apply where retention of the information is necessary for exercising the right of freedom of expression. This exemption may require, in some instances, organisations to conduct assessments of potentially competing interests. Nonetheless, the case law regarding the disclosure tort is instructive and a considerable number of resources are available as a result of the decision in *Google Spain* to assist those that will make the determinations, for example the Article 29 Data Protection Working Group Guidelines. The OPC should issue specific guidance on conducting such assessments to assist those making the determinations.

9. A 'straw man' of the proposed new erasure IPP is set out below as Figure 2. This thesis recommends that the straw man IPP forms the basis of future law reform proposals for the Privacy Act in this regard.[1284]

10. To support the enhanced erasure tool, it is also recommended that IPP 8 is amended to align its grounds for non-use with the grounds of erasure in the proposed new IPP. This amendment will ensure consistency between the proposed new IPP and IPP 8 and provide people with another mechanism to ensure agency use of their personal information is appropriate. The proposed new wording of the existing IPP 8 is set out below (with the new parts shown underlined), but with one feature which requires additional comment. It is recommended that the 'reasonable steps' are retained in IPP 8. This retention of a requirement that has been rejected for IPP 9 is because IPP 8 imposes obligations on agencies *without input from individuals*. In such instances, not having reasonable steps may impose a burden too great for some organisations. However, where a person advises an agency that a use is likely to breach the IPP 8, then an agency must act appropriately on that advice (for example, by weighing the full facts and interests on both sides) or risk being in breach of the reasonable steps.

    With the recommended amendments incorporated, it is proposed that IPP 8 should state:

[1284] For an example of another proposed erasure tool for New Zealand see Karlsen, above n 1249, at 539–540.

Information privacy principle 8

Accuracy, Relevance, of personal information to be checked before use or disclosure

An agency that holds personal information must not use or disclose that information without taking such steps that are, in the circumstances, reasonable to ensure that the information is:
(a) accurate, complete and up to date; and
(b) adequate, relevant, necessary and not misleading or excessive,
having regard to the purposes for which it was collected, held or used.

Figure 2

Proposed New Erasure IPP

Information privacy principle x

Erasure of personal information

(1) An individual whose personal information is held by an agency can require that agency to erase his or her personal information held by that agency where:

(a) The information is inaccurate, incomplete or out of date having regard to the purposes for which it was collected or held;

(b) The information is inadequate, irrelevant, unnecessary, misleading or excessive having regard to the purposes for which it was collected or held;

(c) The information has been retained in contravention of IPP 9;

(d) The information has been retained in compliance with IPP 9, however, the purposes are overridden by the interests or rights of the individual which require protection of personal information; or

(e) The agency has otherwise breached any IPP set out in this Act which directly affects the personal information of that individual.

(2) Where an individual successfully establishes a right to erasure under s (1), the individual shall request the agency to erase the information, and the agency shall erase the personal information without undue delay. Where erasure of the information is not practicable, then the agency shall take such steps to obscure the information that are agreeable to the individual concerned.

(3) The right set out in this section shall not apply, or its method of exercising may be modified accordingly, to the extent that retention of the information is necessary for exercising the right of freedom of expression or compliance with any legal obligation to which the agency is subject which requires retention of the information.

B Disclosure Tort

1 Elements of the cause of action

In order to establish the cause of action for the disclosure tort, the plaintiff must prove: (1) the existence of facts in respect of which there is a reasonable expectation of privacy; and (2)

publicity given to those private facts that would be considered highly offensive to an objective reasonable person. This thesis recommends that this test is refined as set out below.

1. The second element of the cause of action – the highly offensive test – is abandoned. The reasons for this recommendation are detailed in Chapter 6 above.

2. The remaining reasonable expectation test is elaborated upon by recognition that the test comprises the elements described in paras 2.1–2.3 below.

    2.1. Consideration of the specific circumstances of the case. It is difficult to provide a comprehensive list of the types of activities that need to be considered, but generally this element will look at the nature of the information at issue, as well as a range of factors like the location of the plaintiff, plaintiff attributes (for example, whether they are a public figure, their age and actions regarding the disclosure) and plaintiff's consent. Other relevant factors are the nature and purpose of the intrusion (including how the information came into the hands of the defendant) and the effects on the plaintiff. For once public facts, other factors should be considered, such as the length of time since original publication, changed circumstances during that period of time, the extent of the original and current publication, and the current accessibility of the original information.

    2.2. An empirical analysis of the social and regulatory environment in which the claimed invasion arose. This analysis should include consideration of wider societal attitudes to privacy, the prevailing statutory environment in New Zealand, including the Privacy Act 2020, BSA jurisprudence and the Clean Slate Act, together with any international legislation that may impact on societal understandings of privacy, including the GDPR.

    2.3. The core values assessment which requires consideration of the core values and benefit to be derived from protecting the privacy interest in the particular case. In easy cases – involving inherently private information like medical, or health or financial information, or information that reveals intimate details of a person's lifestyle – the benefits and core values will be obvious, and can be disposed of in short order. However, for difficult cases, what is required is a careful consideration of the individual and societal benefits of allowing the zone of privacy. These benefits could be supporting liberty, rehabilitation, dignity,

personhood, autonomy, sanctity of the home, intimacy, and relationship-building. For a once public fact scenario, the core values assessment will involve consideration of interests in rehabilitation, prevention of harm, liberty to develop self, and protection of dignity and autonomy.

2 Defence

The final element of the disclosure tort is the legitimate public interest defence. This thesis argues that in determining if the defence of public interest has been established, the courts should employ a proportionality framework, as was described in detail in Chapter 7. A diagrammatic representation of the proportionality framework is set out in Figure 3 below.

Figure 4 sets out a diagrammatic representation of the recommended changes to the entire disclosure tort.

