

**Trial and Error: Does the public's right to know really mean the
new media's right to reveal?**

Brenda J.P. Kiernan

MCS

June 2012

**Trial and Error: Does the public's right to know really
mean the new media's right to reveal?**

**An investigation into new media and privacy issues in New
Zealand and overseas.**

Brenda J.P. Kiernan

**A thesis submitted to Auckland University of Technology
in partial fulfilment of the requirements for the degree of**

MASTER OF COMMUNICATIONS (MCS)

June 2012

ATTESTATION OF AUTHORSHIP

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the qualification of any degree or diploma of a university or other institution of higher learning.

ACKNOWLEDGEMENTS

Associate Professor Martin Hirst for the humorous and lively discussions shared.

Margaret Linzell-Jones for proofreading.

John Butler, Anna Nelson, Savita Bhaskaran, Kyle Macfadyen and John Lambert for their on-going support, sharing their computer skills and always their humour.

David Smaill, Helen Pritchard, Chris and Leanne Houston, Michael Kiernan, Seamus Kiernan, Trevor Salmon, Bernard and Fiona Scott, Sherilyn Bury, George Giorgobiani and Devlin and Flinn Medemblik: without whom....

ABSTRACT

The growth of digital technologies over the last thirty years has meant that now, more than ever, the ways we access and communicate information has important ramifications when balancing the right of privacy with the public right to know. Increasingly the sophistication of these new technologies has meant that our legal capability to deal with privacy infringement is found wanting and laws that were created in the pre-digital era are lagging behind in an age where information has become a commodity and the world, literally, a paying customer. This study found New Zealand, as in other comparable countries, is beginning to address concerns around privacy issues that new media has exposed and also highlights the need for individual awareness of what control they have over their information once posted online. Harms this study identified from the misuse of personal information ranged from identity theft through to intrusive surveillance and, possible threats to our civil liberties in the name of “national security”. A possible solution to privacy tensions caused when new media and the public’s right to know collide is that proposed by Professor Nissenbaum of New York University, and that is the contextual integrity framework. This framework highlights the need for constraints to be imposed on flows of information in the context of how this information is collected. Information revealed in a particular context always bears the tag of that context and if this information is subsequently used for a purpose other than what it was intended then contextual integrity has been breached. This study recommends collaboration between digital developers and programmers in developing a formal expression of contextual integrity and an adoption of this framework by all institutions involved in the collection, sharing and dissemination of information.

TABLE OF CONTENTS

CHAPTER 1: PRIVACY IN PUBLIC

1.1	Aim	1
1.2	Methodology	1
1.3	Digital Privacy Context	2
1.4	Issues	4
1.4.1	Identity theft	5
1.4.2	Misuse	5
1.4.3	Legal response	7
1.4.4	Traditional media	8
1.5	Environment	9
1.6	Summary	12

CHAPTER 2: LITERATURE REVIEW

2.1	Introduction	13
2.2	Privacy	13
2.3	Informational privacy	14
2.4	New Zealand context	16
2.5	New Zealand Privacy Act 1993	18
2.6	Suppression	19
2.7	Trial by media	22
2.8	Ethics	24

2.9	Summary	28
-----	---------	----

CHAPTER 3: LEGAL FRAMEWORK

3.1	Introduction	30
3.2	Background	30
3.3	Information privacy	31
3.4	Privacy Act 1993	34
3.5	Digital privacy issues: Identity theft	35
3.5.1	Social media	36
3.5.2	Surveillance	39
3.6	Broadcasting Standards Authority	41
3.7	Press Council	43
3.8	Summary	46

CHAPTER 4: PRIVACY COMMISSIONER

4.1	Introduction	47
4.2	Background	47
4.3	Annual Report	48
4.4	Privacy Commission on Law Commission's Review of Privacy Act	49
4.4.1	Identity crime	52
4.5	New tools for Privacy Commissioner	54

4.6	Summary	55
-----	---------	----

CHAPTER 5: LAW COMMISSION

5.1	Introduction	57
5.2	Review of the New Zealand Privacy Act 1993	57
5.3	Stage 1: Privacy concepts and Issues	59
5.4	Stage 3: Invasion of privacy	61
5.5	Stage 4: Review of the Privacy Act	64
5.5.1	Publication of personal information	65
5.5.2	Identity theft	66
5.6	Summary	66

CHAPTER 6: NAME SUPPRESSION

6.1	Introduction	68
6.2	Issues Paper 13: Suppressing names and evidence	68
6.3	Report 109: Suppressing names and evidence	72
6.4	Media and suppression	74
6.5	Summary	79

CHAPTER 7: SOCIAL MEDIA

7.1	Introduction	80
7.2	Social media sites	80
7.3	Privacy on Facebook	83
7.4	Tracking	86
7.5	Misuse of social media	88
7.6	News media meets 'new media'	92
7.7	Part 2: Speech harms	93
7.8	Summary	95

CHAPTER 8: SURVEILLANCE

8.1	Introduction	97
8.2	Surveillance and privacy	97
8.3	Invasion of privacy: Penalties and remedies	98
8.4	Misuse of surveillance	101
8.5	Search and Surveillance Bill	105
8.5.1	Search and Surveillance law	109
8.6	Summary	109

CHAPTER 9: CONCLUSION

9.1	Public versus private	113
9.2	New media's right to reveal	115
9.3	Contextual integrity	116
9.4	Recommendations	118
9.5	The future	118

BIBLIOGRAPHY	120
---------------------	------------

LIST OF FIGURES

Figure 3.1	Top U.S media sites: December 2009	37
Figure 3.2	Use a social network site	38
Figure 5.1	The most common forms of E-Crime 2005/6 experienced in New Zealand	61
Figure 7.1	Weekly market share of visits to Facebook and Google	81
Figure 7.2	Twitter growth 2008-2009	82
Figure 7.3	Video views for YouTube vs. its competitors	83
Figure 7.4	Number of Facebook users in millions	84

LIST OF ABBREVIATIONS	x
------------------------------	----------

IST OF ABBREVIATIONS

BSA	Broadcasting Standards Authority
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
ISP	Internet Service Provider
NBR	National Business Review
OPC	Office of the Privacy Commissioner
NZLC	New Zealand Law Commission
PC	Press Council

Chapter 1

INTRODUCTION: PRIVACY IN PUBLIC

1.1 Aim

With the explosive growth of new media technologies, privacy has increasingly become a relative notion. Exactly what does remain private in this digital age of tell all angst, what safeguards are there from new media intrusion and data matching? Or are we to accept the notion that we have “zero privacy anyway” and “Get over it” (Sprenger, 1999)? This thesis aims to examine digital privacy issues; review New Zealand’s legal responses to these issues; discuss contemporary use and misuse of social networking forums by the news media and others, and determine whether anyone really is guarding the guardians.

1.2 Methodology

This study investigated, reviewed and discussed various reports that have raised concerns around informational privacy issues in the digital era. In the course of this investigation I have also analysed and examined proposed recommendations about law changes in New Zealand, in the context of how rapid technological development has created privacy tensions.

The framework for this thesis is built around the twin themes of the techno-legal time gap and ethico-legal paradoxes that arise from digital privacy issues. Definitions of both terms

will be the ones used by Hirst and Patching (2005, p.283, p.266). The techno-legal time gap refers to the time it takes for legislation to regulate the socially undesirable aspects of new media technologies and the ethico-legal paradox refers to the confusion that arises when action is morally right but legally wrong, or vice versa.

1.3 Digital Privacy Context

For the purposes of this thesis, I have used digital privacy to mean privacy of personal information once it is placed online through Internet based technologies. Privacy issues raised by such technologies that I have identified as being problematic revolve around: indefinite storage of information; aggregation and use thereof; identity theft; government intrusion; flouting of suppression laws and traditional media usage of social networking sites. In particular, I intend to explore the implications of: commercial and illegal use of our digital footprint; private versus public domain; possible threats to our existing civil liberties and the legal and ethical problems arising from the use and abuse of personal information.

Recent English controversy over the 'outing' on Twitter of the name of an English soccer player, who was granted blanket suppression by court injunction, over an alleged affair, is an example of the former theme, and the arrest of an Australian journalist and subsequent seizure of his iPad by the police, is an example of the latter.

English privacy laws are such that they have what is known as a 'super' injunction which prevents English media from reporting, not only about a case where the name of the person who has sought the suppression order and details about the case are suppressed, but also the media's ability to say the court has even given this injunction. However, in this particular case, the identity of the English soccer player was soon revealed through the social messaging site Twitter and Scottish newspaper *Sunday Herald* – neither of which are liable under the super injunction as both sites are located outside the jurisdiction in which the injunction would apply. The *Sunday Herald* justified the decision to run the story by citing, in as many words, the techno-legal time gap:

Today we identify the footballer whose name has been linked to a court super injunction by thousands of postings on Twitter. Why? Because we believe it is unsustainable that the law can be used to prevent newspapers from publishing information that readers can access on the internet at the click of a mouse (Davis, 2011).

The ethico-legal dilemma was neatly illustrated at a 2011 security conference in Queensland Australia, whereby Fairfax deputy technology editor Ben Grubb wrote about security expert Christian Heinrich's slide show demonstration of vulnerabilities on social websites such as Facebook. As part of the demonstration, Heinrich revealed how he had been able to access the Facebook photos of a rival security expert's wife, without using a username or password. Hours after this story was published on Fairfax's news sites, Grubb was interviewed by Queensland police and, as a consequence, his iPad was seized and he was arrested in relation to receiving unlawfully obtained property (Grubb, 2011, May 19).

While it was legal for Heinrich to use these photos as a demonstration of the weakness of privacy settings on social media sites, without any semblance of obtaining permission, was it ethical? Heinrich believed so, using the justification of the photos being in a public sphere. Also while it was legal for the police to seize Grubb's iPad, was it ethical to make a complete copy of *all* the information Grubb had on it, whether it related to the matter or not?

1.4 Issues

Conventional issues around personal privacy are turned on their head in the digital era; every time anyone interacts in the digital environment a trail is left, and this trail or "digital footprint" (phrase attributed to Nicholas Negroponte in his 1996 book *Being Digital*) is stored indefinitely. The implications for individual information security are many and complex.

An example of how a digital trail can be used is that offered by the website 'Spokeo'. The online site advertises an ability to aggregate data from online and offline sources (for example phone directories, social networks, marketing surveys, real estate listings, business websites) to deliver the "most comprehensive snapshot of people related data". Spokeo states that it can locate virtually anyone in the world so long as they have a social network account (About Spokeo, 2011). The potential threat to privacy from such sites is that linkages are made, accurate or otherwise, to individuals' personal information and the uses that this information is put to (Heuston, 2011.)

1.4.1 Identity Theft

One possible and very real threat from misuse of digital personal information is that of identity theft. While identity theft is not a new phenomenon per se, the New Zealand Law Commission's *Review of the Privacy Act (2010)* does say that the development of technology, particularly the Internet, had made identity theft more prevalent and that techniques are evolving and transforming into new types of threats very rapidly (New Zealand Law Commission Issues Paper 17 [NZLC IP17], p. 445). Offenders are increasingly using social networking sites to gather details about victims which they then use, for example, to hack into bank accounts. The Commission members believe that identity crime harms a victim's privacy and sense of individuality (NZLC IP17, 2010 p. 448).

Credit check agency Veda's (Australia and New Zealand) latest figures reveal that identity fraud has risen by 50 per cent in the last two years and Managing Director, John Pearson, said that identity crime is not just something that happens overseas. The Department of Internal Affairs translates these figures to estimate "as many as 133,000 New Zealanders may be victims, costing the economy more than \$200 million annually" (Greig, 2012).

1.4.2 Misuse

Google chief executive Eric Schmidt warned in August 2010 that he believed young people were posting too much personal data on the Internet and that they may be forced at some point in their future to change their names to escape their digital past (Taylor,

2010.) The New Zealand Office of the Privacy Commissioner's comments on a recent UMR Research survey indicated that 88 per cent of New Zealanders were most concerned about information children put on the Internet about themselves and 83 per cent were concerned about the security of personal information on the Internet. The survey also found that more than half of users (57 per cent) of social networking sites believed they were mainly private spaces. At the time, Privacy Commissioner Marie Shroff commented:

"That's a high number of people who think they're more private on their social networking sites than they actually may be. So they're likely to put information up there not realizing that they could be sharing it with the whole world – that's risky for them." (Privacy Commission Media Release, 2010)

An example of deliberate malicious sharing of personal information happened on July 23rd 2010 when New Zealander Joshua Smith posted online a naked picture of his ex-girlfriend for millions of Facebook users to see and hacked her account so she could not remove the image. After 12 hours, police and Facebook authorities shut down the woman's account but not before it was available to approximately 500 million plus users of the social network. On November 12th 2010, New Zealand judge Andrew Becroft made legal history when he jailed Joshua Simon for four months for posting the image on Facebook. In a neat twist on the techno-legal time gap, Judge Becroft said he was adapting an old print law for the Internet age and that "Technology can't be used in this way. You would do incalculable damage to someone's reputation" ("Naked lover...", 2010).

However, adapting an old print law for the Internet age does not 'cut it' in this digital era where technologies are outstripping our legal ability to protect our personal information. While the author's intent is not to promote paranoia of the 'Big Brother' kind, it is to draw attention to the fact of the techno-legal time gap dilemma and question what protection we have over what is accessible about us. For example, in chapter 8 on Social media the case of the 'Facebook Predator' serves to illustrate the damage that is done when 'stolen' information is used to create a fake Internet profile.

1.4.3 Legal Response

In 2006, the New Zealand Law Commission was entrusted with a review of New Zealand's privacy law and, as part of this review, the Law Commission identified two key motivators for the growth of surveillance technology: commercial advantages in developing and applying technology to gather personal information, and security imperatives to combat crime and the threat of terrorism (NZLC SP19, 2008). Further, the Law Commission noted that surveillance was not well regulated by current law and that technology is rapidly developing to create new ways of invading privacy (NZLC R113, 2010).

In 2012, the New Zealand Search and Surveillance Bill was passed into law. Privacy watchdogs suggest this law will increase government intrusion into citizens' lives, in that it grants sweeping powers to government agencies such as Police, Customs or Internal Affairs to bug and secretly film inside suspects' homes. The introduction of the "production order" can also force individuals and media to turn over documents and

reveal confidential sources (Cheng, 2010). Chapter 8 on Surveillance will explore this debate in more detail.

1.4.4 Traditional Media

A particularly problematic issue of digital privacy is the use by traditional media of information found on the Internet. On page 23 of the New Zealand Law Commission's Study Paper 19 (2008) on *Privacy concepts and issues*, it states that complaints about breaches of privacy in the news media are made to the New Zealand Press Council and that there is no body charged with accountability for maintaining privacy standards on the Internet. The Law Commission report notes that content is published on the Internet without legal advice or editorial control in many instances, and that there are a number of other issues in this area, such as how much privacy can there be in a public place. This issue of privacy in public was most recently brought again to the attention of the New Zealand Press Council (NZPC) in February 2011 with the Case 2173 of Aparangi Hemara against *The Herald on Sunday*, over the paper's use of his wedding photo, sourced from Mr Hemara's mother's Facebook page.

Mr Hemara objected to the use of his wedding photo attached to an article in *The Herald on Sunday* (2010, November 28) regarding a violent attack he, and his subsequent wife, suffered whilst living in Scotland. Mr Hemara said permission was not granted for the newspaper to use their wedding photograph and that the word "Supplied" with the photo was misleading (NZPC No. 2173 p. 2). The Press Council did not uphold Mr Hemara's

complaint, in part because its' members said that Facebook is not a private space but a public sphere.

In Case 2166 (Gen O'Halloran against *The New Zealand Herald*) December 2010, the Press Council stated that the Internet is a public place and publication of a photograph on an open page therefore indicates to the news media that there is an implied use for news purposes. In the ruling on Mr Hemara's case, the Press Council reiterated this stance and also reminded users of social media sites, despite the best intentions of individuals, that it is not easy, not always possible to protect privacy, or enforce copyright issues, which illustrates another example of both the techno-legal time gap and the ethico-legal dilemma (NZPC No.2173 p. 2).

1.5 Environment

As briefly outlined, the advent of new media technologies is challenging our notions of privacy and revealing the insufficiency of legal frameworks to protect us in our globally connected world. Privacy is a relative notion, and the New Zealand Law Commission (NZLC) Study Paper 19 on *Privacy concepts and issues* (2008) examines the history of privacy to understand that its' meaning is not fixed, but changes over time. The NZLC goes on to say that it is helpful to understand that the level of privacy we have come to expect has probably only existed for a few generations at most (p. 99-100).

The former United Kingdom's Chief Information Commissioner, Richard Thomas, warned in 2004 that Britain risks "sleepwalking into a surveillance society" because of the Government's plans for identity cards and a population register ("Beware rise of Big Brother...", 2004). However, on the other side of the privacy issue is the balance that needs to be maintained with regard to the public's right to know, which should not be confused with the public's desire to know; in other words, legitimate public interest versus public curiosity. Case number 2048 Graeme Hart against the *Herald on Sunday* (2008) as judged by members of the New Zealand Press Council serves to illustrate this very point.

Mr and Mrs. Hart (Mr Hart is considered to be New Zealand's wealthiest individual) took exception to the Herald's publication of proposed renovations to their mansion, in particular aerial photographs of the property with accompanying text boxes, including an arrow indicating the location of a new bedroom for grandchildren. The ten members of the Council (one was absent) were equally divided between those upholding the complaint and those that were not, and highlights the difficulty in drawing the line in maintaining the right to privacy and the public's right to know. The reason for not upholding the complaint was twofold: everything published was publicly available (albeit through special effort and a fee payment to the local council) and the Press Council is:

"charged with promoting freedom of expression and, in our opinion, it should be slow to give ground to privacy or any other development that would inevitably see freedom of expression diminished; it certainly should not be the vanguard of change." (New Zealand Press Council Case Number 2048, p. 3)

In May 2008 media law academic, Steven Price, stated on his Law Journal blog his thoughts on the NZLC's *Privacy concepts and issues* (2008) Study Paper 19 and he made the comment that too often New Zealand tends to muddle through with jury rigged solutions to particular problems so that our law develops without any coherency (Price, 2008). Professor of Communication and Senior Faculty Fellow of Information Law at New York University, Helen Nissenbaun, believes that privacy needs to be considered in particular contexts, and that the public-private distinction is a dead-end for conceptualising a right to privacy and formulating policy. In her view, far too much time is spent on deciding whether information or place is either private or public, rather what people care about is what constraints ought to be imposed on flows of this or that information in this or that place (Citron, p. 2).

It appears that concerns over privacy have been closely linked with the changes in technology and these concerns are largely reflected in the fore mentioned issues regarding what types of information and places are considered private and under what conditions it is permissible to invade privacy. The idea of privacy needs to be rethought in the 21st century and a possible solution may be that of the one put forward in Professor Helen Nissenbaun's book *Privacy in Context* (2009) and that is, the notion of 'contextual integrity'.

Visiting scholar at Stanford University, Evgeny Morozov, states in his article (2010) that he believes the idea of contextual integrity to be brilliant. He summarises Nissenbaum,

saying that information revealed in a particular context always bears the tag of that context and, as such, no information is context free so it is not 'open' for all takers, even if revealed in public spaces. When applying this framework to new media there is nothing wrong with digital memory as long as the information is only remembered in appropriate contexts (p. 2).

1.6 Summary

Technology has made it technically, economically and socially feasible to collect, use, re-use and share enormous amounts of personal information in a variety of contexts for a variety of reasons. The pervasiveness of new media technologies in our lives means that our notions of privacy are being constantly challenged and has profound implications in relation to our freedoms – how we are reactive and proactive in responding to these challenges is the basis of this thesis.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

As more of our information is digitised and made available online, tensions have arisen in balancing privacy with freedom of information and expression. This chapter highlights some of the weaknesses in privacy law that have become apparent with the advent of new technologies, and illustrates how new media, in its pursuit of “public interest” stories, appears to be moving away from the ethics of traditional media.

2.2 Privacy

New Zealand media law academic Steven Price, author of *Media Minefield* believes that infringement of privacy is the fastest developing area of media law (2007 p. 257). With the advent of the Internet, it is now possible for vast quantities of information and events to be collected and shared and this is one area where possible infringements on personal privacy may occur. As of 2012, the New Zealand Law Commission has completed an examination of this and other privacy issues that will necessitate changes to the New Zealand Privacy Act 1993.

Former president of the New Zealand Law Commission, Sir Geoffrey Palmer, believes that privacy law should offer greater protection given the threats posed by new technology and he adds: “Technology is developing rapidly and continually creating new ways of invading privacy” (“Watchdog wants...,” 2010). Palmer goes on to say

that the challenge lies in balancing protection against the cost of weakening freedom of information.

In general terms this balancing of privacy and the public's right to know often takes the form of defamation issues, name suppression violations, media intrusion into personal privacy and informational privacy breaches. New media has expanded the reach of journalism and presents "its practitioners with opportunities and dilemmas" (Leach, 2009).

2.3 Informational Privacy

One of the challenges we face over issues of privacy in the new media age is that of control over informational privacy, that is, for example, information about our buying habits, health and lifestyle, online sites visited – information that is gathered from government and business databases and credit card use, to name but a few sources.

According to Moor (2004), once our personal information is digitised and made available over a computer network, or via the Internet, it becomes what he calls "greased data" that can easily "slip across" cyberspace between network nodes. He argues that, as a result, "personal information may no longer be controlled" by those to whom it refers and it may well be accessed by those "who have no right to do so" (p. 252).

Virtually every transaction we make generates an information or data trail and, in the USA, the resulting dossier of information may be used, sold, published or correlated with other sources of data and it is completely legal, states Law Professor Jessica Litman (2000) in her paper on 'Information privacy/information property'. In Europe, however, it is illegal "to release personal data to a third party, or even to use it for a purpose unrelated to the reason for which it was collated" without the consent of the subject (p. 1286).

An example of lack of possible informational privacy is new media coverage of criminal trials where there is high public interest. Associate Professor at the University of Western Australia, Stepniak's comparative study of five common law jurisdictions (UK, USA, Canada, Australia and NZ) regarding electronic media access to courts revealed that "judicial attitude is the pivotal factor" as to determining whether such coverage is "in the interests of the administration of justice and not merely the media right" (2005, p. 8).