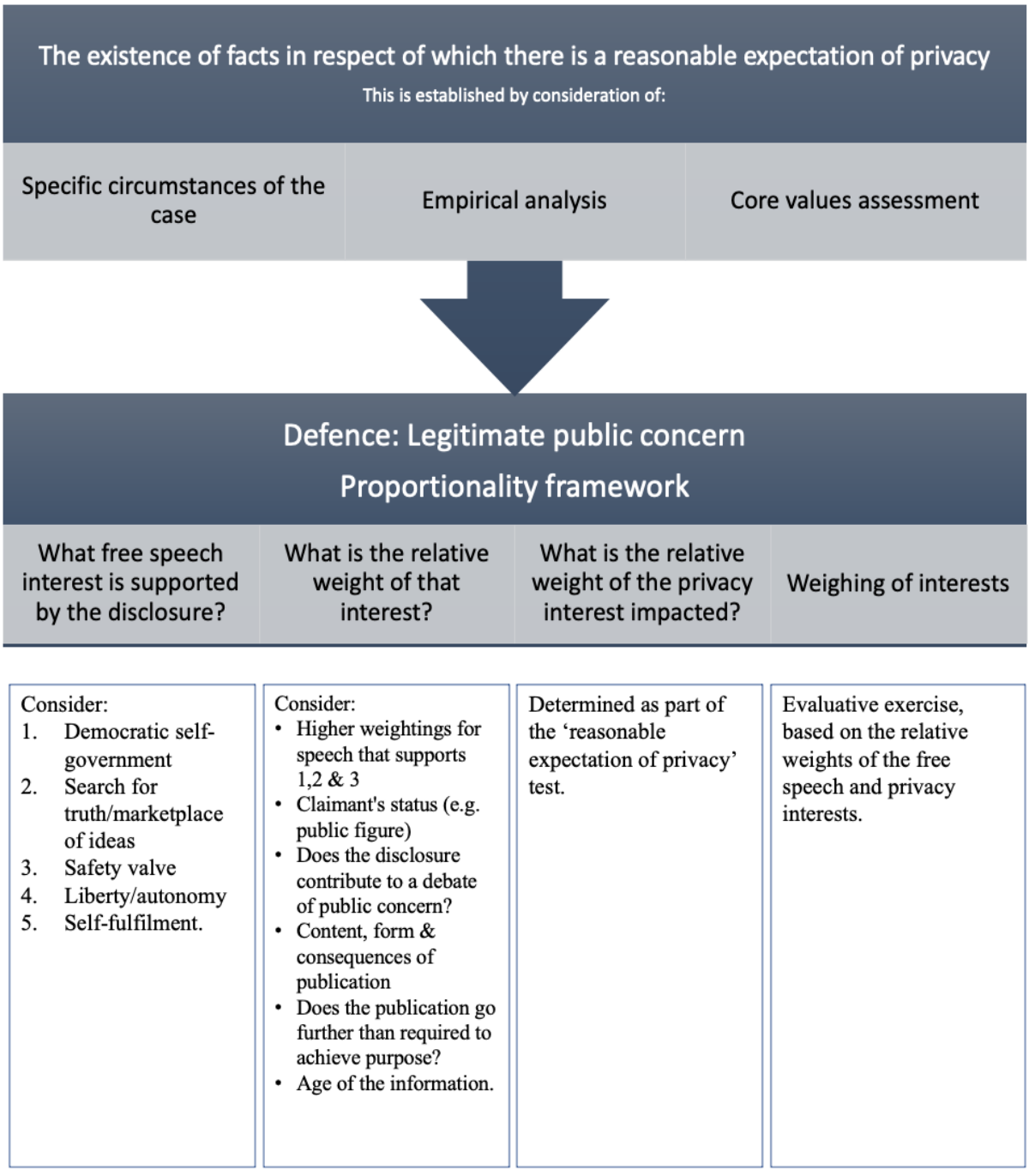
Figure 3

Proportionality Framework

Defence: Legitimate public concern Proportionality framework			
What free speech interest is supported by the disclosure?	What is the relative weight of that interest?	What is the relative weight of the privacy interest impacted?	Weighing of interests
Consider: 1. Democratic self-government 2. Search for truth/marketplace of ideas 3. Safety valve 4. Liberty/autonomy 5. Self-fulfilment.	Consider: • Higher weightings for speech that supports 1,2 & 3 • Claimant's status (e.g. public figure) • Does the disclosure contribute to a debate of public concern? • Content, form & consequences of publication • Does the publication go further than required to achieve purpose? • Age of the information.	Determined as part of the 'reasonable expectation of privacy' test.	Evaluative exercise, based on the relative weights of the free speech and privacy interests.

Figure 4

Disclosure Tort



C Harmful Digital Communications Act 2015

The ability to use the HDCA as a limited RTBF in the form of a right to erasure akin to those seen in data protection statutes, and its relatively recent addition to the toolbox to address the risks of the digital information age, argue against any need to make substantial changes to the Act at this point in time. The Act's use as a tool to address privacy issues needs to be monitored. However, the present research has determined two particular parts of the Act require immediate change. These areas have the potential to hamper the overall usefulness of the current Act, including as a tool to help protect once public facts. The first area of concern is s 12(2)(a). As argued in Chapter 8(III), the requirement for a serious or repeated breach appears redundant considering the harm requirement and the s 19(5) factors the court must consider before granting an order under the Act. The second concerns clarity on the jurisdictional reach of the Act, which should be amended to mirror that of the Privacy Act 2020, so that multinational organisations who run ubiquitous tools that cause substantial harm cannot easily escape the requirements of the Act.

III Conclusion

This chapter has drawn together all the present research into a recommended package of amendments to enable appropriate protection for once public facts. The package of amendments takes a whole-of-law approach, recognising that what is required is a suite of protective legal measures which can be deployed in the most appropriate circumstances, depending on who has committed the breach of privacy, what the complainant wants to achieve, and the resources they have to dedicate to the matter. It is argued that these protective legal measures can be achieved by amendments to the Privacy Act 2020, the HDCA, and the disclosure tort.

In addition to the direct amendments and refinements recommended, this thesis has identified two other changes which it strongly advocates for, and which would ensure that privacy fulfils its potential as an interest that society values, both generally and for those trying to rebuild their lives under the stigma of a criminal conviction. A first change is recognition of privacy as a human right – preferably as a new right under the NZBORA, but at a minimum via judicial recognition of its essential importance as a right. The second is a review of the Clean Slate Act. As noted above, the Clean Slate Act is narrow and fails to recognise that sometimes having previous convictions for lesser prison sentences hidden can be an important component of supporting rehabilitation. A broadly pitched Clean Slate Act would help to

ensure a deeper societal commitment to the policies of rehabilitation and redemption that underpin the Act.

10 CONCLUSION

In 1983 Parent argued that: "What belongs to the public domain cannot without glaring paradox be called private".[1285] Since that time, people have begun to live their lives in public ways that were unthinkable then. People post information onto SNSs, they find the information they want on (or via) the internet (including news and government records), they are subject to known or unknown surveillance in public places, and they carry devices that are continually gathering data. The present research has taken one aspect of the fundamental change that has occurred in information management in the last 40 years – the persistent availability of historical public information (once public facts) – and considered whether protecting this information as 'private' is still a glaring paradox; or is protecting such information the next step in the evolution of privacy law.

Ultimately what the research has found is that once public facts should gain privacy protection in law in New Zealand, in appropriate circumstances. Protecting once public facts assists in protecting people's interests in rehabilitation, redemption, forgiveness, autonomy, liberty and dignity, it protects people from substantial harm, and is broadly consistent with the development of privacy law internationally. Protecting once public facts is not a glaring paradox; it is privacy for our time. However, for once public facts to achieve an appropriate level of protection in New Zealand, various amendments to New Zealand's legal mechanisms for protecting privacy are recommended.

I Addressing the Research Questions

The present research started with the overarching question of whether once public facts should gain privacy protection in law. To address this question, five research sub-questions were posited. This chapter revisits those sub-questions and provides a summary of how the present research addressed those questions.

The first research sub-question asked whether it was appropriate to discuss once public facts under the banner of privacy. Chapter 3 addressed this question and argued that commonly cited theories of privacy have provided room for protection of once public facts. Furthermore, many privacy scholars have argued compellingly for a broad view of privacy that protects privacy in public. Acceptance of these arguments means that it does not matter whether once public facts are viewed as 're-growing' their private status or are simply still public facts, they

[1285] Parent, above n 78, at 308.

can theoretically be protected by the law of privacy. It was recognised at this stage of the research that tikanga Māori is an important input into concepts of privacy in New Zealand. However, due to a lack of scholarship on the topic, no conclusions could be drawn between tikanga Māori's concept of privacy and once public facts. Instead, the research noted that more scholarship on Māori and privacy is required, and that ultimately legal mechanisms which where broad and principled would allow for nuanced cultural perspectives in the future.

The second research sub-question asked what are the core values affected by once public facts. Using 'anchoring vignettes', real-life scenarios involving once public facts, Chapter 4 considered the core values at the heart of privacy, and argued that protecting once public facts can protect the values of liberty, rehabilitation, self-development, dignity and autonomy. It also found that failure to protect these interests can cause significant harms, for example emotional distress, job losses and ostracisation from family and friends, that may often exceed the actual wrong that was done. Furthermore, the present research has determined that the benefits of protecting once public fact remain despite the fact that modern information technology has fundamentally changed information management. The thesis has ultimately determined that the values society holds near should dictate the shape of technology, not vice versa.

The third research sub-question asked what existing legal mechanisms can be used to protect once public facts, and how effective those mechanisms were. Chapters 5, 6, 7 and 8 discussed the existing legal mechanisms, being the Privacy Act 2020, the common law disclosure tort, and the HDCA. This research found that the Privacy Act provides little protection for once public facts. The use restrictions (IPP 8) and erasure tools (IPP 7) in the Act are not broad enough to provide protection akin to that which exists internationally. This conclusion, alongside the benefits to be gained from protecting once public facts, led to the research arguing that amendments are required to the Privacy Act to address the gaps. These proposed amendments include a new erasure IPP and amendments to IPP 8.

In contrast, the research has argued that the disclosure tort can protect once public facts in appropriate circumstances and that such protection is consistent with the development of the disclosure tort to date. However, the present research also argues that improvements could be made to the tort to ensure robust protection for private information, including once public facts. The research on the HDCA found that the HDCA does provide a limited form of RTBF akin to the erasure mechanisms from data protection statutes. This erasure tool can be used against content publishers, but not search engines. However, there is a risk that the HDCA's

narrow interpretation to date, limited visibility as an erasure tool that can protect personal information and its jurisdictional reach may impact its overall effectiveness. The operation of the HDCA should be closely monitored to better understand its effectiveness as a privacy-protecting mechanism. In the short term, however, some amendments are recommended, including removing s 12(2)(a) and clarifying the HDCA's jurisdictional reach by ensuring it mirrors that set out in the Privacy Act 2020.

The fourth research sub-question asked how privacy and free speech should be balanced when they conflict. The conflict between privacy and free speech is of particular import to once public facts because once public facts are facts that are, or have been, public at some time. Chapter 7 considered the conflict between privacy and free speech in detail. The chapter delved into the reasons why free speech is so important, how the courts in New Zealand had attempted to address the conflict in the disclosure tort, and how various statutory mechanisms (including the Privacy Act 2020 and the Broadcasting Act 1989) have also addressed the conflict. The chapter argued that the development of the disclosure tort in New Zealand does not provide any particular free speech constraint on protecting once public facts, and that what was required in balancing privacy and free speech in the disclosure tort was a close focus on the facts of the case and an assessment of the relative weight of the interests involved. However, the chapter also argued that the defence to the disclosure tort would benefit from the application of a structured and principled framework for determining whether or not a disclosure was of legitimate public concern. In regard to the statutory balancing of privacy and free speech, it was argued that, to ensure compliance with the NZBORA, the proposed new erasure tool in the Privacy Act 2020 needed to include a specific requirement for agencies to weigh up the competing interests of privacy and free speech when it received an erasure request.

The final research sub-question asked what amendments to the existing legal privacy laws were required to ensure appropriate protection for once public facts. The conclusions set out in Chapters 5, 6, 7 and 8 proposed a suite of amendments and refinements to the legal mechanisms canvassed. In Chapter 9, these amendments were wrapped up into a package of recommended amendments, and set out the specific detail of each amendment. In addition to direct amendments to the Privacy Act 2020, the disclosure tort, and the HDCA, the present research also strongly advocates for two further developments which will help to recognise the importance of privacy. These changes are the recognition of privacy as a human right – preferably as a new right under the NZBORA, but at a minimum via judicial recognition of its status as a right, and a review of the Clean Slate Act. A broadly pitched Clean Slate Act

would help to ensure a deeper commitment to the policies of rehabilitation and redemption that underpin the Act.

II Contributions of the Research

This thesis makes several contributions to the literature of privacy and once public facts. Its contributions are predominantly in the areas of theory and law reform. In regard to the theory of privacy and once public facts, the present research has contributed by identifying the extent to which current and predominant theories of privacy are broad enough to encompass once public facts and arguing that most of these theories are wide enough to allow protection of once public facts under the banner of privacy. Furthermore, the present research's consideration of the core values of privacy and how protecting a zone of privacy around once public facts can uphold the same core values, demonstrates that protecting once public facts is an issue that society should care about.

This thesis' contribution to law reform takes the form of a proposed package of recommended amendments to a range of legal mechanisms in New Zealand to protect privacy. The value of this contribution is in the deep analysis that supports those recommendations. The present research has not simply looked at what is happening in other jurisdictions and said 'that is needed here'. Instead, the research has started with the roots of privacy, its core values and argued that protecting once public facts is an important issue for privacy. It has considered whether protection of once public facts is consistent with the development of the law to date, and benchmarked New Zealand's legal protections against those in comparator overseas jurisdictions.

The package of law reform contained in the research also takes a 'whole-of-law' approach, proposing amendments and refinements across the suite of privacy laws in New Zealand. In 2018, during the legislative review process for the Privacy Act 1993, the Ministry of Justice recommended the RTBF as a future law reform topic.[1286] This present research could be used as a baseline for that law reform process, giving the law process a welcome head start. The HDCA appears to have been the subject of little research to date, with none focusing on its role in regard to privacy. This thesis contributes to a better understanding of that Act's role as a privacy-protecting mechanism. The disclosure tort is still in development in New Zealand. This thesis provides in-depth research on its development to date and proposes enhancements and refinements that could assist with the tort's continued development. Recently, the Court

[1286] Ministry of Justice, above n 683, at 41.

of Appeal noted that the disclosure tort "may well benefit from re-examination".[1287] The analysis and conclusions in this thesis can contribute to that re-examination.

There is also hope that the contribution of this thesis will be wider. There are common-law jurisdictions whose development of the disclosure tort has occurred slower than in New Zealand (for example, Australia and Canada). The laws and legal systems of these countries have much in common with New Zealand, so this thesis might provide useful insight for the future development of privacy law in those jurisdictions.

[1287] *Hyndman*, above n 789, at [73].

BIBLIOGRAPHY

A Cases

1 New Zealand

Courts

Andrews v Television New Zealand Ltd [2009] 1 NZLR 220 (HC).

Bradley v Wingnut Films Ltd [1993] 1 NZLR 415 (HC).

Brooker v Police [2007] NZSC 30, [2007] 3 NZLR 91.

Brown v Attorney General [2006] NZAR 552 (DC).

C v Holland [2012] NZHC 2155, [2012] 3 NZLR 672.

Clague v APN News and Media Ltd [2012] NZHC 2898, [2013] NZAR 99.

Driver v Radio New Zealand Ltd [2020] NZHC 2903.

Henderson v Walker [2019] NZHC 2184.

Hosking v Runting [2005] 1 NZLR 1 (CA).

Hyndman v Walker [2019] NZHC 2188.

Hyndman v Walker [2021] NZCA 25.

L v G [2002] NZAR 495 (DC).

Lange v Atkinson [1997] 2 NZLR 22 (HC).

P v D [2000] 2 NZLR 591 (HC).

Peters v Bennett [2020] NZHC 761.

Police v B [2017] NZHC 526, [2017] 3 NZLR 203.

Reekie v Television New Zealand Ltd HC Auckland CIV-2009-404-003728, 8 February 2010.

Rogers v Television New Zealand Ltd 22 CRNZ 668 (HC).

Rogers v Television New Zealand Ltd [2007] 1 NZLR 156 (CA).

Rogers v Television New Zealand Ltd [2007] NZSC 91, [2008] 2 NZLR 277.

Takamore v Clarke [2012] NZSC 116; [2013] 2 NZLR 733.

Tucker v News Media Ownership Ltd [1986] 2 NZLR 716 (HC).

TV3 Network Services Ltd v Broadcasting Standards Authority [1995] 2 NZLR 720 (HC).

TVNZ v KW HC Auckland CIV-2007-485-1609, 18 December 2008.

V v Google [2019] NZHC 488.

Wensor v Stuff [2017] NZDC 979.

X v R [2020] NZCA 387.