Internet based information regarding jury trials, accurate or otherwise, may be widely publicised. There is valid concern that Internet and web-based technologies might affect a fair trial and "that they overextend the right of public and press access" (Lederer & Hulse, 2008 p. 21). One such example of this occurred in England in 2011, when juror Joanne Fraill became the first person in the United Kingdom to be convicted of contempt of court for using the Internet, when she used Facebook to exchange messages with a defendant already acquitted in an ongoing drug trial. This interaction caused the multi million pound trial to collapse (one of a series of four trials

estimated to have cost six million pounds) and Fraill was jailed for eight months (Holden, 2011).

Closer to home, the trial and subsequent conviction of Clayton Weatherston for the murder of Sophie Elliott in 2009 caused a huge public debate, both on and off line, over his defence of provocation. During Weatherston's trial, the New Zealand Solicitor-General announced an investigation into websites and blogs that were commenting in such a way as to raise concerns that they breached contempt of court laws. One such Facebook page with the title "Clayton Weatherston is a Murderer" was published during the trial and purportedly contained damning comments on Weatherston's guilt (Legal challenges..., 2009). Media law academic Steven Price commented on his media law journal website that:

There is some research to suggest that juries want to be seen to be making decisions that are consistent with community attitudes. If there's a volley of views, strongly biased one way, on well-read websites, that starts to come close to the sort of real risk that the law of contempt is supposed to guard against (Price, 2009, July 12).

2.4 New Zealand Context

Information Privacy Principle 3 of the New Zealand Privacy Act 1993 specifically sets out "how a website goes about collecting information from someone" (Chung & Paynter, p. 4). In their study of privacy issues on the Internet in New Zealand, Chung and Paynter (2002) look at New Zealand based web sites and their use of privacy statements in relation to information gathering. Chung and Paynter believe that, in

order for New Zealanders to have confidence when engaging in business activities on the Internet, consumers must be made aware of the fact, purpose and recipient of information collection, contact details of the company(ies) collecting and holding the information and subjects' rights of access to, and correction of, personal information. Of the 140 New Zealand websites Chung and Paynter studied, they found that 66 per cent collected some sort of personal data from consumers and of that 66 per cent all but 19 per cent provided notice of purpose of information collection (p. 5).

The principles of information privacy are relevant to this study because, as Chung and Paynter have pointed out, personal information collection does exist in New Zealand and it may be possible to access information that potential victims believe to be held on secure sites. The growth of such social media sites as Facebook, Twitter and Bebo have illustrated this point where "private material can swiftly, and irretrievably, become too public" (Dudding, 2010). While the Privacy Act prevents "government departments or businesses from disclosing information about individuals without first considering their right to privacy" (Dudding, 2010), it does not prevent individuals from collecting personal information for their own "personal, family or household affairs" (Section 56, New Zealand Privacy Act, 1993).

In 2011, British advertising company WPP claimed it has created the world's largest database of individuals' Internet behaviour and says it is capable of 'tracking' most of the British population. WPP says it is gathering data in order to enable advertisers to improve the targeting of their adverts online, and that they have built individual

profiles of over 500 million global Internet users. Currently, Europe and the United States is looking at ways to either ban secret tracking of web users or, alternatively, to ensure that there are easier ways to 'opt out' of websites retaining personal information (Foley, 2011).

2.5 New Zealand Privacy Act 1993

In New Zealand, the Privacy Act of 1993 sets out 12 privacy principles which "operate as guidelines for agencies that collect, store and use personal information about identifiable individuals" (Burrows & Cheer, 2005, p. 272). Key provisions of the Act regulate ways in which this personal information may be obtained and requires that it is securely held when it is obtained. The Act restricts the uses to which this information is put and provides the subject with the right of access to it.

In essence, the Privacy Act "is mainly about data management" and "does not apply to the media in its news gathering activities" (Price, 2007, p. 263). This creates the potential for news organisations covering legal proceedings (subject to laws of suppression, contempt and defamation) to invade privacy of litigants in pursuit of 'public interest' stories.

In New Zealand, two regulatory bodies have the responsibility of dealing with complaints arising from possible privacy breaches from traditional and new media sources and these are the Broadcasting Standards Authority (BSA) and the Press Council (PC). The BSA is government funded and appointed and ultimately responsible

to the Minister of Broadcasting, however the PC (which considers complaints against the print media, including their websites) is a self regulating and voluntary body that has no legislative backing with “no legally enforceable punitive powers” (Burrows & Cheer, 2005, p. 620). Both the BSA and PC are guided by principles that are designed to protect “privacy of person, space and personal information” (Principle 3 of The Privacy Act 1993). Price asserts in his book *Media Minefield* that the most common violation of privacy is the publication of private facts; the rule of thumb being whether this disclosure is highly offensive to the reasonable person in the shoes of the plaintiff.

2.6 Suppression

The granting of name suppression has often been criticised by the public as being made more readily available to those that have attained prominence or a level of celebrity in society. Against this background are the legal challenges posed by the Internet in publishing material that is under suppression orders and the question, just how adaptable is our law in dealing with these challenges?

Grounds for suppression of evidence and the consequential right to prohibit publication are granted to New Zealand courts through the Criminal Justice Act 1985. Section 138(2) of the Act states that there are five grounds on which a court may make an order forbidding publication: justice; public morality; the reputation of any victim of any alleged sexual offence; the reputation of any victim of any alleged extortion; or the security or defence of New Zealand (New Zealand Law Commission Report 109 [NZLC R109], p. 10).

Sections 140 and 140(1) give the courts the power to suppress publication of the names or particulars of the victim and the accused respectively (NZLC R109, p.10 & 17). Name suppression is automatic if: the witness is a minor; the subject is a victim of sexual assault; the person is accused or convicted of incest; a compulsory blood test is sought; a person works for the Secret Intelligence Service or, in some cases, if the witness is an undercover police officer (Burrows, 2006, p. 17). Section 138 of the Criminal Justice Act 1985 sets out the grounds on which name suppression is justified: in the interests of a fair trial; extreme hardship to the victims and the accused or to people connected with the accused and risk of suspicion being cast on others (NZLC R109, p. 22 & 23).

The NZLC R109 (2009) noted the strongest area of concern regarding suppressing names or identifying particulars of accused or convicted persons are over that of “names of prominent people”; that these people “are perceived to be treated differently or in some favoured light” (p. 17). Because of this concern, the former President of the Law Commission, Sir Geoffrey Palmer, stated that “The grounds on which suppression may be granted need to be clarified and tightened – they should be transparent, explicit and consistently applied” (Mitchell, 2009).

Burrows and Cheer (2005) state that the advent of the Internet has had considerable impact on suppression orders and the NZLC R109 (2009) discusses at length the challenges the Internet poses to a person’s right to a fair trial. “The law, it would be

fair to say, is having some difficulty keeping up with this new technology” (p. 339). Hirst and Patching (2007) describe this as the “techno-legal time gap” - “the gap between the time it takes for legislation to regulate the socially undesirable aspects of that technology” (p.283).

Among areas of concern noted by the NZLC R109 (2009) were those of information being continuously available on the Internet and of this information being “fresh”, in the sense of this information being regularly updated from legitimate, or otherwise, sources, and of information being easily passed to numerous websites. In criminal investigations “in particular, the information will be of a developing nature based upon reports as investigation progresses” (p. 63). The evidence presented in court gives the jury “the final picture” and comment on the developing nature of this evidence, via the Internet, may “colour” jury perspective, in that the coverage may be inaccurate, emotive and sensationalised (p. 63).

New Zealand law is “unclear” regarding information service providers (ISPs) passing on information (Burrows & Cheer, 2005, p. 47). In relation to name suppression, the Law Commission (2009) recommends that where ISPs (Internet Service Providers) or content hosts become aware “that they are carrying or hosting an offending publication to take steps within their means to prevent the material from being further published.” The Law Commission noted it was “impractical” for ISPs to prevent further publication by others (NZLC R109, p. 66).

While ISPs may argue they are “mere conduits” (Burrows & Cheer, 2005, p. 47) and part of their business is to pass on information, the Law Commission believes that websites carrying or hosting information in breach of a suppression order could potentially be held in contempt of court and that it “should be an offence for them to fail to remove the information or to fail to block access to it...” (NZLC R109, p. 66).

2.7 Trial by media

The issue of “trial by media” – “the media taking on the roles of judge, jury and executioner” as defined by Hirst & Patching (2007, p. 198) - through social media facilities such as ‘blogging’, newsgroups and bulletin boards via the Internet is also grounds for concern over possible breaches of suppression orders. Burrows and Cheer (2005) state that, in New Zealand, “the fact that the defamation appeared in ‘cyberspace’ makes no difference to the application of defamation law” (p. 46).

However, New Zealand media law academic Steven Price’s blog on his website states that he believes that trial by media is exactly what the media is for, not to say we should not criticise inaccurate or unbalanced reporting. Price points out that sometimes criminal charges are laid because of investigative journalism and that investigation and exposure of wrongdoing is not the exclusive province of the police and the criminal justice system. Media is subject to the law of contempt and defamation and media silence does not take into account public interest in free communication of information and opinion (Price, 2009, October 21).

The phone hacking by journalists of the now defunct *News of the World* is an example in hand of investigative journalism that led to criminal charges being laid. *Guardian* reporter Nick Davies first reported evidence of phone hacking by *News of the World* reporters in 2009 but the British Metropolitan Police chose not to re launch an inquiry (a previous investigation in 2006 by the police had resulted in two convictions of illegal phone hacking), however in July 2011 Davies broke the story that journalists from the *News of the World* had hacked the phone of a 13 year old murder victim while police were still searching for her. The resultant public furore lead to the papers' closure on the 10th July 2011 and to the arrest of ex editor of *News of the World* Andy Coulson and the former chief executive Rebekah Brooks.

In May 2012, Rebekah Brooks was charged with three counts of conspiracy over allegations that she tried to conceal evidence from detectives investigating phone hacking and alleged bribes to public officials. Brooks is to appear in court in June 2012. There has been no decision to charge Andy Coulson.

The issue of public interest as opposed to what is of interest to the public and how new and traditional media report high-profile court cases is often a contentious one. Doctor of Philosophy at Bond University, Joy Cameron-Dow, examines this issue in her article 'The question of crime' (2009) and she believes that the Internet, through links to multi-media facilities, offers far more graphic detail and specificity than is available in mainstream media, bringing the audience closer to the scene of the crime and the people involved (p. 71). Cameron-Dow makes the telling point (citing Richards & Sarre

2003) that journalists are “more in the business of revealing information than protecting it” (p. 74).

Former editor of the New Zealand Listener and freelance journalist, Finlay Macdonald, explored this theme of public interest and “celebrity justice” vis-a-vis name suppression, questioning the media’s role in hyping society’s hunger for celebrity gossip on the one hand, while demanding celebrities receive no special treatment on the other. Macdonald believes that the Internet and Twitter capacity renders name suppression almost redundant, because of our “voyeuristic celebrity culture” fuels a greater interest in finding out the name(s) of the person or people involved, and this is the reality of today’s crime and scandal-heavy news (Macdonald, 2009).

2.8 Ethics

Immediacy of information from new media technology has created an “ethno-legal paradox”, defined by Hirst & Patching (2007), as the confusion that arises when an action is morally right but legally wrong or vice versa (p. 266). As digital media has evolved, the need for ethical guidelines has become paramount, because of, if nothing else, the global reach of information posted online. Leading Melbourne media lawyer Peter Bartlett analyses such a case, when he discusses Australian broadcaster Derryn Hinch’s legal fight when he breached a suppression order and named two sex offenders on his website (Bartlett, 2011).

Hinch argued that the Australian Serious Sex Offenders Act 2009 was invalid as it “breached the implied freedom of political communication.” Chief Justice French rejected this argument but did observe that political communication could include social and economic features of Australian society. This notwithstanding, Hinch’s appeal against his contempt of court charges was ultimately defeated by the High Court with a 7-0 verdict (Bartlett, 2011).

Bartlett notes that while Hinch truly believes that the public have a right to know the identity of a serious sex offender, to the point that Hinch is willing to risk jail for this belief, the real issue is that the breaching of suppression orders is illegal, regardless, and that the law needs to change, not the ways we find to circumvent the law.

Professor Steve Kohm from the University of Winnipeg states in his journal article from *Crime, Media, Culture* (2009) that he believes shame is a dubious method of applying justice. Kohm believes the media’s relationship to the criminal justice system can operate on an emotional level, whereby the lines of information and entertainment are blurred, and in turn, this structures public narratives about crime and crime control (Kohm, p. 189).

Visiting scholar at Stanford University and contributing editor to *Boston Review* Evgeny Morozov describes “technological determinism” – the belief that certain technologies

are bound to produce certain social, cultural, and political effects – as a force being used to convince the public that the march of technology is unstoppable and unidirectional and thus obscures the roles and responsibilities of human decision makers. Morozov’s belief is that Facebook executives justify their assault on privacy by claiming this is where society is heading anyway and it is appealing to such deterministic narratives that Facebook manages to obscure its own role in the process (Morozov, 2011, p. 291).

Professor of Media, Culture and Communication at New York University, Helen Nissenbaum, sees privacy as a value that is a casualty of progress driven by technologies of information and would like to apply a framework of “contextual integrity” when formulating an approach to evaluating these systems and prescribing legitimate responses to them. According to Nissenbaum, the framework would create finely calibrated systems of social norms governing the flow of personal information in distinct social contexts and will define and sustain essential activities and key relationships and interests (Nissenbaum, p. 3).

The contextual integrity framework, when applied, clearly reveals ethical breaches when, for example, privacy settings on social media sites are circumnavigated to access information to bolster poor journalistic investigation or integrity when researching stories of a ‘public interest’ nature. An example of bolstering poor journalistic investigation is surely one breathless reporter’s by-line on the Carmen Thomas murder investigation which read “Sunday News this week uncovered photos

on 32-year-old [Carmen] Thomas's Facebook page...". Carmen Thomas went missing in June 2010 and her ex-partner was accused of her murder when her body was found four months later. The headline suggested these photos (which showed Carmen with two All Blacks) were recent (at this stage Carmen had been missing three weeks) and that they were the result of investigative journalism. However, on further reading you were informed "It's not known when or where the photos were taken but the social networking site has recorded them as being uploaded on September 22, 2008 (Bunting, 2010).

As mentioned in Chapter 1 of this thesis, the Privacy Act does not apply to media in respect to its news gathering activities nor the use of images or information found on social networking sites deemed to be in breach of privacy, and that on a number of occasions the New Zealand Press Council has ruled social media sites to be a public sphere. However, this aside, Bunting's admission further into the story that the "Facebook photos are only visible to Thomas' friends and their friends", surely is an example of trivial and unethical reporting and an exploitation of other peoples inability to navigate the complex privacy settings on Facebook. Furthermore, the question must be asked, of what public interest are two-year-old photos?

Interestingly, the Danish press council ruled in 2010 that journalists were not allowed to report on information found on *private* Facebook accounts, reasoning that what is found there is reserved for those that have been authorised to access the profile. Global news agency AFP (Agence France-Presse) said this ruling created a "legal

precedent on how media can use Facebook". The Danish press council made clear the distinction between private and public settings on Facebook, the former setting can only be accessed if the person is accepted as a 'friend' and the latter means that any information under this setting is available to any Facebook user (Smith, 2010).

The erosion of ethical standards and corresponding quality of journalism that has begun to arise from the misuse of such digital platforms as blogging, tweeting, and social networking present considerable challenges to balance and accuracy when news reporting. When financial gain, or cost cutting, is the main determinant, quality news reporting suffers and can lead to serious violations of all sorts of ethical standards, privacy being one of them. The author is not advocating the abandonment of these new media tools, rather the renewal of traditional media controls and the reaffirming that, ultimately, ethical guidelines in the digital era will be adhered to, or should be adhered to, on the same journalistic ethical code that applied to traditional media in the past.

2.9 Summary

As digital technology evolves, weaknesses in our privacy law are becoming apparent and one of the challenges we face over issues of privacy in the new media age is that of control over informational privacy. Once online, our Internet behaviour can be 'tracked'. This data can then be collated, and in turn on-sold, so that advertisers, for example, are able to improve their targeting of adverts. The Internet has also proved a challenge when applying suppression orders. The Law Commission has recommended

websites that carry or host information in breach of suppression orders, be made aware they could be held in contempt of court if the information is not removed or blocked.

New media technology has also created ethical dilemmas when the issue of public interest, as opposed to what is of interest to the public, collide. Social media has proved to be a rich source of information that can be exploited by those that take on the roles of judge, jury and executioner. A possible solution to privacy breaches is a framework of “contextual integrity” as proposed by Professor Nissenbaum. When this framework is applied to systems governing the flow of personal information in specific contexts, privacy breaches are clearly revealed when information is used for purposes other than what it was intended for.

Chapter 3

LEGAL FRAMEWORK

3.1 Introduction

This chapter outlines the legal framework for privacy protection in New Zealand as provided by the Privacy Act and discusses the role of the Broadcasting Standards Authority and the Press Council within this framework. I have also examined privacy tensions created through technological development and how this technology has exposed weaknesses within the law to protect our privacy.

3.2 Background

In Chapter 4 of the New Zealand Law Commission's *Review of the law of privacy* (NZLC SP19, 2008) the Law Commission traces the development of privacy in statute and common law in New Zealand and says that these statutes and laws provided "patchy" protection for some aspects of privacy, however privacy itself was not something specifically mentioned as something the law protected until the mid-1970s (p. 12.).

Technological development, says the Law Commission, is in part the reason for its review of privacy law in New Zealand, in particular, the storage and processing of personal information. The growth and development of the Internet has occurred since the New

Zealand Privacy Act 1993 and, as a result, the Law Commission states, this has given rise to new and difficult privacy issues (NZLC SP19, p. 13 & 18).

3.3 Information Privacy

Information privacy is sacrosanct and the linchpin of parliamentary democracy, and safeguarded through clause 3 of the New Zealand Privacy Act 1993; without the belief that the ballot box is private, that confidentiality exists between health professional and patient, that the law of the land upholds the concepts of private property and certain individual freedoms, democracy would not exist. However, the electronic age we now move in has meant that communication has become more complex, simultaneous and detached from place or territory. We have become part of a global audience that offers us new ways of collecting and disseminating information, which in turn has given rise to new markets that, in essence, traffic information and create privacy tensions that did not exist decades ago.

Prior to the advent of the Internet and new digital communicative technologies, privacy concerns were limited to the ability of traditional media of television, radio and print to infringe. Data information was gathered through electoral rolls, credit card transactions, product warranty cards and so on, and on-sold as informational databases for direct marketers, as an example, to sell to potential customers.

Hirst and Harrison (2007) explain that this capture of information at the point of sale is an important key to media profitability; that media interest lies in being able to directly target the audience as consumers and those databases full of consumer information raise important issues about individual privacy (p.34). As mentioned in Chapter 2, Chung & Paynter's study (2002) of privacy issues around information gathering on New Zealand based websites revealed approximately 12 per cent of websites studied collected information without providing the purpose for said collection (p. 4). Harvey's article on *Internet crime in New Zealand* stated that one in three New Zealanders had been affected by cybercrime, whereas in 2009 as a comparison "showed 36% of us had experienced a traditional crime" (2010, p. A9).

With the move from analogue to digital technology, there came dramatic improvements in the size, quality, pace and storage of data transmitted and because personal information in a digital format can be easily copied and integrated, it enables online marketers to create a highly personalised individual construct. Therefore, this personal information has the potential to become a serious threat to privacy if certain safeguards are not in place. The Internet allows for interactive two-way communication and, accordingly, poses unique information privacy threats that differ from traditional marketing channels, according to Malhotra, Kim and Agarwal in their study of privacy concerns (2004). They noted (p. 337) the four areas of concerns were those over how the information was collected; unauthorised secondary use; improper access and errors. As

an aside, it has been recorded that this lack of consumer confidence in information privacy is the major setback to the growth of e-commerce (Chung & Paynter, p. 4).

If privacy is to exist in this digital age, we must become educated in the ways information privacy can be breached and legislation must be adjusted to incorporate the ramifications of “fresh” information. Fresh information refers to what is mentioned in the New Zealand Law Commission Report 109 *Suppressing names and evidence* (2009) when they discuss how websites on the Internet are continually adding to existing information and therefore keeping it constantly in mind:

“...electronic information on the Internet is readily available, and easily searchable,... Although the evidence at court presents the final picture, the “colour” of that evidence could be affected by reference to developing investigation information” (NZLC R109, p. 63).

Of equal concern regarding “fresh” information being posted is also the fact that old or stale information remains accessible.

While traditional media information may also be contaminated, in the sense of being sensationalised and one sided, its readers’ attention has often moved to the next day’s reported event, this phenomenon known in legal circles as “slippery memory”; the Internet however, continues to update and add even more salacious detail (“Judge calls bluff”, 2010).

3.4 Privacy Act 1993

The New Zealand Privacy Act of 1993 applies to the handling of all personal information collected or held by public agencies. Personal information is defined as any information about identifiable, living people, regardless if it is on a computer or print file. Agencies are any people or organisations that hold any personal information. The Privacy Act is built around twelve informational privacy principles:

- Collection of personal information (principles 1-4);
- Storage and security of personal information (principle 5);
- Requests for access to and correction of personal information (principles 6 and 7; plus parts 4 and 5 of the Act);
- Accuracy of personal information (principle 8);
- Retention of personal information (principle 9);
- Use and disclosure of personal information (principles 10 and 11); and
- Using unique identifiers (principle 12) (Privacy Act, 1993).

The website devoted to the explanation of the New Zealand Privacy Act (www.privacy.org.nz) and associated information, states that the Act is primarily concerned with good personal information handling practices; it also sets out a complaint mechanism and contains rules regulating data matching.

The New Zealand Law Commission's final report, *Review of the Privacy Act 1993*, the last of a four stage review of privacy law in New Zealand was tabled in parliament in August 2011. One of the report's recommendations is that online and other news media, which are not governed by complaints bodies such as the Broadcasting Standards Authority and the Press Council, would be subject to the soon to be revised Privacy Act, in that

“publication” of personal information now includes the Internet, and it would become an offence:

if the collection, use or disclosure of information would be “highly offensive”. The report also recommends an amendment that would prevent others from further using or disclosing such information, even though it is accessible from a “publicly available publication” (Key Recommendations, 2011).