Tribunals

Armfield v Naughton [2014] NZHRRT 48.
CanWest TV Works Ltd v XY [2008] NZAR 1.
EFG v Commissioner of Police HRRT 11/2005, 21 December 2006.
Hammond v Credit Union Baywide [2015] NZHRRT 6
Henderson v Commissioner of Inland Revenue HRRT 49/02, 10 June 2004.
Macdonald v Healthcare Hawkes Bay [2000] NZCRT 35.
Plumtree v Attorney-General on behalf of the New Zealand Defence Force HRRT 29-01, 2 October 2002.
Wilson v Accident Compensation Corporation HRRT 14/2002, 1 July 2003.

Office of the Privacy Commissioner

Case Note 13066 [1998] NZPrivCmr 10 (1 April 1998).
Case Note 15376 [2001] NZPrivCmr 1 (April 2001).
Case Note 218236 [2011] NZ PrivCmr 4 (1 February 2011).
Case Note 284027 [2018] NZPrivCmr 1 (18 January 2018).

Broadcasting Standards Authority

Anne Baker (2) v Television New Zealand Ltd 12/12/96, BSA Decision Nos 1996-170, 1996-171.
Arthur v Television New Zealand Ltd 22/02/07, BSA Decision No 2006-115.
Balfour v Television New Zealand Ltd 21/3/06, BSA Decision No 2005-129.
Devereux v Television New Zealand Ltd 25/08/15, BSA Decision Nos 2015-027.
Drury v TV3 Network Services Ltd 10/10/96, BSA Decision Nos 130-96, 131-96 and 132-96.
FS v Television New Zealand Ltd 19/12/2012, BSA Decision No 2012-036.
IY v Mediaworks TV Ltd 5/09/2018, BSA Decision No 2018-032.
Lewis v TVNZ 12/02/08, BSA Decision No 2007-109.
MA v TVNZ Ltd, 22/02/11, BSA Decision No 2010-084.
MM v TV3 Network Services Ltd 15/07/99, BSA Decision Nos 1999-103, 1999-104.
Mrs S v TV3 Network Services Ltd 19/1/94, BSA Decision No 1994-001.
Reekie v Television New Zealand Ltd 6/7/10, BSA Decision No 2009-111.

Rickard v Television New Zealand Ltd 19/04/17, BSA Decision No 2016-098.
SW v Television New Zealand Ltd 18/12/2015, BSA Decision No 2015-030.
T v Television New Zealand Ltd 1/10/98, BSA Decision No 1998-119.
Television New Zealand Ltd v Walden 19/9/06, Decision No 2006-061.
TJ v Television New Zealand Ltd 17/06/04, BSA Decision No 2013-092.

2 Australia

Australian Broadcasting Corporation v Lenah Game Meats Ltd (2001) 208 CLR 199.
Jane Doe v Australian Broadcasting Corporation [2007] VCC 281 (CC).
Giller v Procopets [2008] VSCA 236 (CA), (2008) 24 VR 1.
Grosse v Purvis [2003] QDC 151, (2003) Aust Torts Reports 81-706 (DC).
Wilson v Ferguson [2015] WASC 15 (SC).

3 Canada

Canada v John Doe 2016 FCA 191, [2016] FCJ No 695 (CA).
Griffin v Sullivan 2008 BCSC 827, [2008] BCJ No 1333 (SC).
Jane Doe 464533 v ND 2016 ONSC 541, [2016] OJ No 382 (SC).
Jones v Tsige 2012 ONCA 32, [2012] OJ No 148 (CA).

4 England

Campbell v MGN Ltd [2004] UKHL 22, [2004] 2 AC 457.
London Regional Transport v The Mayor of London [2001] EWCA Civ 1491, [2001] All ER (D) 80 (Aug).
McKennitt and others v Ash and another [2005] EWHC 3003 (QB), [2006] IP & T 605.
Mosley v News Group Newspapers Ltd [2008] EWHC 1777 (QB), [2008] All ER (D) 322 (Jul).
Murray v Express Newspapers [2008] EWCA Civ 446, [2009] Ch 481.
NT 1 & NT 2 v Google LLC [2018] EWHC 799 (QB), [2019] QB 344.
OBG Ltd v Allan; Douglas v Hello! Ltd (No 3) [2007] UKHL 21, [2008] 1 AC 1.
PJS v News Group Newspapers Ltd [2016] UKSC 26, [2016] AC 1081.
R v Broadcasting Complaints Commission, ex parte Granada Television Limited [1995] EMLR 163 (CA).

R v Chief Constable of the North Wales Police and others, ex parte AB and another [1997] 3 WLR 724 (QB).
R v Secretary of State for the Home Department, ex p Simms [2000] 2 AC 115 (HL).
Re S (a child) [2003] EWCA Civ 963, [2004] Fam 43.
Richard v British Broadcasting Corporation [2018] EWHC 1837 (Ch), [2018] 3 WLR 1715.
Vidal-Hall and others v Google Inc [2015] EWCA Civ 311, [2016] QB 1003.
Weller v Associated Newspapers Ltd [2015] EWCA Civ 1176, [2016] 1 WLR 1541.
XKF v BBC [2018] EWHC 1560 (QB).
Yeo v Times Newspapers Limited [2015] EWHC 3375 (QB), [2015] All ER (D) 230 (Nov).

5 Europe

Axel Springer AG v Germany (2012) 55 EHHR 6.
Beizaras and Levickas v Lithuania [2020] ECHR 19 (ECHR).
Case C-131/12 Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales ECLI:EU:C:2014:317.
Case of LB v Hungary ECHR 36345/16, 12 January 2021.
Case of National Federation of Sportspersons' Associations and Unions (FNASS) and Others v France ECHR 48151/11 and 77769/13, 18 April 2018.
Hurbain v Belgium [2021] ECHR 544 (Grand Chamber).
Joined Cases C-141/12 *YS v Minister voor Immigratie, Integratie en Asiel* and Case C-372/12 *Minister voor Immigraties, Integratie en Asiel v M and S* ECLI:EU:C:2014:2081.
Karakó v Hungary (App no 39311/05), 28 April 2009.
ML and WW v Germany [2018] ECHR 554 (ECHR).
NŠ v Croatia ECHR 36908/13, 10 September 2020.
Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland ECHR 931/13, 27 June 2017.
Sky Österreich GmbH v Österreichischer Rundfunk ECLI:EU:C:2013:28.
Von Hannover v Germany (2005) 40 EHRR 1.
Von Hannover v Germany (No 2) (2012) 55 EHRR 15.

6 United States

Barberi v News-Journal Co 189 A 2d 773 (Del 1963).
Bartnicki v Vopper 532 US 514 (2001).
Briscoe v Reader's Digest Association 483 P 2d 34 (Cal 1971).
Campbell v Seabury Press 614 F 2d 395 (5th Cir 1980).

Carlisle v Fawcett Publication Inc 201 Cal App 2d 733 (1962).
Cox Broadcasting Corp v Cohn 420 US 469 (1975).
Diaz v Oakland Tribune Inc 139 Cal App 3d 118 (1983).
Dun & Bradstreet Inc v Greenmoss Builders Inc 472 US 749 (1985).
Florida Star v BJF 491 US 524 (1989).
*Gates v Discovery Communications Inc Gates*101 P 3d 552 (Cal 2004).
Gilbert v Medical Economics Co 665 F 2d 305 (10h Cir 1981)
Gill v Hearst Publishing Company 253 P 2d 441 (Cal 1953).
Henningsen v Bloom field Motors Inc 161 A 2d 69 (1960).
Hill v National Collegiate Athletic Assn. P 2d 633 (Cal 1994).
Howard v Des Moines Register & Tribune Co 283 NW 2d 289 (Iowa 1979).
Kapellas v Koffman 459 P 2d 912 (Cal 1969).
Konigsberg v State Bar of California 366 US 36 (1961).
Melvin v Reid 297 P 91 (Cal App 1931).
Moreno v Hanford Sentinel Inc 172 Cal App 4th 1125 (2009).
Multimedia WMAZ v Kubach 443 SE 2d 491 (Ga App 1994).
O'Hilderbrandt v Columbia Broadcasting System Inc 40 Cal App 3d 323 (1974).
Oklahoma Publishing Co v District Court of Oklahoma 430 US 308 (1977).
Rawlins v Hutchinson Publishing Co 543 P 2d 988 (Kan 1975).
Riggs v Palmer 115 NY 506 (1889).
Roshto v Hebert 439 So 2d 428 (La 1983).
Shulman v Group W Productions 955 P 2d 469 (Cal 1998).
Sidis v F-R Pub Corp 113 F 2d 806 (2d Cir 1940).
Smith v Daily Mail Publishing Co 443 US 97 (1979).
Smith v National Broadcasting Co 292 P 2d 600 (Cal App 1956).
Uranga v Federated Publs Inc 67 P 3d 29 (Idaho 2003).
US Department of Justice v Reporters Committee for Freedom of the Press 489 US 749 (1989).
Werner v Times-Mirror Co 193 Cal App 2d 111 (1961).
YG v Jewish Hospital of St Louis 795 SW 2d 488 (Mo App 1990).

B Legislation

1 New Zealand

Broadcasting Act 1989.

Child Protection (Child Sex Offender Government Agency Registration) Act 2016.
Criminal Records (Clean Slate) Act 2004.
Criminal Records (Expungement of Convictions for Historical Homosexual Offences) Act 2018.
Harmful Digital Communications Act 2015.
Health Information Privacy Code 1994.
New Zealand Bill of Rights Act 1990.
Privacy Act 1993.
Privacy Act 2020.
Summary Offences Act 1981.

2 Australia

Crimes Act 1914 (Cth).
Criminal Records Act 1991 (NSW).
Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld).
Privacy Act 1998 (Cth).
Spent Convictions Act 2000 (ACT).

3 Canada

British Columbia Privacy Act RSBC 1996 c 373.
Canadian Charter of Rights and Freedoms (Part I of the Constitution Act 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11).
Manitoba Privacy Act CCSM 1987 c P125.
Newfoundland Privacy Act RSNL 1990 c P-22.
Personal Information Protection Act, S.A.2003, c.P-6.5.
Personal Information Protection and Electronic Documents Act, SC 2000.
Saskatchewan Privacy Act RSS 1978 c P-24.

4 England

Human Rights Act 1998
Rehabilitation of Offenders Act 1974.

5 Europe

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data [1995] OJL 281.

Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data [2016] OJ L 119.

6 United States

CA Bus & Prof Code § 22581.
United States Constitution.

C Treaties and International Documents

International Covenant on Civil and Political Rights (open for signature 16 December 1966, entered into force 23 March 1976).

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (opened for signature 4 November 1950, entered into force 3 September 1953).

Te Tiriti o Waitangi (the Treaty of Waitangi).

Universal Declaration of Human Rights GA Res 217A (1948).

Declaration on the Rights of Indigenous Peoples GA Res 61/295 (2007).

D Books and Chapters in Books

American Law Institute *Restatement of the Law of Torts* (2 ed, 1977).

D Anderson "The Failure of American Privacy Law" in Basil Markesinis (ed) *Protecting Privacy* (Oxford University Press, Oxford, 1999).

Jordan Anderson “Dangerous Neighbours: Risk Control, Community Notification and Sex Offender Release” in J Pratt and J Anderson (eds) *Criminal Justice, Risk and Revolt against Uncertainty* (Palgrave Macmillan, Cham, 2020) 93.

Eric Barendt “‘A Reasonable Expectation of Privacy’: A Coherent or Redundant Concept?” in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 96.

S I Benn “Privacy, Freedom and Respect for Persons” in J Rolland Pennock and John W Chapman *Privacy: Nomos XIII* (Atherton Press, New York 1971) 1.

Jeff Berryman “Remedies for Breach of Privacy in Canada” in Jason NE Varuhas and N A Moreham (eds) *Remedies for Breach of Privacy* (Bloomsbury Academic, London, 2018).

Samuel Beswick and William Fotherby “The Divergent Paths of Commonwealth Privacy Torts” in Margaret I Hall (ed) *The Canadian Law of Obligations: Private Law for the 21st Century and Beyond* (LexisNexis Canada Inc, Toronto, 2018) 225.

Brian Bix *Jurisprudence: Theory and Context* (7th ed, Sweet & Maxwell, London, 2015).

Danah Boyd *It's Complicated: The Social Lives of Networked Teens* (Yale University Press, New Haven, 2014).

Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A commentary* (2nd ed, LexisNexis NZ Ltd, Wellington, 2015).

Lee A Bygrave *Data Privacy Law: An International Perspective* (Oxford University Press, Oxford, 2014).

Ursula Cheer *Burrows and Cheer Media Law in New Zealand* (7th ed, LexisNexis NZ Limited, Wellington, 2015).

Ursula Cheer and Stephen Todd “Invasion of Privacy” in Stephen Todd and others (eds) *Todd on Torts* (8th ed, Thomson Reuters, Wellington, 2019) 977.

Iain Christie and Adam Wolanski "Context and Background" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 3.

Julie E Cohen *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, New Haven (Conn), 2012).

Ian Dobinson and Francis Johns "Qualitative Legal Research" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 16.

Ronald Dworkin *Taking Rights Seriously* (Bloomsbury, London, 2013).

Arlene Fink *Conducting Research Literature Reviews: From the Internet to Paper* (Sage Publications, Los Angeles, 2014).

Lawrence M Friedman *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy* (2007 Standord University Press Stanford California).

Shane Greenstein *How the Internet Became Commercial* (Princeton, Princeton University Press, 2015).

Andres Guadamuz "Developing a Right to be Forgotten" in Tatiana-Eleni Synodinou and others (eds) *EU Internet Law: Regulation and Enforcement* (Springer International Publishing AG, Switzerland, 2017).

Yuriko Haga "Right to be Forgotten: A New Privacy Right in the Era of Internet" in Marcelo Corrales, Mark Fenwick, Nikolaus Forgó (eds) *New Technology, Big Data and the Law* (Springer Nature Singapore Pte Ltd, Singapore, 2017).

H L A Hart *The Concept of Law* (2nd ed, Clarendon Press, Oxford, 1994).

Davis Harvey *Collisions in the Digital Paradigm: Law and Rule-making in the Internet Age* (Hart Publishing, Oxford, 2017).

David Harvey *Internet.law.nz: Selected Issues* (4th ed, LexisNexis, Wellington, 2015).

Mark van Hoecke *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart Publishing, Oxford, 2011).

Māui Hudson and others "He Matapihi ki te Mana Raraunga" - Conceptualising Big Data through a Māori lens in Hēmi Whaanga, Te Taka Keegan & Mark Apperley (eds) *He Whare Hangarau Māori – Language, Culture & Technology* (Faculty of Māori and Indigenous Studies, University of Waikato, Hamilton, 2017).

Chris D L Hunt "Reasonable Expectations of Privacy in Canadian Tort Law" in Margaret I Hall (ed) *The Canadian Law of Obligations: Private Law for the 21st Century and Beyond* (LexisNexis Canada Inc, Toronto, 2018) 269.

Grant Huscroft "Freedom of Expression" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney *The New Zealand Bill of Rights* (Oxford University Press, Auckland, 2003) 308.

Terry Hutchinson "Doctrinal research: Researching the jury" in Dawn Watkins and Mandy Burton (eds) *Research Methods in Law* (Routledge, London 2013) 7.

Julie C Inness *Privacy, Intimacy, and Isolation* (Oxford University Press, New York, 1992).

Meg Leta Jones *Ctrl + Z: The Right to be Forgotten* (New York University Press, New York, 2016).