3.5 Digital Privacy Issues: Identity Theft

Technological advancements have meant that information can be interlinked and distributed at a touch of a button, but this does not mean because we can, we have to. While we have handed over personal information in the past to, say, lending institutions, government agencies, schools and so forth for some time, the big difference in the new media age is, that this information is increasingly fuelling what is known as ‘identity theft’.

Identity theft is a crime in which an imposter utilises key pieces of personal information, for example, your IRD number or driver’s license for example and uses this information to gain access to your finances to commit fraud, or provide false identification in order to benefit themselves in some way; in short, a theft of your good name. The advent of the Internet has accelerated this crime because it is a great source of obtaining identifying data through what might appear to be innocuous information sharing on such social networking sites as Facebook or MySpace. While this information in itself may be of little value, it adds together to provide a construct of a fuller profile, enabling others to assume your identity for criminal purposes.

In Coopes' article on cyber-crime she states that 65 per cent of the world's two billion internet users are estimated to have fallen victim to this crime, and it is a trade so lucrative it is thought to be worth several times more than the illegal drugs racket. Coopes quotes statistics provided by Symantec, a security software corporation, from its Australian cyber safety campaign run in conjunction with the Australian government. One of the speakers at the opening of the November 2010 campaign was Australian Federal Police National Manager of High Tech Crimes Operations, Assistant Commissioner Neil Gaughan, and he had to say:

What is most important is your identity and when that is lost on the internet, it could be gone forever. The trans-national nature of internet crimes makes them difficult to investigate, leaving law enforcement sometimes lagging behind fast moving gangs. Greater cooperation between nations and with corporations such as Facebook was key (Coopes, 2010).

Identity theft is a result of our continued casual approach to the information we post online about ourselves. In order to prevent illegal data matching activity we, as consumers, need to be better educated in ways to protect information that we disclose online and in turn insist that institutions have systems in place that protects this information.

3.5.1 Social Media

The growth of social networking sites on the Internet continues to soar. Nielson’s review of networking traffic ending December 2009 states that 67 per cent of global social media users visited Facebook and Facebook reported 400 million monthly active users at the beginning of February 2010 (Eldon, 2010). While social media sites are popular because of a sense of openness and connections made through interactive participation, there is no “ownership” of such sites and therefore no “control” and contributors can hide behind a fake transparency.

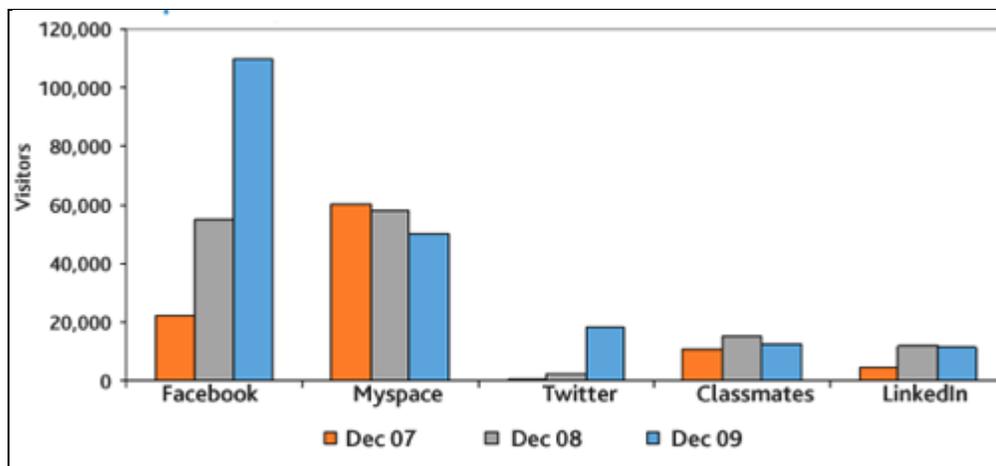


Figure 3.1. Top U.S media sites: December 2009

[Graph] Retrieved from <http://searchmarketingcommunications.com/2010/01/27/top-u-s-social-media-sites-december-2009/> Copyright 2009 by Search Marketing Communications. Reprinted with permission

This dramatic rise in the use of social networking sites is also reflected in New Zealand as shown in the graph below, which was generated from fieldwork done by UMR research in March 2010 in New Zealand. Their report *Individual Privacy and Personal Information* (included in the Privacy Commissioner’s *Annual Report 2010*) also noted high levels of concern about individual privacy and risks to personal information on the internet (p. 4).



Figure 3.2. Use a social network site (Yes's Only)

Do you use a social networking site such as Facebook or Bebo?

Base: All, n=750

NB: In August 2007 this was asked as "I have a page on MySpace, Facebook or equivalent site"

NB: In June 2009 this was asked as "I use a social networking site such as Facebook, Twitter or Bebo"

[Graph] Source: UMR research *Individual privacy & personal information* (2010, March) Office of the Privacy Commissioner. Retrieved from <http://www.privacy.org.nz/assets/Files/Surveys/Privacy-survey-2010.pdf> Reprinted with permission

We are moving in a much more complex and sophisticated information environment than ever before and, while public awareness is growing around issues of online privacy and basic precautionary measures such as spam filters and installation of anti-virus software is being used, technology such as the Internet is developing at a break neck pace which often leaves consumers with a surface understanding of online threats to privacy. Malhotra, Kim & Agarwal (2004) identified in their study on Internet use and privacy concerns, that while the notion of information privacy itself might sound straightforward, the practical boundaries of information privacy in actuality varies due to external factors such as industry sectors, cultures and regulatory concerns. One of the major findings of

this study was that online consumers consider it most important to (1) be aware of and (2) have direct control over personal information stored on marketers' databases (p. 337 & 350).

In general, European countries have strict privacy laws, whereas the United States has industry specific regulatory rules and, because of the increasingly borderless nature of the growing global economy, information practices need to be uniform and universal. With this in mind, the New Zealand government passed an amendment to the Privacy Act in September 2011 which, according to the media release from the Privacy Commission website (2010, September 8), ensures that personal information sent from overseas to New Zealand for processing has effective privacy protection. European officials had noted, prior to this amendment, that there existed a possible loophole in New Zealand law whereby data could be routed through New Zealand to a third country to get around European law.

3.5.2 Surveillance

In stage 3 of its review of privacy, *Invasion of privacy: penalties and remedies*, (NZLC R113) the Law Commission comprehensively dealt with the issue of surveillance and concluded there was a need for reform. The Commission report cited as one of its reasons that the benefits of surveillance need to be balanced against the need for protection against invasion of privacy. It also noted that the current law around surveillance contains a

number of notable gaps (for example there is no law around tracking devices) and New Zealand needs to be comparable with other democratic countries (pg. 15 & 16).

The Search and Surveillance Bill is intended to “implement a comprehensive reform of search and surveillance legislation” and many of the proposed changes are based on the Law Commission’s 1997 report (NZLC R97) on *Search and surveillance powers* (Search and Surveillance Bill, p. 1). This bill has created considerable opposition from civil liberty and media organisations concerning, amongst other things, the proposed introduction of the “Production order” – an order which can force people to hand over documents to the police. Chapter 8 of this thesis examines concerns of civil liberty groups and the media over the Search and Surveillance Bill, which as of 1st October 2012 has become the Search and Surveillance Act.

Another of the Law Commission members’ recommendations from their stage 3 review of privacy (NZLC R113) was that there should be a new Surveillance Devices Act, which would prohibit private individuals from intrusive use of visual surveillance, interception and tracking devices (p. 3 & 4). Commission members believe surveillance technology is growing at such a degree, and its potential virtually unlimited, that it is important to put boundaries in place to control its harmful use before it is too late. Current law has not kept pace and these issues are examined in more detail in Chapter 8 of this thesis.

Within the New Zealand legal framework lays two regulatory bodies established, in part, to deal with privacy breaches and these are the Broadcasting Standards Authority and the Press Council.

3.6 Broadcasting Standards Authority

The Broadcasting Standards Authority (BSA) was created to oversee the broadcasting standards regime in New Zealand and is empowered to operate through the Broadcasting Act 1989. Its role is to: receive and determine complaints; issue advice regarding broadcasting standards and ethical conduct and develop codes of conduct. The Authority is an independent Crown Entity, which means the government cannot direct the Authority in its work.

Privacy standards in the broadcast media are regulated by the BSA. Complaints must be made first to the broadcaster and, if the complainant is dissatisfied, then it goes to the BSA. The one exception to this process is if the complaint is about privacy, which may be made direct to the BSA. The BSA may award compensation for invasions of privacy. However, there is no one body that is charged with maintaining privacy standards on the Internet and the Law Commission's 2008 study paper on *Privacy concepts and issues* (NZLC SP19) notes that content is published on the Internet, in many instances, without legal advice or editorial control. The major problem is one of enforcement – particularly if the host of the website is overseas and therefore outside of New Zealand's jurisdiction (p. 23).

Chair of the BSA (2011), Peter Radich, made this comment in the 2010 Broadcasting Standards Authority Annual Report:

We are very conscious of the presence of the global internet and the influences it has particularly on younger people. We are acutely aware of the challenges involved in maintaining standards in the segment of traditional broadcasting when similar standards do not apply to internet broadcasting (p. 4).

The Law Commission is well aware of regulatory gaps around new media and privacy and the former Minister responsible for the Law Commission, the Honorable Simon Power (2011), has instructed the Commission to review this, and explicitly answer the following:

- How to define “news media” for the purposes of the law;
- Whether and to what extent the jurisdiction of the Broadcasting Standards Authority and/ or the Press Council should be extended to cover currently unregulated news media and, if so, what legislative changes would be required to achieve this end; and
- Whether then existing criminal and civil remedies for wrongs such as defamation, harassment, breach of confidence and privacy are effective in the new media environment and if not whether alternative remedies may be available (“Review of Regulatory...,” 2010).

The Commission released its preliminary analysis ready for public consultation in December 2011, entitled *The news media meets ‘new media’* (NZLC IP27). The Commission members propose that all news media, regardless of format or platform should come under a new and independent regulator (p. 9). Answers to the above questions and preliminary responses to the Law Commission’s proposals are discussed in more detail in Chapter 7 of this thesis.

3.7 Press Council

The Press Council (PC) was established by the New Zealand print media industry in 1972 and is a self-regulating complaints body. The PC's role is to determine complaints involving the press and also in promoting freedom of speech and of the press. The scope of the PC applies to published material in newsprint, magazines and their websites that subscribe financially to the PC, however the PC will adjudicate complaints about non-subscribing publications as well.

The first independent review of the PC since its inception took place in 2007 and was co-authored by retired judge Sir Ian Barker and Economics Professor Lewis Evans. In their study of the PC, the authors noted that "genuine" convergence amongst what had previously been separate, now existed between media and was only likely to increase in the future, and that convergence of media is affecting the nature of publication, rendering it more difficult for traditional regulation by any organisation: government or private. Enforcing professional standards, such as the respect of privacy, and obtaining commitment to any regulatory regime, from those disseminating material in the Internet are going to pose significant difficulties the authors state (Barker & Evans, p. 15).

While the BSA acknowledges (Principle 2) that 'public' facts can become private again, legal academic Dr Nicole Moreham believes the BSA should also recognise that a fact can

be 'private' even though it relates to something which occurred in a publicly accessible place (Moreham, p. 7). The PC has determined that social media websites and links with open access become, in effect, public places, and as such the onus lies on the social network poster to set the level of privacy on their social media page. In the PC's 2010 *Annual Report*, it states that a publication or website must show that republishing such material is justified on the grounds that it is newsworthy and in the public interest, and that the material would also have to be directly relevant to the matter of public interest (p. 6).

An overseas example of where this can go badly wrong was when the *Scottish Sunday Express* published an article on March 8, 2009, about what had happened to some of the survivors – now turning eighteen – of the 1996 Dunblane massacre. Based on information and pictures sourced from their social networking sites, the article claimed the survivors had “shamed” the memory of those that died with their “foul-mouthed boasts about sex, brawls and drink fuelled antics” (Murray, 2009).

A complaint was laid with the United Kingdom Press Complaints Commission (PCC) by Mullan, Weir and Campbell on the grounds the article seriously intruded into their sons' private lives and published photos of them, when they had previously been shielded from public view. The paper defended itself by arguing that the information was publicly accessible on social networking sites and the identities of the individuals were well-known, as they had been named at the time of the shooting.

The PCC upheld the complaint, however in its' statement the committee of the PCC said that it considers it can be acceptable in some circumstances for the press to publish information taken from such websites, even if the material was originally intended for a small group of acquaintances rather than a mass audience; that aside, circumventing privacy settings to obtain information would require a public interest justification (Press Complaints Commission, p. 2). Once again, this is a neat illustration of where Professor Helen Nissenbaum's idea of thinking about privacy as "contextual integrity" becomes helpful.

If the contextual integrity framework was applied in this instance, rather than dwelling on the notion of expectations of privacy the emphasis would be on the norms governing the flow of personal information in distinct social contexts, in this case social media sites, and the expectations around these norms in terms of what information is being posted and who is the audience. When these informational norms are flouted, as illustrated in the article in the *Scottish Sunday Express* and the publication of photos taken from some of the survivors' social media sites then contextual integrity is violated. While the PCC and the like mention a public interest justification for the using of social media site information by the media, this does raise the question of who is driving the interest, the public or the media.

The members of the New Zealand Press Council state in their 2010 *Annual Report* (p. 6) that they expect such complaints to continue as more and more information is shared on

social media websites and reminds those that access these sites when publishing in newsprint to adhere to ethical principles. Sadly, this admonishment is seldom followed in the face of what sells and perhaps the onus needs to be put upon web designers to be mindful of protecting contextual norms and values when conceptualising and designing web sites.

3.8 Summary

Privacy is intrinsically bound up with democracy and for democracy to exist certain aspects of privacy must be safeguarded. The way we interact online means we have become part of a global audience that offers us new ways of collecting and disseminating Information – information that in essence has become a commodity.

The Privacy Act 1993 applies to the handling of all personal information. “Publication” of personal information includes the Internet. Thus it would become an offence to collect, use or disclose information that is considered “highly offensive”.

Lying within the legal framework of privacy protection in New Zealand is the BSA and PC. Both the BSA and PC acknowledge the difficulties and challenges when information is published without the constraints of legal advice or editorial control. The PC in particular has reminded users of social media sites that these sites are in effect public places and any information posted there may be used for purposes other than what was intended.

Chapter 4

PRIVACY COMMISSIONER

4.1 Introduction

In this chapter I analyse the role of the Privacy Commissioner in the context of privacy protection. I have also examined the response of the Privacy Commissioner to the Law Commission's review of the Privacy Act and draw attention to the problem of identity crime.

4.2 Background

Alongside the creation of the New Zealand Privacy Act 1993 was the provision of the Office of the Privacy Commissioner (OPC), which was tasked with administering the Privacy Act. The office is an independent crown entity and has the responsibility to report through the Minister of Justice to Parliament and is accountable for its functions under the Public Finance Act (Haines, p. 257).

Included among the wide range of functions of the Office are:

- the investigative role it undertakes on receiving privacy complaints;
- monitoring of information matching (the regulation of government information matching operations to minimise privacy risks and maintain public confidence in the handling of shared personal data);

- modification (if necessary) of the information privacy principles or application thereof;
- and to take into account international guidelines applicable to protecting individual privacy.

Another major role of the OPC is to comment on legislative and administrative policy proposals that affect individual privacy (Haines, p. 257).

4.3 Annual Report 2010

In the key points of the *Annual Report* of the Privacy Commissioner 2010 (p. 9) it was noted that media enquiries had more than doubled from 2008 and appeared to reflect a growing public awareness and concern about privacy, particularly in relation to information technology, and the use of surveillance devices such as CCTV security cameras and tracking devices.

In response to public concern relating to information technology, the OPC conducted an official inquiry into Google's collection of Wi-Fi information for its "Street View" filming in New Zealand. Street View was launched in 2008 and was a new feature for Google Maps that let Internet users view and navigate 360 degree street level imagery of New Zealand's cities, towns, suburbs, regions and remote areas (Google Press Release, 2008). While Google was filming, it also collected other information from unsecured Wi-Fi networks within the range of the Street View cars, namely "payload" information.

Payload information is the actual content of unencrypted communications crossing the wireless network, such as emails, and in its findings the OPC stated that Google had no legitimate reason for such a seriously intrusive collection of information – breaching privacy principles 1, 3 and 4 of the New Zealand Privacy Act. This issue of Street View filming by Google was also hotly contested in Germany in 2010. Ilse Aigner, Germany’s Consumer Protection Minister at the time, feared that this geographic data could be cross linked and that there had to be a determination at what point a service provider has violated a person’s right to privacy (Spiegel Online, 2010).

This very question regarding ISPs having crossed the line in relation to a person’s right to privacy was examined in the New Zealand Law Commission’s review of the Privacy Act. Chapters 5 and 6 of this thesis examine this issue in more detail.

4.4 Privacy Commission on Law Commission’s *Review of Privacy Act: Technology*

In its role as commentator on legislative and administrative policy, members of the Office of the Privacy Commissioner made submissions on the Law Commission’s report on *Invasion of privacy: penalties and remedies* (NZLC R113, 2010) and their issues paper *Review of the Privacy Act 1993* (NZLC IP17, 2010). Of interest to this thesis is the latter submission, in particular Chapters 13 and 17 on Technology and Identity Crime.

The Law Commission members outlined the key technological developments in their review of the Privacy Act 1993 such as: the vast amounts of collected stored and re-used personal information the Internet facilitates and the phenomenal rise of social networking sites; the rise of surveillance technologies such as CCTV, GPS and RFID (Closed Circuit TV, Global Positioning System and Radio Frequency Identification respectively) and advances in computer technology such as Cloud computing and Deep packet inspection (NZLC IP17, p. 367-371). Commission members asked “Is the basic framework of the Privacy Act adequate to deal with technological change? Should the privacy principles remain technologically neutral?” (NZLC IP17, p.352).

The OPC’s response on the first question posed, stated in its *Submission on the Law Commission’s review (2010)*, was that if given the substantial changes foreshadowed in the Issues paper *Review of the Privacy Act 1993* (such as empowering the Privacy Commissioner to direct public or private agencies to produce Privacy impact assessments (PIAs) for any new projects that may have significant impact on the handling of personal information), the Office will be more effective in responding to technological change (p. 83).

The OPC emphasised three themes in its 2010 submission: the empowering of individuals; making the Privacy Act more effective and rising to the challenge of the electronic age. Examples to achieve these were provided by the OPC, such as mandatory breach

notification when individuals' privacy had been violated; secondly the OPC argued it needed a "bigger stick" to effectively enforce recalcitrant agencies to do the right thing (for example compliance reviews) and thirdly promoting privacy enhancing technologies (p. 4).

In regard to the second question "Should the privacy principles remain technologically neutral?" the OPC believed that there is a need to be realistic about what privacy law can achieve in respect to technological change, particularly given the fact that New Zealand has little ability to influence major software developers and global vendors. The better strategy, the OPC feels, is to be involved in developing compatible global solutions that collectively engage regulators, privacy professionals and software developers and vendors (p. 84).

While this strategy is fine in theory, the reality is that global market forces come into play here and the ethics of whether privacy is invaded or not has little bearing when information becomes a commodity and is sold. Companies are now realising the worth of the data that they have been collecting (through magazine subscriptions, credit card applications and so forth) and are now on selling this information to companies entirely devoted to collecting personal information in order to directly target consumers with advertising.

4.4.1 Identity Crime

“Are there any changes needed, either to the Privacy Act or to other laws, to better address identity crime?” (NZLC IP17, p. 466). The OPC states that the primary relevance of the Privacy Act to identity crime is the obligation that it places upon agencies to protect personal information that they hold (*Submission on Law Commission’s Review*, p. 98). In the Law Commission’s fourth and final stage report on *Review of the Privacy Act 1993* (2011) one of its key recommendations is that agencies which have lost or compromised personal data (as in, had it stolen through hacking) are required to inform victims of the data breach (Key Recommendations, p. 2).

The relationship between technology developments and privacy issues is entwined and one of the reasons behind the difficulty in creating privacy information law, according to Research Professor of Law at George Washington University, Daniel Solove, is the difficulty in formulating a compelling theory of privacy and that information privacy law is a mosaic of various types of law (for example tort, property and contract law) (Solove, p. 56). This idea is also echoed by the OPC in saying that the primary response to identity crime will probably be in criminal law rather than the Privacy Act (*Submission on Law Commission’s Review*, p. 98).

Solove believes the inherent weakness around privacy information protection lies in the ‘architecture’ that makes people vulnerable to such crimes and unable to adequately

repair the damage. The “digital dossiers” that are created through our digital interactions are not controlled by us but by such entities as government departments and private companies, and the ease of which identity crime is committed is because of an architecture that does not provide adequate security and Solove says it does not afford us with a sufficient degree of participation in its collection, dissemination and use (Solove, p. 115).

Significant changes proposed In the Law Commission members’ final report *Review of the Privacy Act 1993* (NZLC R123, 2011) would in part address these weaknesses that Solove identified, in that the Commission members recommend the Privacy Commissioner:

should be given a power to require an audit of an agency’s practices and systems for handling personal information. The Commissioner would only be able to require an audit for good reasons, such as if there are grounds for believing the agency’s systems are inadequate to protect privacy, or if the agency handles particularly sensitive information (health information, for example) (Key Recommendations, p. 1).

Presumably one of the “good reasons” is offered by the Commission members when it also recommends the Privacy Commissioner be able to make agencies release information, when individual complaints are laid where agencies have failed to provide access on request (Key Recommendations, p. 2.). The report also recommends:

the creation of two new offences in the Privacy Act: impersonating a person in order to obtain or misuse that person’s information, and destroying personal information in order to evade a request under the Act for access to that information (Questions and Answers, p. 3).

However, even with these recommendations in place, Solove says we have still got it wrong – even the term ‘identity theft’ is a misnomer, in that, it is treated as a series of

crimes rather than a larger problem about the way personal information is handled – a ‘theft’ rather than a product of inadequate security (Solove, p. 115). Solove would take it a step further than that recommended by the Law Commission report and make it a legal requirement for the establishment of specific measures of control over entities maintaining digital dossiers, and that these entities be held responsible for any inaccuracies or deficiencies in the information (p. 121).