Bert-Jaap Koops and Masa Galic "Conceptualizing space and place: lessons from geography for the debate on privacy in public" in Tjerk Timan, Bryce Clayton Newell, Bert-Jaap Koops (eds) *Privacy in Public Space Conceptual and Regulatory Challenges* (Edward Elgar Pub, Northampton MA, 2017) 19.

Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Toward an Agenda* (ANU Press, Acton ACT, 2016).

David Lindsay "The 'Right to Be Forgotten' in European Data Protection Law" in Norman Witzleb (ed) *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, New York, 2014) 290.

Māori Marsden "God Man and Universe: A Māori View" in Michael King (ed) *Te Ao Hurihuri: The World Moves On – Aspects of Māoritanga* (Hick Smith & Sons Ltd, Wellington, 1975) 191.

Viktor Mayer-Schönberger *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, Princeton, 2009).

Joan Metge *New Growth From Old: The Whānau in the Modern World* (Victoria University Press, Wellington, 1995).

John Stuart Mill *On Liberty* (Penguin Books Ltd, London, 1974).

Brian C Murchison "Revisiting the American Action for Public Disclosure of Private Facts" in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, Cambridge, 2006) 32.

Helen Fay Nissenbaum *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books, California, 2010).

Michael Pendleton "Non-empirical Discovery in Legal Scholarship – Choosing, Researching and Writing a Traditional Scholarly Article" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 159.

Stephen Penk "Common Law Privacy Protection in Other Jurisdictions" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 113.

Stephen Penk "Future Directions and Issues" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 429.

Stephen Penk "Thinking About Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 1.

Gavin Phillipson "Press Freedom, the Public Interest and Privacy" in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 136.

Richard A Posner *The Economics of Justice* (Harvard University Press, Cambridge (Massachusetts), 1981).

Priscilla M Regan *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, Chapel Hill, 1995).

Khylee Qunice "Māori Concepts and Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 29.

Jon Ronson *So You've Been Publicly Shamed* (Picador, Basingstoke, 2015).

Paul Roth *Privacy Law and Practice* (online ed, LexisNexis, Wellington, 2018).

Daniel J Solove *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, New Haven, 2007).

Rosemary Tobin "Media Regulation: The Press Council and the Broadcasting Standards Authority" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 243.

Rosemary Tobin "The Common Law Tort of Invasion of Privacy in New Zealand" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 89.

Kristina Trykhlib "The Principle of Proportionality in the Jurisprudence of the European Court of Human Rights" (2020) EU and Comparative Law Issues and Challenges Series 128.

Raymond Wacks *Privacy: A Very Short Introduction* (2nd ed, Oxford University Press, Oxford, 2015).

Raymond Wacks *Privacy Vol 1* (Aldershot, Dartmouth 1993).

James Waldo, Herbert Lin and Lynette I Millett *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, Washing DC, 2007).

Mark Warby "Justifications and Defences" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 529.

Mark Warby, Adam Speker and David Hirst "Breach of Confidence" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 163.

Mark Warby, Adam Speker and David Hirst "Misuse of Personal Information" in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat and Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, New York, 2011) 223.

Alan F Westin *Privacy and Freedom* (Atheneum, New York, 1967).

Geoffrey Wilson "Comparative Legal Scholarship" in Mike McConville and Wing Hong Chui (eds) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007) 87.

Normann Witzleb "Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy" in Moreham and Varuhas (eds) *Remedies for Breach of Privacy* (Bloomsbury, Oxford, 2018) 377.

Shoshana Zuboff *The Age of Surveillance Capitalism* (Profile Books Ltd, London, 2019).

E Journal Articles

Patricia Sanchez Abril "Recasting Privacy Torts in a Spaceless World" (2007) 21 Harv J L & Tech 1 at 7.

Patricia Sanchez Abril and Jacqueline D Lipton "The right to be forgotten: who decides what the world forgets? (Data Privacy: Your Rights in a Digital World)" (2015) 103 Ky L J 363.

Anita L. Allen "Coercing Privacy" (1999) 40 Wm & Mary L Rev 723.

Anita Allen “Dredging up the Past: Lifelogging, Memory, and Surveillance” (2008) 75 U Chi L Rev 47.

Irwin Altman “Privacy Regulation: Culturally Universal or Culturally Specific?” (1977) 33 Journal of Social Issues 66.

Heidi Reamer Anderson “The Mythical Right to Obscurity: Pragmatic Defense of No Privacy in Public” (2012) 7 ISJLP 543.

Noberto Nuno Gomes de Andrade “Oblivion: The Right to be Different from Oneself Reproposing the Right to be Forgotten” (2012) 13 IDP 122.

Lisa M Austin “Re-reading Westin” (2019) 20 Theoretical Inquiries in Law 53.

Stephen Bates “The Prostitute, the Prodigy, and the Private Past” (2012) 17 Communication Law and Policy 175.

SI Benn “Privacy and Respect for Persons: A Reply” (1980) 58 Australian Journal of Philosophy 54.

Paul A Bernal “A Right to Delete?” (2011) 2(2) EJLT 1.

Danah Boyd “Autistic Social Software” (speech given at Supernova Conference, 24 June 2004) 35.

Petra Butler “The Case for a Right to Privacy in the New Zealand Bill of Rights Act” (2013) 11 NZJPIL 213.

Anne Cheung “Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd” (2009) 1 JML 191.

Vincent Blasi “The Checking Value in First Amendment Theory” (1977) Am B Found Res J 521.

Vincent Blasi “The First Amendment and the Ideal of Civic Courage: The Brandies Opinion in Whitney v California” (1988) 29 WM & Mary L Rev 653.

Edward J Bloustein “Privacy as an Aspect of Human Dignity” (1964) 39 NYU L Rev 962.

Edward J Bloustein “Privacy is Dear at Any Price: A response to Professor Posner’s Economic Theory” (1978) 12 Ga L Rev Georgia Law Review 429.

John Burrows “Invasion of Privacy – *Hosking* and Beyond” [2006] NZ Law Review 389.

Des Butler “A Tort of Invasion of Privacy in Australia” (2005) 29 MULR 339.

Lee A Bygrave “A Right to be Forgotten” (2015) 58 Communications of the ACM 35.

Edward L Carter “Argentina’s Right to Be Forgotten” (2013) 27 Emory Int’l L Rev 23.

Ursula Cheer “The Future of Privacy: Recent Legal Developments in New Zealand” (2007) 13 Canterbury L Rev 169.

Natalie Coates “The Recognition of Tikanga in the Common Law of New Zealand” (2015) NZ L Rev 1.

Julie E Cohen “Examined Lives: Informational Privacy and the Subject as Object” (2000) 52 Stan L Rev 1373.

Julie E Cohen “What Privacy is For” (2013) 126 Harv L Rev 1904.

Rahui De', Neena Pandey and Abhipsa Pal “Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice” (2020) 55 International journal of information management 102171 <https://doi.org/10.1016/j.ijinfomgt.2020.102171>.

Cécile de Terwangne “Internet Privacy and the Right to be Forgotten/Right to Oblivion” (2012) 13 IDP 109.

Judith Wagner DeCew “The Scope of Privacy in Law and Ethics” (1986) 5 L & Phil 145.

Thomas I Emerson “Toward a General Theory of the First Amendment” (1963) 72 Yale L J 877.

Cynthia L Estlund "Speech on Matters of Public Concern: The Perils of an Emerging First Amendment Category" (1990) 59 Geo Wash L Rev 1.

Patrick C File "A History of Practical Obscurity: Clarifying and Contemplating the Twentieth Century Roots of a Digital Age Concept of Privacy" (2017) 6 U Balt J Media L & Ethics 4.

Charles Fried "Privacy" (1968) 77 Yale L J 475.

Ruth Gavison "Privacy and the Limits of Law" 89 Yale L J 421.