4.5 New tools for the Privacy Commissioner

The Law Commission’s final 2011 report *Review of the Privacy Act 1993* (NZLC R123) details a number of recommendations made in relation to broadening the Privacy Commissioner’s powers, in order, the report says, to be more effective in ensuring compliance with the Privacy Act. As it stands enforcement of the Privacy Act is complaints driven, in that people can complain to the Privacy Commissioner about breaches of their privacy rights. However the Commissioner has limited powers to take action on her own initiative and the Law Commission report states such a system is not well suited to sorting out underlying problems. In order to address this, the Law Commission report recommends the Privacy Commissioner should have the ability to issue a notice to an agency that is in breach of the Privacy Act and to take action to bring its practices into compliance with the Act (NZLC R123, p. 14 & 15).

Secondly the Privacy Commissioner should be able to make decisions about ensuring agencies release information held about individuals, when they request access to it and,

thirdly, the Commissioner should be given the power to audit an agency's systems for handling personal information, on the grounds that best practices are not being met to protect privacy, or the information held is particularly sensitive – the Law Commission report cites health information as an example of this (NZLC R123, chpt. 6).

The current (2012) Privacy Commissioner, Marie Schroff, welcomed these proposed changes, saying it would give better protection for individuals and quick, cheap and effective answers when bad things happened. Schroff said the only people to end up worse off as a result of these proposals would be criminals and the cowboys (Barton, 2011).

4.6 Summary

The Office of the Privacy Commissioner is tasked with administering the Privacy Act. One of the OPC's roles is to comment on legislative and administrative policy proposals that affect individual privacy. Submissions were made on the Law Commission's review of the Privacy Act and as a result of this (and further research by the Law Commission) the following recommendations were proposed by the Law Commission to empower the OPC to:

- direct public or private agencies to produce Privacy Impact Assessments (PIA's)
- direct agencies to issue mandatory breach notification when individuals' privacy has been violated

- ensure agencies release information on request
- audit agencies systems for handling personal information

Chapter 5

LAW COMMISSION

5.1 Introduction

The New Zealand Law Commission Act 1985 established the office of the Law Commission, whose purpose is to promote the systematic review, reform and development of the law of New Zealand (Law Commission Act, 1985). Funding is provided by the Government and the Law Commission informs and supports discussions in order “to improve the quality, relevance and effectiveness of New Zealand law (About the Commission, 2011). The Law Commission makes recommendations to the Government regarding law reform and, for the purposes of this thesis, I am examining the Law Commission’s review of how new media is continuing to transform our notions of privacy.

5.2 Review of the New Zealand Privacy Act 1993

The Law Commission is researched based and reviews specific laws and its processes, decided on by either itself or under the advisement from the Minister of Justice. In 2006 the Law Commission was asked by the Government to undertake a review of privacy laws in New Zealand, the reason being that there had been no major review of the then thirteen-year-old Privacy Act and, since its inception, there have been dramatic advancements in technologies that have wide reaching implications on our notions of privacy.

The Law Commission has completed a four stage review of privacy with stages one, three and four, privacy concepts, invasion of privacy and a review of the Privacy Act respectively, pertinent to the theme of this thesis. The Commission also conducted a separate but ongoing project around the Criminal Procedure Act 2011 with the publication of the Issues paper *Suppressing names and evidence* (2009), which is examined in Chapter 6 of this thesis.

The last stage of the Commission's review of privacy was tabled in Parliament in August 2011 and reflects a mammoth five-year effort, in that the entire four stage review consists of one miscellaneous paper (which was produced online only), a study paper, three issues papers (previously known as preliminary papers) and three separate final reports.

In the final instance, the Law Commission found that the Privacy Act was "generally working well" and that the flexible approach when the Act was applied was well suited, while adapting itself to new technologies. However, because the Commission has recommended some major changes to some aspects of the Act, the Commission believes that Parliament would be best to pass a new Act rather than amending the present one (Questions and Answers, 2011, p. 1).

5.3 Stage 1: Privacy Concepts and Issues (NZLC SP19, 2008)

This stage of the Commission's review provided a conceptual framework examining social attitudes towards privacy, technology developments that challenge our notions of privacy and international trends towards privacy. The Commission paper states that, more than any other development, technological change has raised the salience of the privacy issue and in particular the emerging practices of surveillance – which are examine in more detail in Chapter 8 (NZLC SP19, p. 8).

The Commission paper finds that two techniques in particular are of great concern over issues of privacy and are made possible through the use of the Internet, these being data matching and data mining. The first technique refers to comparing information gathering from a variety of sources, with the general aim of finding information that relates to the one person, and the second extracting information that is implicit in data sets. The concerns over both are regarding the possible criminal use this information is put to and the uncovering of previously unknown information and the errors that this collation can create (NZLC SP19, p. 18).

The New Zealand Crime and Security survey (NZCASS) to which 5,400 responded, provided by the Ministry of Justice, gives an insight into the burgeoning identity related risk occurring:

- **Identity theft.** In NZCASS 2006, 2.8% reported one or the other of two forms of identity theft they were asked about. This equates to about 93,000 New Zealanders in private households aged 15 or more.
- **Internet fraud.** Among computer users, 1.7% said they had bought something over the Internet or by email where they believed they were a victim of fraud. This figure is based on all computer users. The proportion among those who had actually used the Internet or email for a purchase would be higher (Executive summary, 2007).

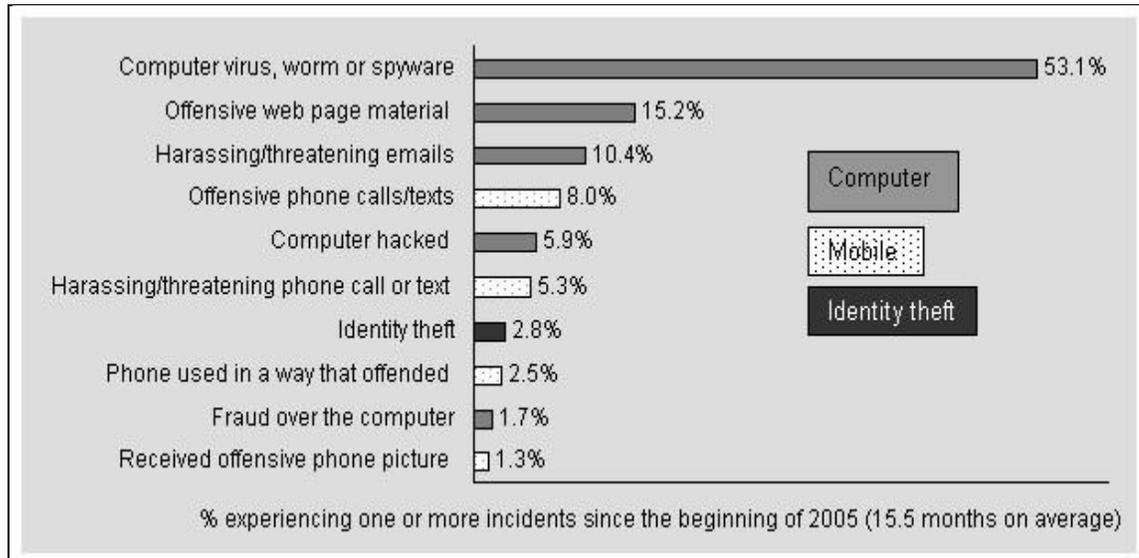


Figure 5.1. The most common forms of E-Crime 2005/6 experienced in New Zealand. [Graph] Source: New Zealand Ministry of Justice. Retrieved from <http://www.justice.govt.nz/publications/global-publications/t/the-experience-of-e-crime/executive-summary#figa>. Reprinted with permission.

There are two main ways personal information is solicited via Internet use, firstly by soliciting information from the user when registering on a website, such as filling out a questionnaire, and secondly, and more importantly, covertly, when a person explores a website, that website can gather information about their Internet service provider (ISP), their Internet protocol (IP) address, and exactly what parts of the website were explored and for how long. Key concerns regarding digital information that is captured willingly, or even unknowingly, revolve around: the inaccuracy of bias of said information; that it might

be used for purposes other than what it was collected for; and disclosure of information without consent or even awareness (NZLC SP19, p. 18).

Another area of concern the Commission's paper identified regarding the Internet is the posting by people of various forms of personal information, about themselves and others, on websites. In particular, the posting of images without consent of the individuals involved, has grave privacy implications, such as the indefinite storage of such images and the potential for them to be 'doctored', taken out of context or given new meanings.

5.4 Stage 3: Invasion of Privacy (NZLC R113, 2010)

Traditional media and subsequent advertising revenue flows are being threatened by the convergence of print and broadcast media via the Internet and its user generated audience and, as a consequence of this competition, there appears to be a growing emphasis in the traditional media on celebrity gossip and entertainment to drive sales. Further, due to the rise in popularity of social media sites and the accessibility of content that is published thereon, these sites are often targeted by traditional media to bolster the content of news items. The Law Commission's Issue paper 2009 examined privacy tensions created through blurred lines of entertainment and news, and the intrusive methods of gathering material, and asked several questions related to media and legal restrictions concerning surveillance and possible exemptions (NZLC IP, p. 291).

The subsequent 2010 report (NZLC R113) noted that while privacy featured well behind complaints (to the Broadcasting Standards Authority and Press Council) about accuracy, fairness and balance, serious breaches of privacy did occur and that there must be machinery to deal with them (p.76). Because the term ‘media’ is no longer the traditional preserve of broadcasters and print, the Law Commission Report recommends that it is desirable to frame exemptions and defenses by the media in its news gathering activities along the lines of the “legitimate public concern” defense, as established in the *Hosking* tort, which the report states protects the media and other potential defendants who publish material with justified cause (p. 80) – in short, the Law Commission members believe that:

- The tort of invasion of privacy recognised in *Hosking v Runtig* should be left to develop at common law.
- Any recognition and development of a tort of intrusion into solitude, seclusion and private affairs should be left to the common law (NZLC R113, p. 6).

The *Hosking* tort the Law Commission Report refers to relates to the 2004 Court of Appeal judgment whereby New Zealand television and radio presenter Michael Hosking sought a court injunction to prevent *New Idea* magazine from publishing photos of his twin children, taken when they were in their stroller along a public footpath, to illustrate an article about his marriage break-up. The grounds for the requested injunction were that the photographs were intrusive and invaded the children’s right to privacy.

While the Court of Appeal judges found against Hosking, their Honours established that in New Zealand law there is a right of action for the invasion of privacy. In New Zealand jurisdiction there are two fundamental requirements for a successful claim for invasion of privacy:

- The existence of facts in respect of which there is a reasonable expectation of privacy; and
- Publicity given to those private facts that would be considered highly offensive to an objective reasonable person (Evans, 2004, p.184).

The judgment found that there was no reasonable expectation of privacy in that the photographer took pictures of the children in a public place and no disclosure was given of any information relating to where the children lived or that would be useful to someone with ill intent, and furthermore publicising the photos would not offend the ordinary person (Evans, 2004, p.182).

Senior Law Lecturer at Victoria University of Wellington, Katrine Evans, argues in her article *Was privacy the winner on the day?* that the Court could have made more of the factors in favour of the plaintiffs, in that:

It would be perfectly justifiable in a free and democratic society – and also workable – to forbid any child to be targeted for photography (as opposed to being incidentally photographed), even in a public place, in circumstances where: (a) consent has been deliberately circumvented because it is obvious that refusal is likely; and (b) there is no legitimate public concern justifying that photography (Evans, 2004, p.182).

Evans' second criticism of the Court of Appeal's judgment is that it substantially raises, she says, the threshold of granting an injunction without fully discussing the arguments in favour of allowing injunctions in privacy cases. She argues that the judgment stipulates

that in most cases where an injunction to restrain publication in the face of an alleged interference with privacy, damages will be considered an adequate remedy (p. 183). Evans' argues that clearly, in many cases, damages are simply not an adequate remedy, reasoning that the cause for taking the action is automatically thwarted by publication and that a monetary award cannot return information to a non-public state (Evans, 2004, p. 183).

The Law Commission Report 113 also recommends the creation of a new Surveillance Devices Act, which will be examined in more depth in Chapter 8 of this thesis. Suffice to say, this new Act will provide for criminal offences and a right of civil action in relation to the use of visual surveillance, tracking and interception devices (p.3).

5.5 Stage 4: Review of the Privacy Act (NZLC R123, 2011)

In this final stage of the Law Commission's review of privacy in New Zealand, the Privacy Act 1993 was examined and was found to be flexible enough in coping with the "fast-moving and unpredictable technological age" (Burrows, 2011). This notwithstanding they did recommend improving the Act, as opposed to creating a new Act which was initially floated in 'Questions and Answers' August 2nd 2011 media release. The key recommendations concerned the Privacy Commissioner's powers (in that they needed widening and strengthening) and amending some exemptions to the Act's privacy principles – namely in information sharing between agencies and the publication of personal information online.

5.5.1 Publication of personal information

While principle 11, section 6 of the Privacy Act 1993, states the limits on disclosure of personal information, section 56 of the Act exempts those publishing information if it:

is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs (Privacy Act, 1993).

This exemption has meant that information or images that are gathered in a domestic context are not subject to the protection of the Privacy Act. For example, cases have been noted by the Law Commission members when investigating the effectiveness of the Privacy Act, where people have posted intimate photos of their ex-partners online. Also noted was the fact that once this information was out there, so to speak, it was not a privacy breach to further on-publish (Burrows, 2011).

Law Commissioner, Professor John Burrows, said that any review of privacy law must consider whether new technologies pose new threats to privacy and, in this case, these exemptions, combined with the global reach of digital technologies, has meant that publication and distribution of private information can cause significant distress and needs to be redressed. With this in mind, Law Commission members have recommended that the aforementioned exemptions should not apply if the collection, use or disclosure was “highly offensive” and that further disclosure of such information should be prevented even though it could be accessed from a “publicly available publication” (Burrows, 2011).

5.5.2 Identity theft

Chapter 3 of this thesis outlined how new media has been used to collate previously disparately held information in order to perpetrate civil and/or criminal fraud and, while members of the Commission recognised the problem and devoted a chapter to investigating it in their Issues paper (IP17), their recommendation in the final stage of the review on privacy, was, in short, that there should not be new criminal offences to specifically target identity theft.

The reason for this was that the newly revised Credit Reporting Privacy Code (this is a code of practice applying specific rules to credit reporters to ensure the protection of individual privacy) provides a stronger framework in which identity theft and fraud can be identified and further revision will prevent fraudsters using information to open new lines of credit. In addition the introduction of the Identity Information Confirmation Bill 2010 (as of 2012 awaiting its second Parliamentary reading) will provide a service that will permit agencies (subject to individual consent) to confirm identity information recorded under the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Passports Act 1992 and the Citizenship Act 1977 (NZLC R123, p.295 & 297).

5.6 Summary

In 2006 the New Zealand Law Commission undertook a major review of the 1993 Privacy Act in response to rapid technological change since the Act's inception. As a result of the five year review, the Commission found that concerns over privacy were inextricably tied

up with how personal information was being manipulated once online, and the emerging practices of surveillance.

In the final instance, the Law Commission found the Privacy Act was flexible enough in coping in a fluidly changing technological era, however in order to strengthen the Act the following recommendations were made:

- the Privacy Commissioner's powers need to be widened and strengthened
- the creation of a new Surveillance Devices Act – in relation to the use of visual surveillance, tracking and interception devices
- a new mechanism in order to improve information sharing between government agencies
- amending an exemption in the Act for personal information collection – in that it should become an offence if the collection, use or disclosure was “highly offensive”.

Chapter 6

NAME SUPPRESSION

6.1 Introduction

Several high profile cases dubbed “celebrity justice” where semi-famous New Zealanders have been granted permanent name suppression, and the subsequent public outcry, have ramped up the arguments around the issue of suppression orders. The publication of the names of some of these celebrities by a blogger has drawn attention to an issue that has been under review by the Law Commission. In this chapter I examine the Law Commission’s review of our suppression provisions and the media’s take on the application of suppression.

6.2 Issues Paper 13: Suppressing Names and Evidence (NZLC IP13)

The New Zealand Law Commission Issues Paper 13 (NZLC IP13) was released in December 2008 as part of a separate ongoing project around modernising and reforming the criminal justice system. The Issues paper aimed to elicit comments and submissions as to whether the suppression provisions of the New Zealand Criminal Justice Act 1985 were appropriate, in terms of how often and in what circumstances should suppression apply, and the challenges posed to suppression orders by the Internet. Of particular interest to this thesis are Chapters 3, and 4, dealing with name suppression or identifying particulars of accused or convicted person(s), as that of victims and witnesses, and Chapter 8 on the

publication and challenge of the Internet. Of equal interest is the Law Commission's final report (NZLC R109) and recommendations produced a year later in 2009.

Section 140(1) of the New Zealand Criminal Justice Act 1985 gives courts the broad discretion to prohibit publication of names or particulars of the accused or any other person connected with the proceedings:

Court may prohibit publication of names

- (1) Except as otherwise expressly provided in any enactment, a court may make an order prohibiting the publication, in any report or account relating to any proceedings in respect of an offence, of the name, address, or occupation of the person accused or convicted of the offence, or of any other person connected with the proceedings, or any particulars likely to lead to any such person's identification (Section 140(1) New Zealand Criminal Justice Act 1985).

The Section does not set out any criteria for the exercise of this discretion (NZLC IP13, p. 15). The Law Commission's view is that the presumption of innocence is not relevant to name suppression decisions. The Commission believes that the real question is whether the risk of harm to the reputation or dignity of the accused, when it becomes known they have been charged with an offence, warrants a different approach to pre-trial name suppression (NZLC IP13, p. 29). The Issues Paper states it is appropriate for courts to be aware of the impact of publication would have on victims. Regarding the grounds for suppression, the Law Commissions members' views are that there is merit in setting out specific grounds for name suppression, namely the risk of prejudice to a fair trial; undue hardship to the victim; and the overall interests of justice.

Section 140(1) of the Criminal Justice Act 1985 has subsequently been repealed with the advent of the Criminal Procedure Act 2011 (which commences in two parts with the majority of the Act brought into force in 2013) and now states:

200 Court may suppress identity of defendant

- (1) A court may make an order forbidding publication of the name, address, or occupation of a person who is charged with, or convicted or acquitted of, an offence.
- (2) The court may make an order under subsection (1) only if the court is satisfied that publication would be likely to—
 - (a) cause extreme hardship to the person charged with, or convicted of, or acquitted of the offence, or any person connected with that person; or
 - (b) cast suspicion on another person that may cause undue hardship to that person; or
 - (c) cause undue hardship to any victim of the offence; or
 - (d) create a real risk of prejudice to a fair trial; or
 - (e) endanger the safety of any person; or
 - (f) lead to the identification of another person whose name is suppressed by order or by law; or
 - (g) prejudice the maintenance of the law, including the prevention, investigation, and detection of offences; or
 - (h) prejudice the security or defence of New Zealand.
- (3) The fact that a defendant is well known does not, of itself, mean that publication of his or her name will result in extreme hardship for the purposes of subsection (2)(a).
- (4) Despite subsection (2), when a person who is charged with an offence first appears before the court the court may make an interim order under subsection (1) if that person advances an arguable case that one of the grounds in subsection (2) applies.
- (5) An interim order made in accordance with subsection (4) expires at the person's next court appearance, and may only be renewed if the court is satisfied that one of the grounds in subsection (2) applies.
- (6) When determining whether to make an order or further order under subsection (1) that is to have effect permanently, a court must take into account any views of a victim of the offence conveyed in accordance with [section 28](#) of the Victims' Rights Act 2002.

[\(Section 200 Criminal Procedure Act 2011\)](#)

With regard to the argument that suppression orders should be set aside on the grounds that the identity of the accused or victim appears on an overseas website, the Issues Paper states that technology advancement should not be determinative as to whether suppression is applied, rather it should be decided upon how widespread it has been, how accessible the publication is and whether the publication can be considered as spent – the all-important question being: what options are there for controlling this? The Law Commission recommended that where Internet service providers (ISPs) or content hosts become aware of publishing information contrary to suppression orders, it should be an offence for them to fail to remove the information or to fail to block access to it as soon as reasonably practicable (NZLC R109, p. 66).

There are a number of issues with this recommendation, namely whose responsibility would it be to make service providers “aware” of suppressed material? What about overseas based websites that are not subject to New Zealand law? InternetNZ spokesman Jordan Carter said that Internet service providers could not be expected to turn into censors, blocking access to material that is suppressed, especially on overseas websites (Gower, November 17, 2009). Answers provided by the New Zealand Law Society Criminal Committee members to questions raised in the Issues Paper regarding Internet publication of suppressed information, suggest they too had difficulty in finding solutions. The Committee members found problems with forcing service providers or content hosts

into taking down suppressed information, using the example of a blogger who had set up in a foreign country (Krebs, 2009).

Against this background are also issues around the term 'publication', in that should it be defined in legislation? Both the Law Commission and the Law Society thought not, believing it would create more problems than it would solve, the former stating it would be preferable to leave it to the courts to make decisions on a case by case basis (NZLC, R109, p. 66), and the latter saying that publication is about dissemination of information, and the manner in which it is conveyed, electronic or otherwise, is immaterial (Krebs, p. 14).

6.3 Report 109: Suppressing Names and Evidence (NZLC R109)

The New Zealand Law Commission tabled its Report 109, *Suppressing Names and Evidence* in Parliament on 16th November 2009 (NZLC R109). Sir Geoffrey Palmer, then President of the Law Commission, said that the most significant change was in the area of name suppression. Previously the courts had a broad discretion to prohibit publication, he said, and the Law Commission's recommendation was that there should be a clearer test for name suppression, with specified grounds set out in legislation (Palmer, 2009).

Proposed changes in response to the Law Commission report are included in the Criminal Procedure (Reform and Modernisation) Bill which became the Criminal Procedure Act in

2011 and comes into full force in 2013. This Act makes it clear that “wealth, reputation or public awareness” should not be reasons in securing name suppression. Auckland University Faculty of Law Associate Professor Scott Optican believes that this is one of the reasons the Criminal Procedure Act was passed, because name suppression is so open-ended and often goes out without any explanation or rationale from the judge. Optican also notes that the current provision that allows suppression is very broad-based and that the new Act would bring more order to the chaos and guide the discretion more (Koubaridis, 2011).

Former Justice Minister Simon Power said that the Government is looking to introduce legislation allowing judges to grant name suppression only:

- where there is a real risk of prejudice to a fair trial;
- to prevent undue hardship to victims;
- to prevent extreme hardship to the accused and/or persons connected with the accused;
- where publication would endanger the safety of any person;
- where publication would identify another person whose name is suppressed by order or by law;
- where publication would be likely to prejudice the interests of the maintenance of the law, including the prevention, investigation and detection of offences;
- where publication would cast suspicion on other people that may result in undue hardship (NZLC R109, p. 3).

Mr Power went on to say that being famous was not a good enough reason to be granted name suppression and one set of rules was needed for everyone to ensure public confidence in the justice system (“Name suppression...,”2010).

6.4 Media and Suppression

It was also noted in the Issues Paper that the media had expressed a strong view that suppression orders are granted more readily to people who are well-known than to people without a public profile (NZLC IP13, p. 24). The news media also expressed concern about the perceived increase in the use of suppression orders; accessing said information; in the way those orders are sometimes framed; and inconsistencies in media standing to challenge orders (p. 5).

The New Zealand Law Society's Criminal Law Committee's response to Issues Paper 13, as stated by Jonathan Krebs, Convener of the Law Committee, was that in general the media's processes and manner of reporting crime, justice and punishment, were of concern to the point where the Law Committee members believed that the idea of *sub judice* appeared to be overlooked. They questioned whether public interest had become more about public curiosity and stated that name suppression should be more available to the accused than the convicted (Krebs, 2009).

With regard to name suppression being perceived as more readily given to well-known people, the Law Committee members agreed with the comments made in the Issues Paper that publicity is not applied equally to all people and that it must be a relevant factor when weighing up name suppression. The Law Committee members would like the

focus to be on actual or potential impact, on an individual basis, as opposed to creating a “class” of people where suppression is automatically supplied (Krebs, 2009).

Controversy regarding “celebrity justice” had arisen over a number of court cases where high profile offenders were granted name suppression and which was subsequently breached by New Zealand blogger Cameron Slater. Slater, under the guise of blogger ‘Whaleoil’, spent much of 2010 breaching suppression orders as part of his campaign for ‘open justice’ and as an expression of his ‘outrage’ at the apparent ease with which name suppression was granted to so called celebrities. Slater posted online pictorial clues to the identities of two high profile sex cases involving a former Olympian and an entertainer. The latter case caused a media furore at the apparent leniency of the judgment – the entertainer was discharged without conviction for indecently assaulting a teenage girl and granted permanent name suppression.

Slater was arrested on charges of breaching court suppression orders. Slater’s justification for publishing was what he saw as the over use of suppression orders in the New Zealand legal system:

"What we've got here is kind of like creeping death - you get name suppression in this case, and then name suppression in that case - and then it's always lowering the bar so that almost anybody who has got a profile or a reputation to protect can get name suppression" (Radio New Zealand News, 2010).

While Slater was found guilty on eight charges of breaching name suppression, he was granted leave to go to the Court of Appeal on a question of law relating to whether the information or material posted on his 'Whaleoil' blog constituted a publication of a "report or account" in breach of sections 138-140 of the then Criminal Justice Act 1985. This very question around what is the meaning of "report or account" was tackled by members of the Law Commission, who held the view that it would defeat the intention of the sections if this was taken to mean that material suppressed is literally obtained from the proceedings, as opposed to the substance of the information before the court (NZLC IP13, p. 66). Members of the Law Society said they would like the wording updated to include reference to the Internet and its terminology, for example, it should include a reference to a "blog" (Krebs, p. 14). As of 2012 Slater's appeal is yet to be heard before the Court of Appeal.

It can be said that public perception of "open justice" was further eroded (this, despite the fact name suppression is automatic in cases where a child would be identified) over the permanent name suppression of a well-known comedian and subsequent discharge without conviction from sex charges involving his four year old daughter. In part the presiding judge believed the impact on the comedian's career would outweigh the gravity of the crime, however taking that reasoning to its logical conclusion suggests that status confers a leniency that would not be accorded to a less privileged member of society. Or, in other words, as Associate Professor Bill Hodge of Auckland University Law School said,

“if he’d been an auto mechanic, he would be down the drain before you could blink”
(Koubaridis & Gay, 2011).

Interestingly, *The New Zealand Herald* stated in April 2012 that the High Court overturned this sentence and has sent the case back to the District Court for the comedian to be resentenced (“Comedian’s sentence overturned”, 2012).

As a counterpoint to media/public concern over name suppression laws in New Zealand is media law academic Steven Price’s observation, that while much is made by the media that suppression is too easily given, this in fact is not the case. Media hype around “freedom of speech”, “public interest” and “open justice” as arguments against name suppression cases tends to reflect, Price believes, that media have poor understanding of how the laws of name suppression and contempt work, and they routinely beat up name suppression stories to paint the suppressions as unjustified (Price, 2009, November 29). This observation appears to be supported by the table below, sourced from the Ministry of Justice, requested under the Official Information Act, which sets out the number of cases where name suppression was granted in the last six financial years, broken down by jurisdiction. Note that cases may be counted more than once if separate name suppression orders were granted in multiple years.

Table 6.1

Number of cases where name suppression was granted, July 2005-June 2011

Jurisdiction	Court	Number of Cases Where Name Suppression Was Granted					
		JUL05- JUN06	JUL06- JUN07	JUL07- JUN08	JUL08- JUN09	JUL09- JUN10	JUL10- JUN11
Civil	District Court	3	0	1	1	0	1
	High Court	11	11	23	14	17	17
Criminal	Court of Appeal	1	2	2	0	0	0
	District Court	1,713	1,605	1,873	1,779	1,839	1,622
	High Court	163	148	176	126	143	119
	Youth Court	2	4	3	2	7	5
Total		1,893	1,770	2,078	1,922	2,006	1,764

Note Official Information Act request to the Ministry of Justice Electronic Case Management System (CMS). Reprinted with permission.

The Law Commission's 2009 report *Suppressing names and evidence* (NZLC R109) produced a similar table in its review on name suppression cases (from 2004 – 2008) and stated that the increase in suppression orders in the District Court can be attributed to the increase in workload (p. 9). Also stated and reflected in the above table is the fact that, if orders suppressing both evidence and names were made in one single case, that case will be counted twice in the number of cases in which directions were made. The author was unable to ascertain any detailed information about the nature of the cases in which orders were made but inferences can be drawn based on the numbers alone, one being, overall public perception around the apparent ease with which name suppression is handed out is not warranted – as law academic Steven Price asks, “Which is worse: our name suppression laws, or the media’s coverage of them?” (Price, 2009).

6.5 Summary

Public perception regarding the application of name suppression being more readily available to well-known people, combined with the media's process and manner of reporting crime has raised concerns with both the Law Commission and the Law Society.

In 2009 the Law Commission reviewed the suppression provisions as outlined in the Criminal Justice Act 1985 and recommended:

- where ISPs became aware of publishing information contrary to suppression orders, it should be an offense to fail to remove
- there should be a clearer test for name suppression, with specified grounds set out in legislation.
- The Criminal Justice Act 1985 as of 2011 has been replaced by the Criminal Procedure Act.

Chapter 7

SOCIAL MEDIA

7.1 Introduction

Social media refers to the technologies we use to interact online with other people and, because privacy concerns regarding social media is a global issue, New Zealand should be seen in this context. To illustrate privacy tensions when using social media I have examined the phenomenon that is called Facebook and review the Law Commission's Issues paper on new media.

7.2 Social media sites

Traditional media is more about assimilating information with limited options of response, whereas social media is built on interaction with websites and mobile applications and those that use them. Social media is conducted through social network sites; prominent examples of such site applications are Facebook for social sharing, Twitter for blogging in short bursts (information/commentary sharing) and YouTube for video sharing.

To demonstrate the rapid growth of the social media phenomenon in the new millennium the above mentioned network sites provide an instructive illustration. Facebook was founded by 2010 *Time* magazine's Person of the Year, Mark Zuckerberg, in 2004/5. What originally started as Harvard students' rate-the-photo site quickly evolved over the next

few years into the 800 plus million member chatting/photo sharing/game playing/information using site that it is today. By 2010 Facebook overtook Google as the most visited website.

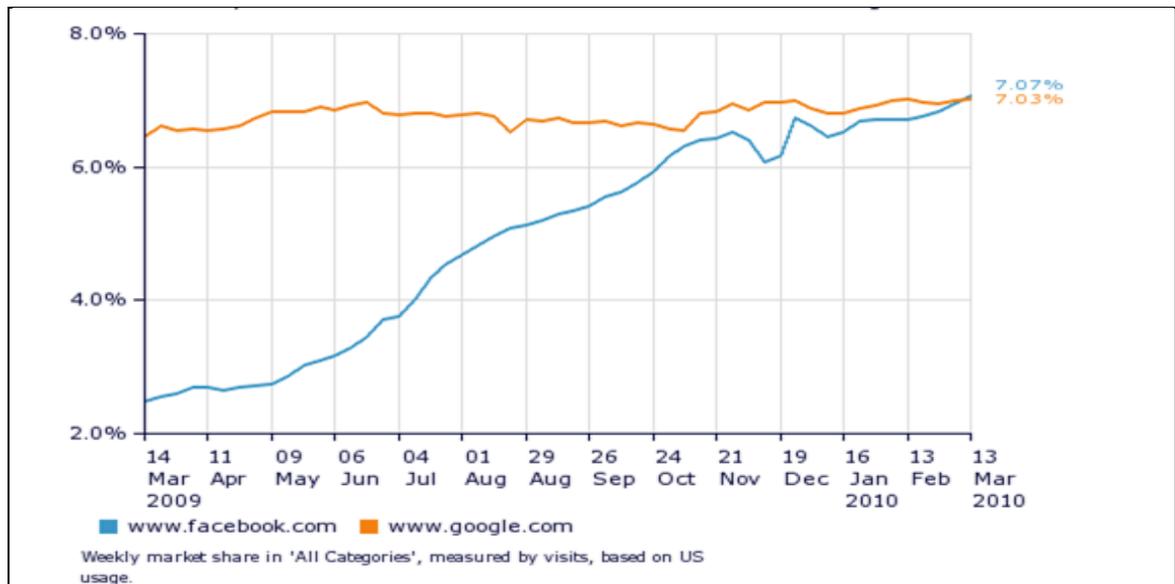


Figure 7.1. Weekly market share of visits to Facebook and Google

[Graph] Retrieved from <http://weblogs.hitwise.com/info/heather-doughty.html/> Copyright 2010 by Hitwise Pty Ltd. Reprinted with permission.

Twitter is a social networking site that relies on micro-blogging (140 character message or less) for communication. Users can communicate with their followers and get information spread around. Twitter was started in 2006 and now the site registers 200 million users (Chapman, 2011). Nicholas Jackson, Associate Editor at *The Atlantic*, an American monthly magazine reporting on technology, says that since Twitter's launch 8 per cent (as of July 2011) of U.S Internet users are on Twitter (as opposed to 50 per cent or so that have a Facebook account) and that the 18–29 year old age group are the most prolific Twitter users (Jackson, 2011).

Here in New Zealand, Hitwise, a company specialising in providing insights into New Zealand Internet usage, stated in their July 2009 newsletter, that the growth of Twitter in New Zealand was astonishing, increasing its market share fourteenfold, jumping from 556 places within twelve months (from June 2008 to June 2009) to rank 39th most popular website in New Zealand (New Zealand Newsletter, 2009).

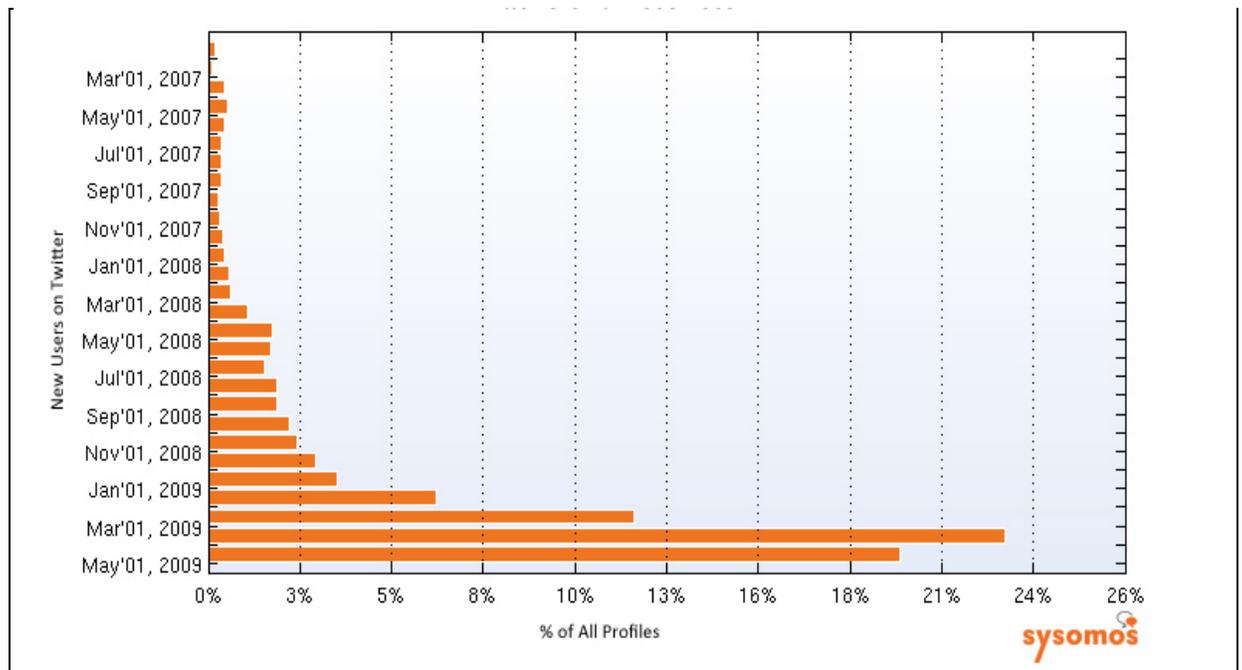


Figure 7.2. Twitter growth 2008-2009

[Graph] Retrieved from <http://www.sysomos.com/insidetwitter/appendix/> Copyright 2009 by Sysomos. Reprinted with permission.

YouTube is a video sharing website and originated in 2005. The content on YouTube is uploaded by registered users but anyone can view these videos. By 2006, 100 million videos were viewed per day and by 2010 YouTube exceeded 2 billion views a day (Yarrow & Angelova, 2010).

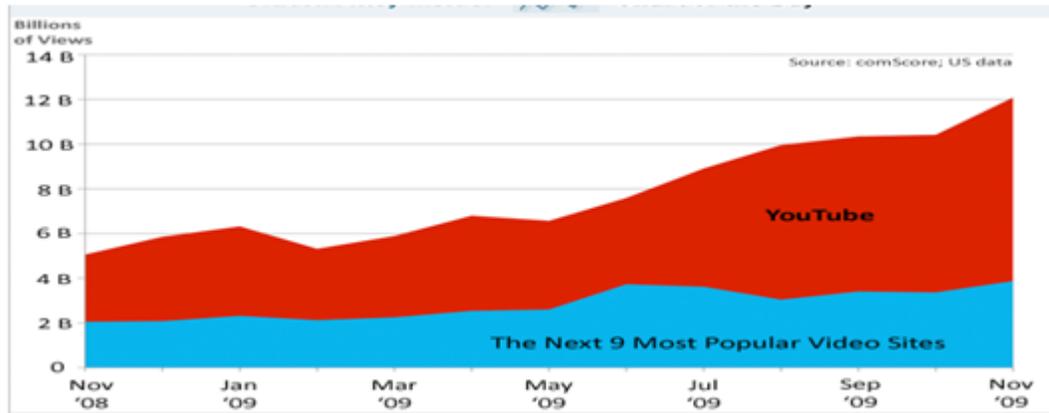


Figure 7.3. Video views for YouTube vs. its competitors
 [Graph] Retrieved from <http://www.businessinsider.com/chart-of-the-day-youtube-vs-its-competitors-2010/> Copyright 2010 by Business Insider. Reprinted with permission.

All these social media sites, to a greater or lesser extent, experience ongoing privacy issues associated with sharing information and for the purposes of this thesis Facebook will be used as a prime example of privacy infringement.

7.3 Privacy on Facebook

As early as 1999 questions over online consumer privacy were raised and, in the case of the CEO of Sun Microsystems’ Scott McNealy, glibly dismissed with the response “You have zero privacy anyway. Get over it” (Sprenger, 1999). Ten years on and this sentiment was echoed when former Google CEO Eric Schmidt predicted that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends’ social media sites (Holman, 2010). Schmidt went on to say that he did not believe society understands what happens when everything is available, knowable and recorded by everyone for all time (Taylor, 2010).

However, what we do understand and are becoming acutely more aware of is how social media pushes, and in some cases ignores, privacy boundaries. As Facebook continues on to world domination (note almost vertical growth figures supplied by Digital Strategist Ben Foster) a number of issues around privacy settings, 'tracking' of logged out users and identity theft have revealed the darker side of this social networking site.

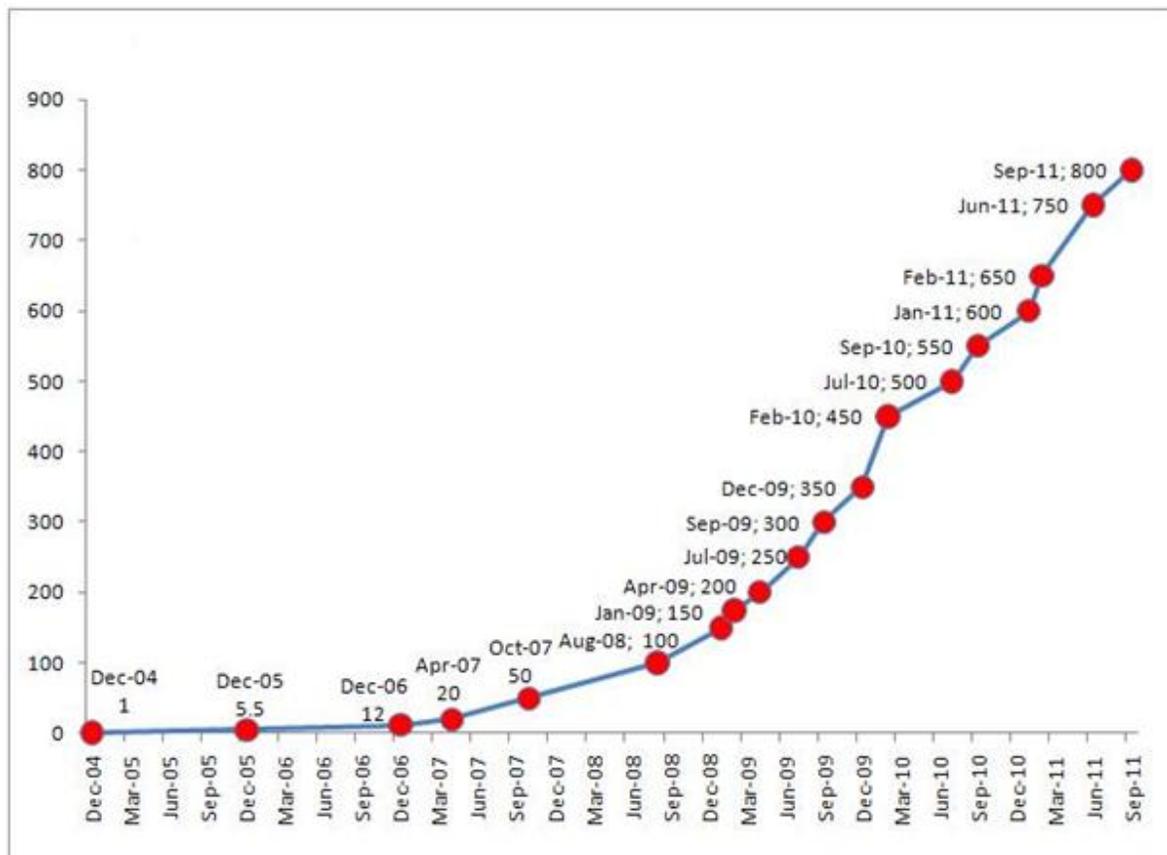


Figure 7.4. Number of Facebook users in millions [Graph]. Retrieved from <http://www.benphoster.com/facebook-user-growth-chart-2004-2011/> Copyright 2011 by Ben Foster. Reprinted with permission.

The ludicrous ease with which privacy settings can be circumnavigated, in part through user ignorance/apathy in trying to navigate the convoluted privacy tab settings, has meant

that what was shared with friends only, can be moved swiftly and irretrievably into the global domain. An example of this happening was outlined in Chapter 1 whereby a jilted lover was jailed for posting a naked photo of his ex-girlfriend on her Facebook page and making it available to all Facebook users worldwide.

Senior staff attorney for American Electronic Frontier Foundation, Kurt Opsahl, who focuses on privacy law, put together an interesting timeline that reflected Facebook's changing ethos in regard to privacy and highlighted excerpts from Facebook's privacy policies that illustrated this gradual erosion. In 2005 Facebook informed us that no personal information submitted would be available to any user of the website who did not belong to at least one of the groups specified by us on our privacy settings. By 2006 this had changed to Facebook stating that its default privacy settings would limit the information displayed in our profile to our school, our specified local area and other reasonable community limitations that Facebook would tell us about (Opsahl, 2010).

2007 saw Facebook declaring that our name, school name and profile picture thumbnail would be available in search results across the Facebook network unless we alter our privacy settings. By 2009 Facebook was giving an explanation of what information set to "everyone" meant: it could be accessed by everyone across the Internet (including those not logged on to Facebook); that the information is subject to indexing by third party search engines; and may be imported and exported by Facebook and others without privacy limitations. Further to this, Facebook stated that the default privacy setting for certain types of information we posted on Facebook is set to "everyone" and for this to

change we had to change the default settings. By 2010 came the explanation that when we connected with an application or website it will have access to “General Information” about us – the term general information includes us, our friends’ names, user IDs, profile pictures and so on (Opsahl, 2010).

Viewed as a cohesive picture, what started out as a private space to connect with groups of your choice rapidly evolved into much of your information going public by default and, consequently, by 2011 Facebook agreed to settle complaints by the United States Federal Trade Commission that it failed to protect users’ privacy or reveal how their data could be used.