Tom Gerety "Redefining Privacy" (1977) Harvard Civil Rights-Civil Liberties Law Review (12) 233.

Fraser Gollogly "The Blemish on the Clean Slate Act: Is There a Right to Be Forgotten in New Zealand?" (2019) 25 Auckland U L Rev 129.

Kent Greenawalt "Free Speech Justifications" (1989) 89 Colum L Rev 119.

James Grimmelmann "Saving Facebook" (2009) 94 Iowa L Rev 1137.

Rainer Grote "The ECHR's Rulings in *Von Hannover v Germany (No 2)* and *Axel Springer AG v Germany*: Rebalancing Freedom of the Press with the Respect for Privacy" 55 German Y B Int'l L 639.

Taryn Gudmanz "Harmful Digital Communications" (2019) 927 Law Talk 46.

Gehan Gunasekara "Making a Difference? The Privacy Act and Employment Relationship Problems in New Zealand" (2018) 28 NZULR 25.

Gehan Gunasekara and Alan Toy "Principles or Rules: The Place of Information Privacy Law" (2011) 24 NZULR 525.

Woodrow Hartzog "The Public Information Fallacy" (2019) 99 B U L Rev 459.

Martin Hilbert and Priscila López “The World's Technological Capacity to Store, Communicate, and Compute” (2011) 332 Science 60.

Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius “The European Union General Data Protection Regulation: What it is and What it Means” (2019) 28 Information & Communications Technology Law 65.

Kirsty Hughes “The Public Figure Doctrine and the Right to Privacy” (2019) 78 CLJ 70.

Chris D L Hunt “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort” (2011) 37 Queens LJ 167.

Chris D L Hunt ‘The Future of Privacy: The Conflict with Free Expression” (2015) 43 Advoc Q 391.

Chris D L Hunt and Nikta Shirazian “Canada’s Statutory Privacy Torts in Commonwealth Perspective” (2016) Oxford U Comparative L Forum 3 <ouclf.law.ox.ac.uk>.

Stanley Ingber “Rethinking Intangible Injuries: A Focus on Remedy” (1985) 73 Cal L Rev 772.

Kylie Jackson-Cox “A 21st Century Right? An Analysis of the Extent to which New Zealand’s Privacy Act 1993 Provides a Right to Be Forgotten” (2019) 28 NZULR 561.

John A Jurata Jr “The Tort that Refuses to Go Away: The Subtle Re-emergence of Public Disclosure of Private Facts” (1999) 36 San Diego L Rev 489.

Meredith Karlsen “Forget Me, Forget Me Not: A ‘Right to be Forgotten’ in New Zealand’s Information Society” [2016] NZ L Rev 507.

B Koops “Forgetting Footprints, Shunning Shadows. A Critical Analysis of the ‘Right to be Forgotten’ in the Big Data Practice” (2011) 8 SCRIPTed 229.

Aleksandra Kuczerawy and Jef Ausloos “From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain” (2016) 14 Colo Tech LJ 219.

Robert G Larson III “Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to be Forgotten are Incompatible with Free Speech” (2013) 18 Communication Law and Policy 91.

Joy Liddicoat “The Right to be Forgotten” (paper presented during Privacy Week to New Zealand Law Society, Continuing Legal Education, and IT & Online Law conferences, May 2015) Privacy Commission <www.privacy.org.nz>.

Jaime A Madell “The Poster's Plight: Bringing the Public Disclosure Tort Online” (2011) 66 N Y U Ann Surv Am L 895.

Andrew J McClurg “Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places” (1995) 73 N C L Rev 989.

Patrick J McNulty “The Public Disclosure of Private Facts: There is Life after Florida Star” (2001) 50 Drave L Rev 93.

David B Menkes and others “Perspectives on Access to Personal Health Information in New Zealand/Aotearoa” (2008) 15 Anthropology & Medicine 199.

Bryce Clayton Newell “Rethinking Reasonable Expectations of Privacy in Online Social Networks” (2011) 12 Rich J L & Tech 12.

Jonathan B Mintz “The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain” (1996) 55 Md L Rev 425.

N A Moreham “Abandoning the ‘High Offensiveness’ Privacy Test” (2018) 4 Canadian Journal of Comparative and Contemporary Law 161.

N Moreham “Privacy in the Common Law: A Doctrinal and Theoretical Analysis” (2005) 121 LQR 628.

Nicole Moreham “Privacy in Public Places” (2006) 65 CLJ 606.

N A Moreham “Unpacking the Reasonable Expectation of Privacy Test” (2018) 134 LQR 651.

Helen Nissenbaum “Privacy as Contextual Integrity” (2004) 79 Wash L Rev 119.

Helen Nissenbaum “Protecting Privacy in an Information Age: The Problem of Privacy in Public” (1998) (17) Law and Philosophy 559.

Stephanie Frances Panzic “Legislating for E- Manners: Deficiencies and Unintended Consequences of the Harmful Digital Communications Act” (2015) 21 Auckland U L Rev 225.

WA Parent “A New Definition of Privacy for the Law” (1983) 2 L & Phil 305.

Elizabeth Paton-Simpson “Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places” (2000) 50 ITLJ 305.

Elizabeth Paton-Simpson “Private Circles and Public Squares: Invasion of Privacy by Publication of Private Facts” (1998) 61 Mod L Rev 318.

Gavin Phillipson “Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act” (2003) 66 MLR 726.

Richard A Posner “The Right of Privacy” (1978) 12 Ga L Rev 393.

Robert C Post “The Social Foundation of Privacy: Community and Self in the Common Law Tort” (1989) 77 Cal L Rev 957.

Connie Davis Powell “You Already have Zero Privacy, Get Over It - Would Warren and Brandeis Argue for Privacy for Social Networking” (2011) 31 Pace L Rev 146.

J J Prescott and Sonja B Starr “Expungement of Criminal Convictions: An Empirical Study” (2020) 133 Harv L Rev 2460.

William Prosser “Privacy” (1960) 48 Cal L Rev 383.

James Rachels “Why Privacy is Important” (1975) 4 Philosophy & Public Affairs 323.

Viviane Reding “The European Data Protection Framework for the Twenty-First Century” (2012) 2 IDPL 119.

Elspeth Reid “Rebalancing Privacy and Freedom of Expression” (16) Edin L R 253.

Neil M Richards “The Limits of Tort Privacy” (2011) 9 J on Telecomm & High Tech L 357.

Neil M Richards “The Puzzle of Brandeis, Privacy, and Speech” (2010) 63 V and L Rev 1295.

Beate Roessler “Privacy as a Human Right” (2017) Proceedings of the Aristotelian Society, Vol CXVII, Part 2 187.

Jeffrey Rosen “The Right to Be Forgotten” (2012) 64 Stan L Rev 88.

Giovanni Sartor “The Right to be Forgotten: Balancing Interests in the Flux of Time” (2016) 24 IJLIT 72.

Lawrence Siry “Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to be Forgotten” (2014) 103 Ky L J 311.

Daniel J Solove “Conceptualizing Privacy” (2002) 90 CLR 1086.

Daniel J Solove “A Taxonomy of Privacy” (2006) 154 U Pa L 477.

Daniel J Solove “The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure” (2003) 53 Duke L J 967.

Lior Jacob Strahilevitz “A Social Networks Theory of Privacy” (2005) 72 U Chi L Rev 919.

Lior Jacob Strahilevitz “Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Reunifying Privacy Law” (2010) 98 Cal L Rev 2007.

Katherine Strandburg “Privacy, Rationality, and Temptation: A Theory of Willpower Norms” (2005) 57 Rutgers L Rev 1235.

Judith Jarvis Thomson “The Right to Privacy” (1975) 4 Philosophy and Public Affairs 295.

Hugh Tomlinson and Aidan Wills “*ML and WW v Germany*—Article 8 Right to be Forgotten and the Media” Entertainment Law Review (2018) Ent LR 235.