7.4 Tracking

Tracking can be defined as the holding of information that connects a person’s actions or reading habits across cyberspace. When there is a relationship between the web user and the website that web users consent to, there is no problem. However, when users are being tracked without their knowledge or permission and this data is on-sold to advertisers for example, concerns arise over what other uses this data is being put to. American digital rights organisation Electronic Frontier Foundation projects director Peter Eckersley, believes that tracking data can be used to figure out your political bent, religious beliefs, sexual preferences, health issues or the fact you are looking for a new job – in short, incomplete or incorrect profiles can be created (Ghazali, 2011).

Facebook officials have acknowledged that they are capable of creating a running log of the web pages that each of its 800 million plus members has visited during the previous 90 days and also keeps track of where millions more non-members of the social network go on the web, after they visit a Facebook integrated site. However, two independent researchers have provided evidence that Facebook tracked “every page you visit” after logging out, and when confronted with this issue Facebook called it a ‘bug’ which they had subsequently ‘fixed’ (Ghazali, 2011). Contrary to this, the United States Federal Commission found that Facebook had deceived consumers by failing to keep privacy promises.

According to its website, the United States Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop and avoid them. The Commission website states that it issues an administrative complaint when it has “reason to believe” that the law has been or is being violated and it appears to the Commission that a proceeding is in the public interest (Federal Trade Commission, 2011).

In the U.S the Federal Commission charged Facebook with eight counts that it deceived consumers by telling them they could keep their information on Facebook private, when in fact Facebook allowed this information to be shared and made public. One of the charges was that Facebook promised users it would not share their personal information with advertisers, when it did. Chairman of the Federal Trade Commission, Jon Leibowitz

said that Facebook is obligated to keep promises about privacy that it makes to its hundreds of millions of users, and that Facebook's innovation does not have to come at the expense of consumer privacy – the Federal Trade Commission action will ensure it will not (Federal Trade Commission, 2011).

7.5 Misuse of Social Media

Cyber-bullying, harassment, defamation, suppression order breaches, identity theft, posting of intimate images are all examples of the misuse of the social media forum and all a threat to well-being and privacy. While some of these issues can be dealt with in a court of law, the 2011 Issues paper (NZLC IP27) from the Law Commission's study on new media, proposes possible solutions to these problems and regulatory gaps created in the digital medium. The following examples highlight how the information that is posted on Facebook can be used for purposes other than what was intended.

28 year old Natalia Burgess of Auckland assumed multiple false online personalities to form internet relationships with teenagers and is accused of having sex with at least one under-age boy. Police investigations of Burgess, dubbed the 'Facebook predator' in 2011, have revealed that Burgess set up fake Facebook accounts using images from other people's profiles. Burgess is also accused, by the mother of a 21 year old male who committed suicide, as being responsible for his death after he was rejected by one of her online personas after a six month courtship on Facebook.

Defamation can be defined as the publication of a statement that harms your reputation by making false statements about you. Education law expert and Secondary Principals' Association president, Patrick Walsh, commenting on a spate of students posting offensive material on Facebook concerning their teachers, said students were open to being sued for defamation. Walsh said that a "handful" of students had been expelled for posting defamatory comments online and that it is a major worry. In one case a student had accessed a teacher aide's Facebook profile and used her information in an online advertisement offering sexual services (Sutton, 2010).

Recruitment company Robert Half New Zealand Limited surveyed 414 New Zealand accounting and finance professionals and found, according to its press release, that 34 per cent of New Zealand hiring managers admitted to checking potential candidates' Facebook profiles. These figures are in keeping with hirers in Australia, but far lower than Hong Kong at 71 per cent and Singapore at 50 per cent, the survey found. Robert Half New Zealand General Manager Megan Alexander, said it was important to manage your online profile and be aware of the image you project (Robert Half, 2011). In other words, posting party photos on a social network site may someday affect your employment opportunities – or to paraphrase the poet Elizabeth Barrett Browning, things seen by candlelight are not the same as seen by day.

In an article in *The New Zealand Herald* it was noted that some public and private agencies

in the U.S were asking prospective employees for their Facebook user names and passwords, in order to vet applicants. This practice has prompted two U.S senators to ask the U.S Attorney General whether this is a violation of federal law. Both senators are drafting a bill that would bar this practice. Catherine Crump, American Civil Liberties Union attorney, commented that she thought it would take some years to decide whether Americans in the digital age have the same privacy rights as previous generations (Valdes, 2012).

In an examination of privacy in the workplace, an amendment to the German Federal Data Protection Act (2009) proposes possible restrictions on employers perusing social networking sites before hiring and, it is believed, will be passed into law in 2012. Approximately just over 20 per cent of the German population subscribes to Facebook and the proposal will increase guidelines for courts when handling cases that will arise as social networking and privacy issues continue to collide (Jolly, 2010).

Taking the information posted on Facebook (and other social networking sites) one step further, are the cases where said information is being used as 'evidence' in court, featuring in employee dismissals, or even third party use of, by journalists, for example. In what is being described as the latest tactic in American litigation in the online age is the trend for lawyers to 'mine' the private zones of Facebook and other social networking sites in the hopes of finding evidence to support their cases. Senior writer for Reuters Legal, Brian Grow, discusses in his article *In U.S courts Facebook posts become less private*

numerous cases whereby courts have granted defendants broad access to “private” photos and comments. Grow describes in one case how a lawyer successfully used information found on the Facebook page of a litigant’s daughter to win a case, and comments that defence lawyers in personal injury cases in particular, were finding social media networks to be a rich source of potentially exculpatory evidence (Grow, 2011).

New Zealand family law barrister, Simon Jefferson, says information found on Facebook or other such sites could count towards credibility, but is of limited evidential use in family law as conduct is excluded in relationship property matters and dissolution of marriage (Koubaridis, 2010). However, what can and has happened in New Zealand is being fired for posting critical comments relating to your employer on Facebook, which a postal worker found out after losing his case over unfair dismissal. Ignorance of the fact his privacy settings on Facebook were not as private as first thought, were not enough to save Mr Hohaia’s position when he was dismissed for using Facebook to criticise his job and “humiliate” his work colleague (Ihaka, 2010).

Third party usage or publication of information found on social networking sites is also open to charges of privacy violations and defamation. One such case reported in the British paper *The Independent* tells of a mother suing six national papers for defamation and breach of privacy after they ran stories based on her daughter’s exaggerated claims posted on Facebook and Bebo, concerning her ‘drunken party’ which only ended when police arrived (Verkaik, 2008). Not only does this action raise questions around privacy

and libel, it reflects sloppy journalism at best and serves to illustrate the breakdown of the most basic of journalistic rules – double check everything.

7.6 News media meets ‘new media’

In October 2010 the office of the Law Commission was directed by the then Minister of Justice, Simon Power, “to review the adequacy of the regulatory environment in which New Zealand’s news media is operating in the digital era.” As noted in Chapter 3 of this thesis, the Commission was charged with specifically answering three questions around: defining news media; whether current jurisdiction of the BSA and/or PC should be extended; and whether existing legal remedies are effective in the new media environment. The resulting Issues paper (27) was released in December 2011 and after receiving submissions and comments from the public and interested parties a final report, with recommendations, is expected to be tabled in Parliament in late 2012 (NZLC IP27, p. 3).

Chapter 2 of the Issues paper provides an overview of the evolving new media landscape and discusses regulatory gaps that have emerged with the public’s growing consumption and participation in online news and the use of social media. This digital environment is creating, members of the Law Commission state, a set of policy and legal challenges, including but not limited to, the fact that web-based publishers are not accountable to any regulator or complaints system other than the basic legal framework which applies to all citizens, restricting speech which defames or causes harm (NZLC IP27, p. 6).

Part two of the Issues paper, chapters 7 and 8, is of particular interest as members of the Law Commission grapple with the array of problems emerging from the digital environment and query whether the law can be better adapted to new media publishing, and whether the courts are the best forum for resolving disputes between free speech and the right to privacy.

7.7 Part 2: Speech harms

In conducting the review of the regulatory environment in which new media operates in New Zealand, Commission members sought information from many organisations such as the New Zealand Police, the Privacy Commission, Netsafe (a company which promotes internet safety in New Zealand), and the Human Rights Commission. Social media sites such as Facebook and Google were also consulted about their own internal systems for managing speech abuses (NZLC IP27, p. 151).

Instances of privacy complaints generated by Internet related abuse the Issues paper cites, are those revolving around breaches ranging from incriminating or inflammatory content found on the complainant's Facebook page and then used against them; when false Facebook pages were created in order to mislead or embarrass the complainant; or the posting of intimate photos or film of them on Facebook or other social media sites as noted in Chapter 5 of this thesis. Ranging further afield, examples are supplied of

worldwide reporting of privacy intrusion via online publishing which has resulted in reputational damage and instances of threats to trial processes such as publication of suppressed evidence (NZLC IP27, p. 154 & 159).

When investigating social media sites such as Facebook and Google for examples of privacy breaches which New Zealand users were reporting, Law Commission members were informed that while Facebook has effective self-regulatory systems that prevent such abuses, neither:

currently captured the sort of information with respect to problem reporting by individual users that would allow them to provide us with the detailed country specific analysis we were seeking (NZLC IP27, p. 180).

This aside, the Issues paper states that through research and consultation there are strong indications that significant harm does occur as the result of malicious use of the Internet as a publishing platform and in turn offer some preliminary ideas to address these problems (NZLC IP27, p. 183).

The Law Commission paper indicated there is merit in creating a legal provision whereby Internet service providers (ISPs) and websites be issued “take-down orders” against material that has been established as unlawful and harmful. Secondly, they recommend fine tuning the Human Rights Act 1993, the Harassment Act 1997 and the Telecommunications Act 2001 to ensure that they apply to harm generated by the use of digital platforms (NZLC IP27, p. 193-194). Thirdly, to fill gaps in the law created by new

media, a recommendation is offered of a new mechanism to facilitate “a single, well publicised and accessible point of contact for those wanting a remedy for harmful communication” – a Communications Tribunal or, failing that, a Communications Commissioner to negotiate solutions (NZLC IP27, p. 201). The new Communications Tribunal or Commissioner would cover any dispute that resulted from publishing in traditional or new media platforms.

Australia is also going through an inquiry into the effectiveness of their current media codes of practice. The resultant report (known as the Finkelstein report), submitted to the government in February 2012, appears to have polarised opinion between those that believe the report proposal of a newly created independent government funded News Media Council is a good idea, and those that believe it would pose a threat to press freedom and free speech. While the report did not find evidence of “the law-breaking cowboy antics seen in British journalism”, the academics that made submissions did believe that the Australian media “needed to be kept on a tighter leash” (Stewart, 2012).

7.8 Summary

Facebook is the largest social network currently (2012) on the Internet. Originally built on the concept of information sharing between networks of people, its potential reach has meant that increasingly, many businesses and other organisations use Facebook as a means of marketing. However, Facebook’s phenomenal growth has come at some cost to participants’ privacy, to the point where the United States Federal Commission charged

Facebook with eight counts of failing to protect users' privacy or reveal how their data could be used.

Social media is a tool like any other, but the ramifications of the misuse of this tool can be far wider and be present far longer than most other tools. In a bid to explore whether existing legal remedies are effective in the new media environment, the New Zealand Law Commission undertook a study of regulatory gaps exposed by public consumption and participation in online news and use of social media. Initial research revealed to the Commission the necessity for a legal response to the malicious use of the Internet as a publishing platform, and indeed any digital platform used in this manner.

Chapter 8

SURVEILLANCE

8.1 Introduction

At the beginning of its review on privacy, the Law Commission commented that more than any other technological development that raised the salience of privacy was the emerging practices of surveillance. This chapter looks at the Search and Surveillance Bill which became law in 2012 and what happens to privacy when technology is misused.

8.2 Surveillance and privacy

In the journal *Contemporary Sociology*, surveillance is referred to as “the process of watching, monitoring, recording and processing the behaviour of people, objects and events in order to govern activity” (Jenness, Smith & Stephan-Norris, p. 7). Increasingly, surveillance is not bound by the notion of security, instead it has become so pervasive in our daily life that it “scarcely takes into account the principles of necessity, purpose limitation and proportionality” (Wright et al., p. 344).

The Law Commission’s study paper (2008) on *Privacy concepts and issues* (NZLC SP19) identified key trends and developments in regard to surveillance which included the convergence of new technologies (in computing, telecommunications and sensing) which has created powerful networked surveillance systems that are:

less visible and more continuous in time and space, provides fewer opportunities for targets to object to or prevent the surveillance, is greater in analytical power, produces data that are more enduring, is disseminated faster and more widely, and is less expensive (NZLC SP19, p. 136).

The implications for privacy are many, ranging from concerns over the relationship between individuals and the state (in terms of social control) and the use the surveillance data is put to in regard to profiling, as well dubious media practices in pursuit of 'public interest' stories (NZLC SP19, p. 139).

Hirst & Harrison (2007) believe that media has played an important role in legitimising the growing level of commercial and political surveillance over society (p. 291). One example they use to illustrate this point is the rise of 'reality' television. *Border Security*, (a show that gives a bird's-eye view of what happens behind the scenes at Australian airports) is mentioned as one of a number of programmes that through the entertainment value these provide "the very act of surveillance is naturalised" and the show is portrayed in such a way as to "reduce the intrusive and invasive nature of what we're seeing" (p. 302).

8.3 Invasion of Privacy: Penalties and Remedies (NZLC R113)

The above New Zealand Law Commission 2010 report states that in its review of privacy, surveillance had emerged as the area where the gaps and inconsistencies in the law were particularly significant. Chapter 3 of the report sets out the most important reform of surveillance law and that is the recommendation of the creation of a new Surveillance Devices Act. Members of the Law Commission believe that current law has not kept up with rapid developments in surveillance technology, in particular, tracking and visual

surveillance. They believe that it is important to make an argument that there need to be strong sanctions to control the most objectionable types of intrusion (NZLC R113, p. 22).

With this in mind, their recommendations state that it should be an offence to trespass on someone's property to install a surveillance device; to film inside someone's dwelling without their consent; to install or use a tracking device to track someone without their consent; and that there should be provision for a right of civil action by any person in breach of any of these criminal offenses (Palmer, 2010).

However, tracking someone online, while not a criminal offence can be perceived as an invasion of privacy, as Jacqueline Sperling, the ex-lover of former Wanganui mayor Michael Laws can testify to. Mr Laws 'outed' himself for being "foolish in my private life" in a bid to pre-empt (as it turned out, non-existent until he bought it to media attention) media publication of "salacious" emails and texts he had exchanged with Sperling (Coleman-Ross, 2010). David Fisher, *The Herald on Sunday* reporter, using Facebook 'friends' and the application of Google maps, triumphantly declared he and another colleague were able to track Sperling's geographic dwelling to such a degree as to be able to "put our people on her doorstep", all because *The Herald on Sunday* wanted to speak "directly" to her (Fisher, 2010).

All of this in pursuit of a story with little or no public interest, and one that came across as a self-congratulatory technological hunt that achieved what? Sprenger herself said “They had no story, so they made me their story, with no regard for my children or my mental or physical well- being” (Edwards, 2010).

The recommendations from the Commission report are designed to target the most objectionable types of surveillance, states the Right Honorable Geoffrey Palmer, former President of the Law Commission, who finds it bizarre the Police need to obtain warrants to do most of these things, yet the law does not prohibit other people doing them. The recommendations do not prohibit people from filming in public, nor does it attempt to limit the use of closed circuit (CCTV) monitoring of premises for security reasons (Palmer, 2010).

The report (NZLC R113) states that the “legitimate public concern” defense is appropriate protection for the media when publishing material with justified cause. The “public concern” defence refers to information that is of legitimate public concern, it is likely to apply to information about threats to public safety, or corruption for example – in short information that may affect the public as opposed to what may titillate. However, how the media obtain their information in pursuit of public interest stories has been questioned recently, both here and abroad.

8.4 Misuse of digital technology

The collision between digital capability and privacy occurred in what the media has dubbed the 'Cuppagate' saga in the run up to the 2011 general elections, when Prime Minister John Key laid a complaint with police over the taping of his conversation with Act's Epsom candidate John Banks in a café. Inadvertently or otherwise a cameraman left a recording device on the café table the politicians were sharing that captured their conversation. The High Court declined to make a judgment on whether the conversation was private because "it would prejudice the ongoing police investigation if a ruling was made" (Cheng, 2011). Public and employment law specialist Mai Chen said the illegality or otherwise of the incident hinged on four questions: Was it a private conversation?; Was the interception intentional?; Does subsequent disclosure (New Zealand First leader Winston Peters revealed the alleged contents at a public meeting) fall foul of the Privacy Act?; Was there a reasonable expectation of privacy? (Chen, 2011).

By March 2012 the New Zealand police decided not to lay charges against the cameraman but had issued him with a 'warning'. This has also meant that the media are not allowed to publish the contents of the tape as it is illegal to disclose the contents of a private conversation that has been unlawfully recorded.

The Leveson Inquiry set up by British Prime Minister David Cameron in July 2011, is another, far more serious, example of suspect media actions in using surveillance to pursue stories of dubious public interest. The inquiry was instigated in response to

revelations that the now defunct *News of the World* newspaper commissioned a private detective to hack murdered schoolgirl Milly Dowler's phone after she disappeared in 2002. The first part of the Inquiry looked at the culture, practices and ethics of the press in general and began with a series of seminars to engage the public and professionals on the wider picture of how the media is working in Britain. Initial public response from prominent actors Hugh Grant and Sienna Miller, author J.K. Rowling, former head of the FIA (world governing body of motor sport) Max Mosley, and Gerry and Kate McCann (parents of abducted daughter Madeline) have all detailed their revulsion at the intrusive surveillance methods and probable phone hacking carried out by the media. In Mosley's case, he has begun legal proceedings against Google in order to remove the fake story (initially run by the *News of the World*) about his alleged 'Nazi orgy' from still appearing online (The Leveson Inquiry, n.d.).

As of May 2012, the Leveson Inquiry has been running just short of a year and appears to be still wrestling with ways to create a mechanism that would restrain the worst aspects of the media in pursuit of public interest stories, with that of freedom of expression. At this stage of the Inquiry witnesses are being interviewed in regard to the relationship between the press and politicians. British newspaper the *Daily Telegraph* chief political commentator, David Osborne, summed up the gist of this particular stage of the Inquiry neatly, when he said on being interviewed:

“Our democracy was starting to become a private conversation between elite groups...Political reporting, as I observed it, had become a matter of private deals, arrangements invisible to the voters” (O'Carroll, 2012).

The Guardian newspaper reporter Nick Davies, credited with revealing the phone hacking by *News of the World* reporters, believes that journalists wanting to publish private information should have to justify what they are writing before a public interest advisory body. Such a body, he believes, would help distinguish between what was published in the public interest as opposed to what was of interest to the public. However, Paul McMullan, former *News of the World* deputy features editor, defended practices of intrusion and of illegal voice mail interception, claiming it is was widespread practice across Fleet Street. McMullan claimed that readers were the ultimate judge and jury that determined what was published, and that “Privacy is the space bad people need to do bad things in” (Cusick, 2011).

Continuing this theme of privacy equating to criminality is the proposal by the British Government to push through legislation that would allow the Government Communications Headquarters (GCHQ – Britain’s electronic listening agency) warrantless access to text messages and emails, websites and conversations over Skype. Under the new law, Internet service providers (ISPs) would be instructed to install this hardware to effect these changes. *The New Zealand Herald* article quoted “a Home Office spokesman” as saying it was vital that police and security services are able to obtain communications data in certain circumstances to investigate crime and terrorism” (“Big brother...” 2012).

Another example of the possible misuse of surveillance technology that is causing controversy is the ‘FootPath’ programme which is being used in many British retail chains

which works by detecting a frequently changing signal from a mobile phone. Through the units installed in various shops, retailers can track the path the customer takes as they move through the premises. The idea behind this technology is to help stores redesign to maximise sales; however, this is happening without the customer being aware that their cell phone is being monitored unless their attention is drawn to a sign somewhere in the store, or the cell phone has been switched off. Incidentally, even when a cell phone is switched off it can still act as a 'transmitter' so to be totally off the 'grid' the battery needs to be removed.

Obvious privacy concerns revolve around possible hacking of this data and compromising personal information stored on customers' phones or employee misuse of this information. All of the data collected is processed by FootPath – in other words being processed by a third party, not the actual shops that bought the technology. Examples of the sort of information collected ranges from overall number of visits, to visit time and frequency, to the nationality of the visitor.

A trial of this technology in two American shopping malls was halted after just one day amid United States Senator Schumer's concerns that the practice violated privacy. Schumer has asked the Federal Trade Commission to examine this 'new' technology and how it sits with existing consumer privacy regulations. Schumer questioned the need for this tracking without informed consumer consent when security cameras, heat maps and people counters are already utilised in many premises. The British manufacturers of

FootPath technology counterargued that tracking of consumers already occurs online and this is a way for 'real world' stores to create a level playing field (Censky, 2011).

8.5 Search and Surveillance Bill

Please note that the author has analysed the Search and Surveillance Bill rather than the Act itself, as the bill became law immediately prior to the submission of this thesis.

The Search and Surveillance Bill (2009) that became law in 2012, is largely based on recommendations put forward in the Law Commission's *Search and surveillance powers* 2007 report (NZLC R97). Currently, as stated in the introduction to the Bill, search and inspection powers are spread across 69 different Acts and do not cover technological advancements adequately (Search and Surveillance Bill, p. 1). The Law Commission made 300 recommendations in its report, including modifications or additions to the present law (NZLC R97, p. 15). Of particular interest to civil liberty groups, the Law Society and indeed the general population are the proposed increased powers around surveillance, the examination and production orders and the extension of these provisions to a broad spectrum of state agencies, such as Customs.

While the current law allows for the planting of listening and tracking devices for alleged serious offending, under the new Act surveillance powers widen to include installing visual devices in homes and workplaces when investigating crimes that warrant sentences of

seven or more years. In the Bill, acknowledgement is made that these latter forms of surveillance devices have “more effect on privacy than others”, and it is proposed to offset these concerns by limiting these powers to the Police, Customs and Internal Affairs, and that “any extension of these more intrusive forms of surveillance to any other enforcement agencies in the future would require consideration by Parliament” (Search and Surveillance Bill, p. 4 & 5).

So exactly how many crimes are committed in New Zealand that warrant seven or more years in custody? The following figures were obtained from the Ministry of Justice website and those figures that receive five or less year’s imprisonment and the subsequent total overall average have been deleted. The 1.2 figure next to the year 2006 refers to the explanation of the terms LES (Law Enforcement System) and CMS (Case Management System) (“Convictions and...,”p. 4, Ministry of Justice, n.d.).