Alan Toy “Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity” (2010) 24 NZULR 222.

Alan Toy “Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy” (2013) 23 NZULR 938.

Alan Toy “Privacy Audits: Expectations and Implementation” (PhD Thesis, University of Auckland, 2016).

Edward Tverdek “What Makes Information “Public”?” (2008) 22 Public Affairs Quarterly 63.

Selen Uncular “The Right to Removal in the Time of Post-Google Spain: Myth or Reality under General Data Protection Regulation?” (2019) 33 IRLCT 309.

Eugene Volokh “Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You” (2000) 52 Stan L Rev 1049.

W Gregory Voss and Céline Castets-Renard “Proposal for an International Taxonomy on the Various Forms of the ‘Right to Be Forgotten’: A Study on the Convergence of Norms” (2016) 14 Colo Tech L J 281.

Raymond Wacks “Poverty of Privacy” (1980) 96 LQR 73.

Samuel D Warren and Louis D Brandeis “Right to Privacy” (1890) Harv L Rev 193.

Rolf H Weber “The Right to be Forgotten: More than a Pandora’s Box” 2 (2011) JIPITEC 120.

Christian Whata "Biculturalism in the Law: The 'I', the 'Kua' and the 'Ka'" (2018) 26 Waikato L Rev 24.

James Q Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) 113 Yale LJ 1151.

Joseph Williams "Lex Aotearoa: An Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law (2013) 21 Waikato L Rev 1.

Paul Wragg "The Benefits of Privacy-Invading Expression" (2013) 64 N Ir Legal Q 187.

Diane L Zimmerman "Requiem for a Heavyweight: A Farewell to Warren and Brandeis' Privacy Tort" 68 Cornell L Rev 291.

F Parliamentary and Government Materials

1 New Zealand

Google New Zealand "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013".

He Taonga Te Matauranga: A Draft Discussion Document–Māori Issues Concerning the Code of Practice for Health Information (Te Puni Kōkiri, May 1993).

Law Commission *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (NZLC MB3, 2012).

Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, March 2009).

Law Commission *Māori Custom and Values in New Zealand Law* (NZLC SP9, 2001).

Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008).

Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2008).

Law Commission *Review of the Privacy Act 1993* (NZLC R123, June 2011).

Ministry of Justice *Departmental Report on the Privacy Bill – Part One* (March 2019).

Ministry of Justice *Departmental Report on the Privacy Bill – Part Two* (March 2019).

Geoffrey W R Palmer and Ministry of Justice *A Bill of Rights for New Zealand: A White Paper* (AJHR, Wellington, 1985).

Privacy Commissioner *Necessary and Desirable – Privacy Act 1993 Review* (November 1998).

Privacy Commissioner "Privacy Commissioner's Submission on the Privacy Bill to the Justice Committee 2018".

Privacy Foundation "Submission to the Justice Committee on the Privacy Bill 2018".

Paul Roth "Submission to the Justice Select Committee on the Privacy Bill 2018".

Alan Toy "Submission to the Justice Committee on the Privacy Bill 2018".

2 Australia

Australia Law Reform Commission *For Your Information: Privacy Law and Practice* (ALRC Report 108, 2008).

Australia Law Reform Commission *Serious Invasions of Privacy in the Digital Age* (ALRC Final Report 123, 2014).

New South Wales Law Reform Commission *Invasion of Privacy* (NSWLRC R120, 2009).

New South Wales Parliament Legislative Council Standing Committee on Law and Justice *Remedies for the Serious Invasion of Privacy in New South Wales* (R57, 2016).

Victorian Law Reform Commission *Surveillance in Public Places* (VLRC R18, 2010).

3 Canada

Office of the Privacy Commissioner of Canada *Draft OPC Position on Online Reputation* (26 January 2018).

4 England

House of Lords European Union Committee *EU Data Protection Law: A 'Right to Be Forgotten'?* (2nd Report of Session 2014–15, HL 40, 30 July 2014).

5 Europe

Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/12* (European Commission, 14/EN WP 225, 26 November 2014).

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* (COM (2010) 609, 4 November 2010).

European Commission (2011) *Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union.*

European Commission *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) (COM/2012/011, 25 January 2012).

European Data Protection Supervisor *Annex to Opinion 3/2015: Comparative Table of GDPR Texts with EDPS Recommendations* (9 October 2015).

G Dissertations

Nin Tomas "Key Concepts of Tikanga Māori (Māori Custom Law) and Their Use as Regulators of Human Relationships to Natural Resources in Tai Tokerau, Past and Present" (PhD thesis, University of Auckland, 2006).

Alan Toy "Privacy Audits: Expectations and Implementation" (PhD Thesis, University of Auckland, 2016).

H Other resources

Antonio Diaz Andrade and others *World Internet Project: The Internet in New Zealand 2017* (New Zealand Work Research Institute, Auckland, 2018).

"ARANZ Code of Ethics" (25 August 2006) ARANZ <https://www.aranz.org.nz>.

Broadcasting Standards Authority *Broadcasting Standards in New Zealand Codebook for Radio, Free-to-Air Television* (2016).

Google's Privacy Policy.

Google Transparency Report (last accessed 4 May 2022).

Artemi Rallo Lombarte "The Origins and Importance of the Right to be Forgotten: The Spanish Experience" (presentation at the University of Oxford, Centre for Socio-Legal Studies, 2012) <http://slideplayer.com/slide/6276508/>.

Mary Madden and Lee Rainie Pew Research Centre (2015) *Americans' Attitudes About Privacy, Security and Surveillance.*

NZ Media Council "Principles" <www.mediacouncil.org.nz>.

Dr Nicole Moreham "Private Matters: A Review of the Privacy Decisions of the Broadcasting Standards Authority" December 2009.

Netsafe "Revealed: Who sends harmful digital communications – and why" (press release, 9 February 2021).

OECD "Privacy Framework" (2013).

Opinion of Advocate General Jääskinen in Case C-131/12 *Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and M C Gonzales* ECLI:EU:C:2013:424.

Pew Research Centre (2014) *Public Perceptions of Privacy and Security in the Post-Snowden Era.*

Russell McVeagh "InfoRM Privacy Update" (15 March 2018, Russell McVeagh <www.russellmcveagh.com>.

Software Advice (2014) *US Attitudes Toward the 'Right to Be Forgotten' Industry View Survey.*

Olivia Solon and Emma Graham-Harrison "The six weeks that brought Cambridge Analytica down" The Guardian (online ed, London, 3 May 2018).

Te Mana Raraunga – the Māori Data Sovereignty Network *Purpose* (17 November 2020) <https://www.temanararaunga.maori.nz>.

Hugh Tomlinson QC "Case Law, Belgium: *Olivier G v Le Soir*. 'Right to be forgotten' requires anonymisation of online newspaper archive" (19 July 2016) Inforrm Blog <https://inforrm.org>.

Hugh Tomlinson QC and Aidan Wills "Case Law, Strasbourg: *Hurbain v Belgium*, Order to anonymise newspaper archive did not violate Article 10" (7 July 2021) Inforrm Blog <https://inforrm.org>.

Mario Trujillo "Public wants 'Right to Be Forgotten' Online" (19 March 2015) The Hill <https://thehill.com>.

"A Guide to the Principles of the Treaty of Waitangi as Expressed by the Courts & the Waitangi Tribunal" Waitangi Tribunal < https://waitangitribunal.govt.nz>.

"Signing of the Treaty" (19 September 2016) Waitangi Tribunal <https://waitangitribunal.govt.nz>.

Helen Winkelmann, Chief Justice of New Zealand "Sir Bruce Slane Memorial Lecture" (Auckland, November 2018).

YouGov (2014) *Right to be Forgotten Omnibus Survey*.