Table 8.1 *Total number of custodial sentences imposed of various lengths 1997 to 2006*¹.



	LES							CMS		
Custodial sentence length imposed	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
>5 to 7 years	131	128	140	99	112	111	135	144	150	143
>7 to 10 years	80	90	75	101	73	96	95	89	125	103
>10 years	22	23	21	19	35	31	43	30	30	43
Life imprisonment	37	24	23	29	19	27	21	21	20	25
Preventive detention	10	9	18	13	9	10	17	33	14	12

Total	8102	8255	8177	7886	7805	7930	8497	10353	10553	10469
-------	------	------	------	------	------	------	------	-------	-------	-------

Notes

1. The system used to log cases was updated in 2004 (from LES to CMS). This has caused changes in the figures and trends in cases that are observed up to and following 2004. In particular, any changes in the number of cases in 2004 may not represent a true change in offender patterns. Accordingly, caution should be used when making inferences based on any change between 2003 and 2004. Please also note that other changes in the above data are partly due to, for example, finalised appeals.

From New Zealand Ministry of Justice. Retrieved from <http://www.justice.govt.nz/publications/global-publications/c/conviction-and-sentencing-1997-to-2005/Publication>. Reprinted with permission.

Firstly, the report from which these statistics were taken states that long determinate sentences of at least ten years duration accounted for less than one per cent of all custodial sentences each year over the decade, so combining the seven to ten year imprisonment figures with those would presumably make a negligible percentage increase (“Conviction and...,” p. 5.). Secondly, the Search and Surveillance Bill itself declares that concerns have been expressed that additional powers which law enforcement officers would receive, regarding using intrusive surveillance devices, were disproportionate to the offending likely to be investigated and would extend their powers unnecessarily – it would appear these figures confirm these concerns (Search and Surveillance Bill, 2009, p. 3). Equally it can be argued that this also shows that law enforcement agencies have been responsibly limited to only the most serious crimes.

However, as mentioned before, if any state agencies other than the Police, Customs or Internal Affairs seek to use these more intrusive surveillance devices they must seek approval by “the Governor General by Order in Council made on the recommendation of the Minister of Justice before being able to do so” (McSoriley, 2011, p. 7). This, combined

with the fact that the threshold for the use of this type of surveillance has been raised from five to seven years, has, as proponents of the Bill believe, addressed concerns about the surveillance device powers contained in the Bill, particularly those regarding agencies other than the New Zealand Police conducting surveillance operations (Search and Surveillance Bill, p. 5).

Examination and Production orders are powers available to the Serious Fraud Office (SFO) and under the Search and Surveillance Bill are to be extended to the Police. The former orders require people to answer questions about the information they hold and the latter orders require people to hand over documents in their possession, when being investigated for business crime punishable by five years or more and serious fraud punishable by seven years or more. Critics of these orders believe that it will pose a threat to media in that it could threaten the ability of the media to protect their sources.

This issue of media protection of sources was highlighted when the SFO used these powers on *The National Business Review* (NBR) – a weekly New Zealand newspaper aimed at the business sector – in 2010 to recover documents relating to stories printed in the NBR that covered the collapse of South Canterbury Finance. Initially the NBR resisted the move but was forced to comply when threatened with prosecution. This rather heavy handed approach by the SFO raises many ethical questions for the media because source confidentiality is one of the cornerstones of journalistic integrity.

Another, perhaps more worrying, additional power to be granted to state agencies when the Search and Surveillance Bill becomes law, is that of remote searching of computer networks, and web-based email accounts such as Gmail and Facebook. Co-founder of Internet group TechLiberty (a New Zealand group concerned about people's civil liberties in the digital world) Thomas Beagle, says that it is almost impossible to restrict computer searches to specific key words and those remote accessing computers have the potential to view a vast range of irrelevant private information (Cumming, 2010). Once again, this issue of privacy rights versus public interest will come down to a judicial balancing act.

8.5.1 Search and Surveillance law

The Search and Surveillance Bill passed into law in October 2012 and media were unable to secure an exemption from powers that would force them to reveal their sources. Justice Minister (2012) Judith Collins, assured the media that should they be presented with an examination or production order they did not wish to comply with (in terms of revealing sources), the information or document could not be viewed by the enforcing officer until a High Court judge decided if privilege applied or not (Young, 2012). The rhetoric from the Minister is lofty but will do little to reassure, if sources cannot be guaranteed confidentiality there will be little motivation to come forward and reveal that which needs public scrutiny.

8.6 Summary

The threat of terrorism and better ways to combat crime are often cited as reasons to push through legislation that increases the levels of surveillance over society. 'Tracking', both online and in reality, is a means, businesses say, of improving ways to target consumers. Media normalise surveillance through entertainment and the rise of tabloid journalism has meant getting the 'edge' on a story is often achieved through intrusive surveillance practices.

The new Surveillance Bill that passed into law in New Zealand in 2012 hopes to combat the most objectionable types of surveillance the public may use, while providing government agencies with more power to combat crime. However, certain aspects of the new law (such as the Examination and Production orders) worry those that believe media freedom is being compromised.

Chapter 9

CONCLUSION

Privacy, like beauty, has many definitions but few absolutes. Depending on your age, gender, ethnicity and socioeconomic background, the importance of privacy as a “right” and in need of protection will vary. That aside, and regardless of how much, or to what degree privacy is valued, it is a concept that is inherent in our western democratic way of life. The right to privacy needs to be acknowledged and balanced against other values in order to maintain and guard against an erosion of a system that, despite its many flaws, has proven to be a vehicle for human freedom.

In terms of the news media, balancing the right of privacy against that of the public’s right to know has often been a contentious issue and with the advent of digital technologies has been exacerbated. When the New Zealand Law Commission began its mammoth task of reviewing privacy law its members discussed the evolving nature of privacy over the last four centuries and asserted that privacy is a relatively modern notion that is directly linked to our social and technological advancement. In other words, as communal living declined and people chose a more separated existence, which technology paradoxically has both enhanced and diminished, they have come to value the notion of privacy as a legitimate and necessary ‘right’.

This thesis has examined how the advent of Internet based technologies has created new

ways in which the privacy of personal information is breached and responses to such breaches both here and abroad. This investigation of personal privacy issues was examined in light of the techno-legal time gap and ethico-legal paradoxes that result from digital privacy intrusion and the moral and legal complexities created by technologies that are outstripping our ability, and more often than not, our awareness, in being able to protect our informational privacy.

Informational privacy refers to the control we have over the access to private information about ourselves that one would *reasonably* expect to remain private within the context of how this information is gathered, used, stored and shared. Harms identified from the misuse of this information ranged from: identity theft; the news media's usage of social networking sites in reporting; tracking of online site visits; malicious posting of personal images; flouting of suppression orders; intrusive surveillance and a gradual erosion of civil liberties in the name of national security.

When viewing informational privacy issues in New Zealand it is important to note that these are global issues and the examples provided reflect this. In this sense, New Zealanders' experiences with privacy intrusion are very similar to what is happening overseas.

9.1 Public versus private

A public space is both physical and digital and events and information garnered from both spheres by the media in its news gathering activities have created tensions around privacy protection in public. The 2004 *Hosking v Runting* Court of Appeal judgment established that in New Zealand there is a right of action for the invasion of privacy. Television and radio host Mike Hosking sought the prevention of the publication of photos of his children taken in a public place on the grounds they invaded his children's right to privacy. In New Zealand jurisdiction there are allowances for an expectation of privacy in public; however, publicity given to those private facts must be considered highly offensive to an objective reasonable person before there is a breach. Hosking's case did not meet this requirement.

While social media sites such as Facebook have been deemed a public sphere, members of the New Zealand Law Commission noted in their Stage 4 *Review of the Privacy Act* (NZLC R123, 2011) that there was a need to amend some exemptions to the Act's privacy principles relating to the publication of personal information found online, in particular the posting of images without consent of the individuals concerned. Also noted was the fact that there was nothing in place to prevent further on-publishing.

The techno-legal time gap, defined by Hirst & Patching (2005) as the time it takes for legislation to regulate socially undesirable aspects of new media technologies was alluded

to by Law Commissioner Professor John Burrows, when he said that any review of privacy law must consider whether new technologies pose new threats to privacy. There is no question that with the advent of digital technologies, the publication and distribution of private information and images can cause significant distress. This was acknowledged by the Commission members when they recommended that an exemption in the Privacy Act that allowed people to collect or hold information in connection with a person's personal or domestic affairs should not apply if this collection and use thereof was "highly offensive". Furthermore, it was also recommended that an amendment should be put in place that prevented others from further using or disclosing such information.

Numerous ethico-legal paradoxes, once again defined by Hirst & Patching (2005) as the confusion which arises when action is morally right but legally wrong, or vice versa, have been created with the advent of new media, which can collide with privacy when freedom of speech is an issue. With the unprecedented amount of information that is posted online, traditional media has found its share of the market constantly under threat and in order to maintain its audience, journalists (but not limited to) have been known to resort to the unethical use of information obtained from the new media forum, under the guise of "public interest" stories.

Britain (the Leveson Inquiry), Australia (the Finklestein Report) and New Zealand (the Law Commission Issues paper on new media, NZLC IP27) have all been engaged in examining the effectiveness of their respective current media codes of practice - partly in light of the

new ways digital technologies have circumnavigated privacy and the ethics of publishing the information found there.

9.2 New media's right to reveal

On appearance at the Leveson Inquiry, former Deputy Features Editor for the now defunct British newspaper *News of the World* Paul McMullan, claimed that 'hacking' (illegal voicemail interception) was a widespread practice, and that the paper's audience were the ones to decide what the paper printed and, in the ultimate justification, commented that privacy was the space that bad people needed to do bad things in. Mr McMullan has defended the public's right to know with brutal pragmatism, in that, in his opinion, nearly all newspapers practice hacking, if the public did not like what they read they would not buy it and the desire for privacy suggests nefarious practices by those that seek it.

McMullan's defence of *News of the World* practices is, in my opinion, both faulty and of school-boy rationale. McMullan is not defending the public's right to know, McMullan is defending unethical, *illegal*, lazy journalism of the worst order – in short, he is defending his inability to recognise news of legitimate public concern.

The new media environment is one where the growth of consumption and participation in online news and the use of social media are unprecedented and, as such, the information

that becomes available through this medium has enormous economic and social benefits. However, this digital environment has created legal challenges, and one of the questions members of the New Zealand Law Commission queried was whether the courts were the best forum for resolving disputes between free speech and the right to privacy.

While opinion may be divided as to whether the establishment of a new tribunal or council to deal with the regulatory gaps and unethical practices created and perpetrated in the new media environment is the way forward (as opposed to a further threat to free speech), it is clear a new framework needs to be provided when considering new media, privacy and the public's right to know.

9.3 Contextual integrity

Helen Nissenbaum, Professor of Media, Culture and Communication at New York University, has provided a neat and elegant solution to privacy challenges created by digital technologies with her idea of contextual integrity (Nissenbaum, 2009). Nissenbaum believes that the public-private distinction is unhelpful when conceptualising a right to privacy and the emphasis should be on what constraints are imposed on flows of information, in the context of how the information was collected. Information revealed in a particular context, for example posting photos on a social media site, always bears the tag of that context, and if these images were then appropriated and used in a way that they were not intended to be used, contextual integrity has been breached.

Each context will have to be examined on its own merits as to what constitutes the 'norms' of that context. In other words, what is considered appropriate in governing the flow of personal information in one context will not necessarily be the same in another, when weighing up privacy intrusion. Nissenbaum acknowledges that while a justificatory framework for contextual integrity is developed to a certain point there is much work to be done by area experts, for example in government departments that gather information (such as in education, healthcare and social development) to articulate the norms associated within the context of their data gathering and possible data sharing, and make clear the reasoning for both.

When the contextual integrity framework is applied to the examples used in this thesis to illustrate informational privacy issues, it quickly becomes clear where privacy breaches have occurred. Obviously for this framework to become the 'norm' we must reject the notion that "privacy is dead" and "get over it" (quotes from Facebook founder Mark Zuckerberg and CEO of Sun Microsystems Scott McNealy respectively) and patronise only the institutions that adopt this model. And therein lays the heart of the matter, money versus morality; why would Facebook for example, adopt a contextual integrity framework when it has sold the idea of privacy as being outdated to its 800 plus million users?

9.4 Recommendations

I believe digital developers and programmers should collaborate in designing and constructing software that develops a formal expression (as in, encoding formulae that allows the sequencing of time and quantifiers) of contextual integrity and, this framework be adopted by all institutions that deal in the collection and sharing of information. Technological advancement is unstoppable but that does not mean ungovernable.

Furthermore, privacy is inextricably bound up with control – who controls what information as well as the constructs and dissemination of that information. For this reason alone, we as citizens must be vigilant in examining any legislation which contributes to the gradual erosion of control over our personal information. History is littered with examples of how badly it can go wrong when checks and balances to power are removed.

9.5 The future

Members of the New Zealand Law Commission noted at the start of their review of the Privacy Act that technological change had raised the salience of the privacy issue and, in particular, the emerging practices of surveillance. Former British Chief Information Commissioner, Richard Thomas, warned the British public that they were sleep walking into a surveillance society because of their government's plans to introduce identity cards and a population register. It appears that the United States and Britain (and to a lesser

extent New Zealand) are using the threat of terrorism as a reason to push through legislation that will give authorities greater access to our personal information.

Often this legislation is sold under the guise of the “nothing to hide, nothing to fear” argument, which is based on the dubious premise that privacy is *only* about hiding bad things, as opposed to privacy being about what *we choose* to reveal about ourselves. Privacy is intrinsic to the concept of democracy but, rightly, must be weighed up against news media’s right to reveal. This ‘right to reveal’ is the judgment made when publishing a story, in that it must be justified on the grounds it is newsworthy and in the public interest. Lord Justice Leveson, on opening the Leveson Inquiry into British media practices, stated that freedom of expression is fundamental to democracy and is an essential check on all aspects of public life, but at the heart of the inquiry was the question of who guards the guardians.

The advent of digital technologies has meant the sharing and use of personal information is a permanent feature in our lives. Former Google CEO Eric Schmidt commented that he did not believe society understands what happens when everything is available, knowable and recorded by everyone for all time. Only time and further research will determine whether current and future generations value the notion of privacy in a world where digital connectivity will be the norm – a society where perhaps we become the ‘watchers’ instead of the ‘guardians’.

BIBLIOGRAPHY

- About the Commission. (2011). Retrieved from <http://www.lawcom.govt.org/about>
- About Spokeo. (2011). Retrieved from <http://www.spokeo.com/blog/about>
- Akel, W. (2007). Privacy and the global media in the information age. *Pacific Journalism Review*, 13(1), p. 40-57. Retrieved from <http://www.pjreview.info>
- Aronson, K., & Sylvie, G., & Todd, R. (1996). Real-time journalism: Implications for news writing. *Newspaper Research Journal*, 17(3/4). Retrieved from <http://www.findarticles.com>
- Barker, Ian., & Evans, Lewis. (2007, November). *Review of the New Zealand Press Council*. Retrieved from http://www.presscouncil.org.nz/articles/press_council_review.pdf
- Barton, Chris. (2011, August 3). Privacy shakeup for the internet age. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Bartlett, Peter. (2011, May 9). Human headline – Name them and shame them. *Melbourne PressClub*. Retrieved from http://www.melbournepressclub.com/news/Human-headline-%E2%80%93-name-them-and-shame-them_09_05_2011
- Big brother set to get more snooping powers in UK. (2012, April 2). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Black, Joanne. (2008, October 4). Fair facts? *New Zealand Listener*. Retrieved from <http://www.listener.co.nz/uncategorized/fair-facts>
- Bloggers could face charges over trial. (2009, July 23). *ONE News*. Retrieved from <http://www.tvnz.co.nz/national-news/bloggers>
- Broadcasting Standards Authority. (2011). *BSA Annual Report 2010*. Retrieved from <http://www.bsa.govt.nz/assets/Annual-Reports/Annual-Report-2010.pdf>
- Bunting, Finbarr. (2010 July 25). Missing mum poses with All Blacks. *Sunday News*. Retrieved from <http://www.stuff.co.nz/sunday-news>
- Burrows, J.F., & Cheer, U. (2005). *Media law in New Zealand* (5th ed.). Auckland, New Zealand: Oxford University Press.
- Burrows, J. (2006). *A journalist's guide to the law* (5th ed.). Wellington, New Zealand: New Zealand Journalists Training Organisation.
- Burrows, John. (2011, August 2). *Privacy protection in a digital age*. [Press release]. Retrieved from http://www.lawcom.govt.nz/sites/default/files/press-release/2011/08/media_release_-_technology.pdf

- Cameron-Dow, J. (2009). The question of crime: How much does the public have the right to know? *Pacific Journalism Review*, 15(2), p. 71-84. Retrieved from <http://www.pjreview.info>
- Castells, M. (1996). *The rise of the networks society*. Oxford, England: Blackwell.
- Cause of death revealed in Carmen Thomas case. (2011, July 15). *Otago Daily Times*. Retrieved from <http://www.odt.co.nz>
- Censky, Annalyn. (2011, November 22). Malls track shoppers' cell phones on Black Friday. *CNN News*. Retrieved from <http://www.money.cnn.com>
- Cerf, V. G. (2004). Internet and the justice system. *Washington Law Review*, 79(2), p. 25-30. Retrieved from <http://www.law.washington.edu>
- Chapman, Glen. (2011, March 22). Twitter marks fifth birthday. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Chen, Mai. (2011, November 11). Privacy, intent and the teapot tape: four questions. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Cheng, D. (2010, November 5). Bill retains end to right of silence. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Cheng, D. (2010, December 7). Spooks at the Rugby World Cup. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Cheng, D. (2011, November 24). Police move in on teapot tape media. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Chung, W., & Paynter, J. (2002, January 7-10). Privacy issues on the internet. 35th HICSS Annual Conference. doi:10.1109/HICSS.2002.994191
- Citron, Danielle. (2010). Bright ideas: Helen Nissenbaum's privacy in context: technology, policy, and the integrity of social life. Retrieved from <http://www.concurringopinions.com/archives/2010/01/bright-ideas-helen-nissenbaums>
- Comedian's sentence overturned. (2012, April 18). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Coopes, Amy. (2010, December 2). Cybercrime 'worth more than illegal drug trade'. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Criminal Justice Act 1985. Retrieved from <http://www.legislation.govt.nz/act/public/1985/0120/latest/whole.html#DLM78869>
- Criminal Procedure Act 2011. Retrieved from <http://www.legislation.govt.nz/act/public/2011/0081/61.0/DLM3359962>

- Cumming, Geoff. (2010, December 4). You can't hide from prying eyes. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Cusick, James. (2011, December 1). Ex-reporter dishes dirt on 'scum' NOTW editors. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Davis, Glenn. (2011, May 22). *Scottish newspaper names Ryan Giggs as footballer who reportedly had an affair with Welsh model*. Retrieved from <http://www.sportsgrid.com/media/ryan-giggs-Sunday-herald-imogen-thomas/>
- Dearing, M. C. (1999). Personal jurisdictions and the internet: Can the traditional principles and landmark cases guide the legal system into the 21st century? *Journal of Technology Law & Policy*, 4(1), p. 1-16. Retrieved from <http://www.grove.ufl.edu/~/techlaw>
- Dudding, Alan. (2010, April 25). Beware the curse of Facebook. *Sunday Star Times*. Retrieved from <http://www.stuff.co.nz/sunday-star-times>
- Edwards, Brian. (2010, August 16). Jackie Sperling writes to Brian Edwards. [Web log post]. Retrieved from <http://www.brianedwardsmedia.co.nz/2010/08/jackie-sperling-writes-to-brian-edwards-media>
- Eldon, E. (2010, February 23). *Nielsen: Facebook led 2009 social media traffic growth in the US and abroad*. Retrieved from <http://www.insidefacebook.com>
- Elliot case reignites contempt debate. (2009, July 22). *ONE News*. Retrieved from <http://www.tvnz.co.nz/national-news/elliott-case-reignites-contempt-debate-2863125>
- Ellis, G. (2005). Different strokes for different folk: Regulatory distinctions in New Zealand media. *Pacific Journalism Review*, 11(2), p. 63-83. Retrieved from <http://www.pjreview.info>
- Evans, Katrine. (2004). Hosking v Runting balancing rights in a privacy tort. *Australasian Legal Information Institute*. Retrieved from <http://www.austlii.edu.au>
- Evans, Katrine. (2004, May). Was Privacy the winner on the day? *New Zealand Law Journal*, 4, p. 181-184. Retrieved from <http://www.lexisnexis.com.ezproxy.aut.ac.nz>
- Elvidge, A. (2008). *Trying times: The right to a fair trial in the changing media environment*. A dissertation submitted in partial fulfilment of the degree of Bachelor of Law (with Honours). Retrieved from <http://www.otago.ac.nz/law>
- Executive summary. (2007, December). Retrieved from <http://www.justice.govt.nz/publications/global-publications/t/the-experience-of-e-crime/executive-summary>
- Farber, D. (2002). Balancing security and liberty. *IEEE Internet Computing*, 5(6), p. 96-99. doi:10.1109/MIC.2001.968840

- Federal Trade Commission. (2011, November 29). *Facebook settles FTC charges that it deceived consumers by failing to keep privacy promises*. Retrieved from <http://www.ftc.gov/opa/2011/11/privacysettlemet.shtm>
- Fisher, David. (2010, August 22). Tracking the cyber footprint. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Flew, T., & McElhinney, S. (2002). Globalization and the structure of new media industries. In Leah Lievrouw & Sonia Livingstone (Eds), *The Handbook of New Media* London, England: Sage.
- Foley, Steven. (2011, July 2). Secret web trackers that know all about you. *Weekend Herald*. Retrieved from <http://www.stuff.co.nz/weekend-herald>
- Ford, Richard. (2004). Beware rise of big brother state, warns data watchdog. *The Times*. Retrieved from <http://www.timesonline.co.uk>
- Gay, E. (2010, May 25). Privacy Commissioner probing Google over data. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Ghazali, Cynthia. (2011, November 18). Facebook keeps tabs on users even after they sign off. *New York Daily Times*. Retrieved from <http://www.nydailynews.com>
- Golding, P., & Murdock G. (2002). Digital possibilities; market realities: the Contradictions of communications convergence. In Leo Patich & Colin Leys *Socialist Register*, (p. 111-129). London, England: Merlin.
- Goodman-Delahunty, J., & Rabone, S. (2005, October 7-9). Multimedia evidence and the jury: Applying principles of effective communication. *23rd AIJA Annual Conference*. Retrieved from <http://www.aija.org.au/ac05/papers.htm>
- Google Press Release. (2008, December 2). *Google street view launches in New Zealand*. Retrieved from <http://www.scoop.co.nz>
- Gower, P. (2009, November 17). Fame still grounds for suppression. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Gower, P. (2009, November 24). Secrecy can't hide name from PM. *The New Zealand Herald*. Retrieved from <http://www.nzherlad.co.nz>
- Graber, D. (2003). The media and democracy: beyond myths and stereotypes. *Annual Review of Political Science*, 6, p. 139-160. Retrieved from <http://www.polisci.annualreviews.org>
- Grow, Brian. (2011, January 27). *In U.S courts Facebook posts become less private*. Retrieved from <http://www.reuters.com/article/2011/01/27/us-facebbok-privacy-idUSTRE70Q7EG20110127>

- Greig, Sara. (2012, March 26). Alias frauds and identity theft keep on rising: Veda. *The National Business Review*. Retrieved from <http://www.nbr.co.nz>
- Grubb, Ben. (2011, May 18). *Security experts go to war: wife targeted*. Retrieved from <http://www.stuff.co.nz/technology/digital-living/5022035>
- Grubb, Ben. (2011, May 19). *Privacy, news and the strong arm of the law*. Retrieved <http://www.stuff.co.nz/technology/digital-living/5018637>
- Haines, R. (1996). The office and functions of New Zealand's privacy commissioner. *Government Information Quarterly*, 13(3), p. 255-274. Retrieved from <http://www.sciencedirect.com>
- Hans, V. P. (1990). Law and the media: an overview and introduction. *Law and Behavior*, 14(5), p. 399-407. doi:10.1007/BF01044219
- Harvey, Sarah. (2011, April 17). There are baddies out in cyberspace. *Sunday Star Times*, p. A9. Retrieved from www.stuff.co.nz/sunday-star-times
- Heuston, George, Z. (2011, January 28). Privacy concerns: from social media aggregation to aggravation. Retrieved from <http://www.oregonlive.com/argus/>
- Hickman, L. (2010, August 8). Every move you make. *Sunday Star Times*. Retrieved From <http://www.stuff.co.nz/sunday-star-times>
- Hirst, M., & Harrison, J. (2007). *Communication and new media: from broadcast to narrowcast*. Melbourne, Australia: Oxford University Press.
- Hirst, M., & Patching, R. (2005). *Journalism ethics: arguments and cases*. Melbourne, Australia: Oxford University Press.
- Holden, Michael. (2011, June 16). Juror jailed for contempt of court after using Facebook. Retrieved from <http://www.uk.reuters.com/article/2011/06/16/uk-britain-juror-idUKTRE75F22K20110616>
- Holman, W. Jenkins Jr. (2010, August 14). Google and the search for the future. Retrieved from <http://online.wsj.com/article>
- Hong, T., & McLaughlin, M.L., & Pryor, L. & Beaudoin, C., & Grabowicz, P. (2005). Internet privacy practices of news & implications for online journalism. *Journalism Studies*, 6(1), p. 15-28. doi:10.1080/1461670052000328177
- Horowitz, D. J. (2004). Technology, values and the justice system: the evolution of the access to justice technology bill of rights. *Washington Law Review*, 79(77), p. 77-104. Retrieved from <http://www.law.washington.edu>
- Hull, D. (2007). Blogging between the lines. *American Journalism Review*, p. 63-67. Retrieved from <http://www.ajr.org>

- Ihaka, James. (2010, August 28). Postie fired for critical Facebook comments. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Jackson, Nicholas. (2011, July 2). Infographic: who is using Twitter, how often, and why? *The Atlantic*. Retrieved from <http://www.theatlantic.com/technology/archive/2011/07/Infographic-who-is-using-twitter-how-often-and-why/241407/>
- Jenness, V., Smith, D.A., Stepan-Norris, J. (2007, March). Editor's Note: Taking a look at Surveillance studies. *Contemporary Sociology: A Journal of Reviews*, 36, vii. doi: 10.117/009430610603600201
- Jolly, David. (2010, August 26). German law would limit Facebook's use in hiring. *New York Times*. Retrieved from <http://www.nytimes.com/2010/08/26/business/global/26fbbook.html>
- Judge calls bluff. (2010, July 10). *Weekend Herald*, p. B3. Retrieved from <http://www.herald.co.nz>
- Key Recommendations. (2011, August 2). Retrieved from http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/key_recommendations_-_for_report_release.pdf
- Kohm, Steven, A. (2009). Naming, shaming and criminal justice: mass-mediated humiliation as entertainment and punishment. *Crime, Media, Culture*, 5, p. 188-205. doi:10.1177/1741659009335724
- Koubaridis, A. (2010, July 8). Angry couples use Facebook in court. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Koubaridis, A., & Gay, E. (2011, September 3). Outrage at comedian's sex abuse discharge. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Koubaridis, A. (2011, November 30). Ex-All Black's child assault secrecy. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Krebs, J. (2009 March 2). *Suppressing names and evidence*. Retrieved from <http://www.lawsociety.org.nz>
- Lanier, Jaron. (2010). *You are not a gadget*. New York, NY: Radom House
- Law Commission Act. (1985). Retrieved from <http://www.legislation.govt.nz/act/public/1985/0151/latest/DLM85588.html>
- Leach, J. (2009). Creating ethical bridges from journalism to digital news. *Nieman Reports*. Retrieved from <http://www.nieman.harvard.edu>
- Leask, Anna. (2009, July 19). Blogger retreats over contempt worry. *Herald on Sunday*. Retrieved from <http://www.nzherald.co.nz>

- Lederer, F., & Hulse, R. (2008). Impractically obscure? Privacy and courtroom proceedings in light of webcasting and other new technologies. *Journal of Technology Law & Policy*, 41(3), p. 10-51. Retrieved from <http://www.grove.ufl.edu/~techlaw>
- Legal challenges over new media. (2009, July 13). *ONE News*. Retrieved from <http://www.tvnz.co.nz/national-news/legal-challenges-over-new-media-2840409>
- Leveson, Brian. (2011, November 14). *Transcript of morning hearing*. Retrieved from <http://www.levenoninquiry.org.uk/wp-content/uploads/2011/11/Transcript-of-Morning-Hearing-14-November-2011.pdf>
- Litman, J. (2000). Information privacy/information property. *Stanford Law Review*, 52(5), p. 1283-1313. doi:10.2139/SSRN.218274
- Malhotra, N.K., & Sung, S.K., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a casual model. *Information Systems Research*, 15(4), p. 336-355. Retrieved from <http://www.isr.journal.informs.org>
- Macdonald, Finlay. (2009, November 22). Suppression proves not all publicity good. *Sunday Star Times*. Retrieved from <http://www.stuff.co.nz/sunday-star-times>
- McSoriley, John. (2011, June 17). *Search and Surveillance Bill 2009 (2010 No 45-2)* Retrieved from <http://www.parliament.nz/en-NZ/PB/Legislation/Bills/BillsDigest/5/f/a/49PLLawBD18791-Search-and-Surveillance-Bill-2009-2010-No-45-2-Bills>
- Milne, R. (2009, July 12). Trial commentators under scrutiny. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Mitchell, M. (2009, March 16). Name suppression rules need changing – lawyers. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Moor, J.H. (2004). Towards a theory of privacy in the information age. In T.W. Bynum & S. Rogerson (Eds.) *Computer ethics and professional responsibility* (pp. 249-262). Oxford, England: Blackwell Publishing
- Moreham, N. (2009). *Private matters: A review of the privacy decisions of the Broadcasting Standards Authority*. Retrieved from <http://www.bsa.govt.nz/private-matters-a-review-of-the-privacy-decisions-of-the-broadcasting-standard-authority>
- Morozov, Evgeny. (2010, May/June). Speak, memory. *Boston Review*. Retrieved from <http://www.bostonreview.net/BR35.3/morozov.php>
- Morozov, Evgeny. (2011). *The Net Delusion*. New York, NY: PublicAffairs.
- Murray, Paula. (2009, March 8). Anniversary shame of Dunblane survivors. *Scottish Sunday Express*. Retrieved from <http://www.jammus.posterous.com/anniversary-shame-of-dunblane-survivors-full>

- Naked photo sends jilted lover to jail. (2010, November 13). *The Dominion Post*. Retrieved from <http://www.stuff.co.nz/dominion-post>
- Name suppression: new laws won't protect famous. (2010, October 5). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- New Zealand Law Commission. (2007). (NZLC R97). *Search and surveillance powers*. Retrieved from http://www.lawcom.govt.nz/sites/default/files/publications/2007/06/Publication_96_358_Part_1_R97%20part_1.pdf
- New Zealand Law Commission. (2008). (NZLC IP13). *Suppressing names and evidence*. Retrieved from http://lawcom.govt.nz/sites/default/files/publications/2008/12/Publications-149_423_SupNames%20WebV%20-%20Issues%20Paper%2013pdf
- New Zealand Law Commission. (2008). (NZLC SP19). *Privacy concepts and issues*. Retrieved from http://www.lawcom.govt.nz/project/review-privacy?quicktabs_23=study_papers#-703
- New Zealand Law Commission. (2009). (NZLC R109). *Suppressing names and evidence*. Retrieved from http://www.lawcom.govt.nz/sites/default/files/publications/2009/11/Publication_149_453_R109.pdf
- New Zealand Law Commission. (2010). (NZLC IP17). *Review of the Privacy Act 1993*. Retrieved from http://www.lawcom.govt.nz/project/review/privacy?quicktabs_23=issues_paper#node-773
- New Zealand Law Commission. (2010). (NZLC R113). *Invasion of Privacy: Penalties and remedies*. Retrieved from http://www.lawcom.govt.nz/sites/default/files/publications/2010/02/Publications_129_457_R113pdf
- New Zealand Law Commission. (2011). (NZLC R123). *Review of the Privacy Act 1993: Review of the law of privacy stage 4*. Retrieved from http://www.lawcom.govt.nz/project/review-privacy?quicktabs_23=report#node-2123
- New Zealand Law Commission. (2011). (NZLC IP27). *The news media meet 'new media'*. Retrieved from <http://www.lawcom.govt.nz/sites/default/files/publications/2011/12/ip27-all-web-v2.pdf>
- New Zealand Law Commission. (2011, December 12). *Review of regulatory gaps and The new media*. Retrieved from http://www.lawcom.govt.nz/project/review-regulatory-gaps-and-new-media?quicktabs_23=issues_paper#quicktabs-23
- New Zealand Ministry of Justice. (n.d.). *Conviction and sentencing of offenders in New Zealand: 1997 to 2006*. Retrieved from <http://www.justice.govt.nz/publications/c/conviction-and-sentencing-of-offenders-in-new-zealand-1997-to-2006/4-custodial-sentences-and-remands>

- New Zealand Ministry of Justice. (2008, October). *Media guide for reporting the courts*. Retrieved from <http://www.justice.govt.nz/media/media-information/media/documents/Media-Guide-FINAL-20081003.pdf>
- New Zealand Newsletter. (2009). Retrieved from <http://www.hitwise.com.news/nz/200907.html>
- New Zealand Office of the Privacy Commissioner. (2010). *Annual report 2010*. Retrieved from <http://www.privacy.org.nz/assests/Files/Reports-to-ParlGovt/OPC-Annual-Report-2010.pdf>
- New Zealand Office of the Privacy Commissioner. (2010, June 14). *Submission by the Office of the Privacy Commissioner on the Law Commissions' review of the Privacy Act 1993: Stage 4*. Retrieved from <http://www.privacy.org.nz/new-zealand-law-commission-privacy-review>
- New Zealand Office of the Privacy Commissioner. (2010, May 23). *New UMR privacy Survey results* [Media release]. Retrieved from <http://www.privacy.org.nz/media-release-new-umr-privacy-survey—results>
- New Zealand Office of the Privacy Commissioner. (2010, September 8). *New powers to block re-export of personal information* [Media release]. Retrieved from <http://www.privacy.org.nz/media-release-new=powers-to-block-re-export-of-personal-information>
- New Zealand Office of the Privacy Commissioner Inquiries. (2010, December 14). *Google's collection of WiFi information during street view filming*. Retrieved from <http://www.privacy.org.nz/google-s-collection-of-wifi-information-during-street-view-filming>
- New Zealand Press Council. (2008, September). *Case Number: 2048 Graeme Hart against Herald on Sunday*. Retrieved from http://www.presscouncil.org.nz/display_ruling.php?case_number=2048
- New Zealand Press Council. (2010, December). *Case Number: 2166 Gen O'Halloran against New Zealand Herald*. Retrieved from http://www.presscouncil.org.nz/display_ruling.php?case_number=2166
- New Zealand Press Council. (2010). *Annual Report 2010*. Retrieved from <http://www.presscouncil.org.nz/articles/NZ%20Press%20Council%20Annual%20Report%202010.pdf>
- New Zealand Press Council. (2011, February). *Case Number: 2173 Aparangi Hemara against Herald on Sunday*. Retrieved from http://www.presscouncil.org.nz/display_ruling.php?case_number=2173
- Nissenbaum, Helen. (2009). *Privacy in context: technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

- O'Brien, Terrence. (2010, January 11). *Facebook's Mark Zuckerberg claims privacy is dead*. Retrieved from <http://www.switched.com/2010/01/11/facebooks-mark-zuckerberg-claims-privacy-is-dead>
- O'Carroll, Lisa. (2012, May 12). Leveson inquiry: make political lying a criminal offence says Peter Osborne. *The Guardian*. Retrieved from <http://www.guardian.co.uk>
- Opsahl, Kurt. (2010, April 28). *Facebook's eroding privacy policy: A timeline*. Retrieved from <http://www.eff.org/deeplinks/2010/04/facebook-timeline>
- Palmer, Geoffrey, Rt Hon Sir. (Ed). (2007). *Reflections on the New Zealand Law Commission: Papers from the twentieth anniversary seminar*. Wellington, New Zealand: LexisNexis.
- Palmer, Geoffrey., Rt Hon Sir. (2009, November 16). *Release of Law Commission Report: Suppressing names and evidence*. [Media release]. Retrieved from http://www.lawcom.govt.nz/sites/default/Files/press-releases/2009/11/Publication_149_454_PR%20Suppressing%20Names%20and%20Evidence%2016112009.pdf
- Palmer, Geoffrey., Rt Hon Sir. (2010, February 26). *Privacy report*. [Media release]. Retrieved from <http://www.lawcom.govt.nz/media/press-release/2010/invasion-privacy-penalties-and-remedies-review-law-privacy-stage-3>
- Pearson, M. (2007). A review of Australia's reforms after a year of operation. *Australian Journalism Review*, 29(1), p. 41-51. Retrieved from <http://epublications.bond.edu.au>
- Perlmutter, D., & Schoen, M. (2007). "If I break a rule, what do I do, fire myself?" Ethics codes of independent blogs. *Journal of Mass Media Ethics*, 22(1), p. 37-48. Retrieved from <http://www.inforaworld.com>
- Porteous, D. (2009, July 14). Contempt fear prompts comment removal. *Otago Daily Times*. Retrieved from <http://www.odt.co.nz>
- Press Complaints Commission. (2009). *Ms Mullan, Mr Weir & Ms Campbell*. Retrieved from <http://www.pcc.org.uk/news/index.html?article=NTc%Mw>
- Price, S. (2007). *Media minefield: a journalists' guide to media regulation in New Zealand*. Wellington, New Zealand: New Zealand Journalists Training Organisation.
- Price, S. (2008, May 28). Review of review of the law of privacy. (Web log message). Retrieved from <http://www.medialawjournal.co.nz>
- Price, S. (2009, July 12). Not quite...(Web log message). Retrieved from <http://www.medialawjournal.co.nz>
- Price, S. (2009, October 21). What's wrong with trial by media? (Web log message). Retrieved from <http://www.medialawjournal.co.nz>

- Price, S. (2009, November 29). Fact suppression. (Web log message). Retrieved from <http://www.medialawjournal.co.nz>
- Price, S. (2010, September 15). A whale of a decision. (Web log message). Retrieved from <http://www.medialawjournal.co.nz>
- Privacy Act 1993. Retrieved from <http://www.legislation.govt.nz/public/1993/0028/latest/DML296639.html>
- Questions and Answers. (2011). Retrieved from Http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/questions_and_answers_-_for_report_release.pdf
- Quill, J. (2008, August 7). Privacy laws that muzzle the media aren't in the public interest. *The Australian*, p. 32. Retrieved from <http://www.theaustralian.com.au>
- Review of regulatory gaps and the new media. (2010, October 19). Retrieved from http://www.lawcom.govt.nz/projects/review-regulatory-gaps-and-new-media?quicktabs_23=general#node-2043
- Riski, R.J., & Grusin, E. (2003). Newspaper's naming policy continues amid controversy. *Newspaper Research Journal*, 24(4), p. 64-76. Retrieved from <http://www.findarticles.com>
- Robert Half NZ Ltd. (2011, April 5). *Don't friend the boss* [Media release]. Retrieved from <http://www.roberthalf.co.nz/media-releases>
- Roberts, J. V., & Doob, A. N. (1990). New media influences on public views of sentencing. *Law and Human Behavior*, 14(5), p. 451-468. doi:10.1007/BF01044222
- Rosen, R.E. (1990). Liberal battle zone and the study of law and the media. *Law and Behavior*, 14(5), p. 511-521. doi:10.1007/BF01044
- Sabbagh, D. (2007, March 9). What interests the public is not always in the public interest. *The Times*, p. 61. Retrieved from <http://www.thetimes.co.uk>
- Samson, A. (2005). Unchallenged bible of NZ media law. *Pacific Journalism Review*, 11(2), 249-253. Retrieved from <http://www.pjreview.info>
- Search and Surveillance Bill 2009. (2010 No 45-2). Retrieved from <http://www.parliament.nz/en-NZ/PB/Legislation/Bills/BillsDigests/5/f/a/49PLLawBD18791-Search-and-Surveillance-Bill-2009-2010-No-45-2-Bills>
- Shroff, M. (2009, August 25). *Linking intelligence to provide value: Personal information, privacy and the information century*. Retrieved from <http://www.privacy.org.nz/speeches-presentations-article>
- Slater guilty of suppression breaches. (2010, September 14). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>

- Smith, Sydney. (2010, October 15). Danish Press Council bans reporting from Facebook accounts with friends only setting. *iMediaEthics*. Retrieved from http://www.imediaethics.org/index.php?option=com_news&task=detail&id=1022
- Solove, Daniel (2004). *The digital person: technology and privacy in the information age*. New York, NY: NYU Press.
- Solove, Daniel. (2007). *The future of reputation: gossip, rumour, and privacy on the Internet*. New Haven, CT: Yale University Press.
- Spiegel Online. (2010, August 19). *Google cannot allow itself to make any further mistakes*. Retrieved from <http://www.spiegel.de/international>
- Sprenger, Polly. (1999, January 26). *Sun on privacy: 'Get over it'*. Retrieved from <http://www.wired.com/politics/law/news/1999/01/17538>
- Stanfield, A. (1998). Cyber courts: Using the internet to assist court processes. *Computer Networks & ISDN Systems*, 30(1-7), p. 559-567. Retrieved from <http://www.science.direct.com>
- Stepniak, D. (2005, October 7-9). Court tv coming to an internet browser near you. *23rd AIJA Annual Conference*. Retrieved from <http://www.aja.org.au/ac05/papers.htm>
- Stewart, Cameron. (2012, March 10). Finkelstein report: Media's great divide. *The Australian*. Retrieved from <http://www.theaustralian.com.au>
- Submissions on SIS bill to be heard in secret – Key. (2010, December 6). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Suppression breach accused blogger to defend charges. (2010, January 5). *Sunday Star Times*. Retrieved from <http://www.stuff.co.nz/sunday-star-times>
- Sutton, M. (2010, July 18). Students face harsh lesson for web abuse. *Sunday Star Times*. Retrieved from <http://www.stuff.co.nz/sunday-star-times>
- Taylor, J. (2010, August 18). *Google boss Eric Schmidt's warning over online privacy*. Retrieved from <http://www.belfasttelegraph.co.uk>
- The Leveson Inquiry. (n.d). *Leveson Inquiry: culture, practice and ethics of the press*. Retrieved from <http://www.levesoninquiry.org.uk>
- Thussu, D.K. (2000). *International communication: Continuity and change* (1st ed.). London, England: Hodder Arnold.
- UMR Omnibus Results. (2010, March). *Individual privacy & personal information*. Retrieved from <http://www.privacy.org.nz/assets/Files/surveys/Privacy-survey-2010.pdf>

- Valdes, Manuel. (2012, March 9). Request for Facebook passwords sparks probe. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Verkaik, Robert. (2008, July 11). Mother sues over tale of 'drunken party' lifted from Bebo. *The Independent*. Retrieved from <http://www.independent.co.uk>
- Watchdog wants law expanded to protect people from prying eyes. (2010, February 27). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Weatherston did not get fair trial, court told. (2011, April 6). *Dominion Post*. Retrieved from <http://www.stuff.co.nz/dominion-post>
- Whale Oil blogger loses High Court appeal. (2011, May 11). *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>
- Wilkin, P. (2001). *The political economy of global communication: An introduction*. London, England: Pluto Press.
- Wood, J.J. (2009, August 17). *An imperfect thing: the media's influence on justice*. Retrieved from <http://www.salient.org.nz>
- Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., De Hert, P., Wadhwa, K., & Bigo, D. (2010). Sorting out smart surveillance. *Computer Law & Security Review* 26, p. 343-354. doi:10.1016/j.clsr.2010.05.007
- Wright, R. (2010, October 5). Fame isn't enough – govt to amend name suppression. TV3. Retrieved from <http://www.3news.co.nz>
- Yarrow, J., & K, Angelova. (2010, January 7). *YouTube's staggering growth continues*. Retrieved from http://www.articles.businessinsider.com/2010-01-07/tech/29962741_1_video-views-total-views-videos-people
- Young, Audrey. (2012, March 23). Labour fails to change search bill. *The New Zealand Herald*. Retrieved from <http://www.nzherald.co.nz>