Dale Stephens

THE INTERNET AND CONSUMER PRIVACY - SHOPPING BASKET OR TOO HARD BASKET.

LLM RESEARCH PAPER

LAWS 532: CONSUMER LAW

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA
UNIVERSITY OF WELLINGTON

2014

Contents

Abstract

The Internet has rapidly become the world's most prevalent form of communication. It can be accessed twenty-four hours a day from virtually any location in the world from a myriad of technologically savvy devices. Internet users can keep up to date with world events, watch movies, listen to music, interact with government agencies, analyse business trends, undertake research and maintain contact with people anywhere. The Internet also provides the ability for users to shop 'online' with virtually any product or service supplier anywhere in the world. This has created concerns regarding the use of personal information obtained through the medium of the Internet. An individual's right to privacy is a right enshrined in legislation and through tort law. With the uptake of technology and the burgeoning use of the Internet the subject of online privacy has become a complex issue for law and policy makers both in New Zealand and internationally. The aim of this paper is to look at the online shopper or consumer and how their information could be protected. This paper looks at the key areas of privacy legislation, the storage of data and the rise of new technologies including 'cloud' computing and suggests that the complexity of online privacy is such that a different approach to access and use of personal information of online shoppers may be required. The rate of technology change, the enormity of the data capture situation and the international accessibility of the Internet are all factors that create an almost impossible situation for ensuring consumer privacy so this paper proposes that the onus moves away from the law and policy makers and put into the hands of the users of the Internet.

Word length

The text of this paper (excluding abstract, table of contents, footnotes and bibliography) comprises 7533 words.

Subjects and Topics

Privacy Legislation
Data Collection
Cloud computing and new technology
Privacy of personal information

I Introduction

New Zealanders go 'online' to complete banking transactions, make requests of government agency's, interact with friends, to watch movies, to listen to music, to participate in online games, to research, follow world events and to shop. There are daily accounts of politicians, business people, celebrities and citizens complaining about the use and misuse of personal information, communications or data accessed via the Internet. New Zealand's 2014 general election campaign has seen major concerns regarding the misuse of potentially illegally obtained information via electronic means.

Societal interactions are changing with traditional methods declining in favour of online processes. The increasing affordability and availability of user-friendly devices facilitating access to the Internet means that anyone can access online information with ease. According to a recent news report:

> "The Internet is where we keep our stuff. Good, bad and neutral - it's all there, either shared with friends or kept between ourselves and our dearest Facebook advertisers, and data harvesters. It's where we keep our lists of ideas, our pictures, our music libraries. It's a living room, a library and a rogues' gallery of everyone we've ever met that we can access from our pants pockets, sometimes by mistake."[1]

New Zealand's General Election has seen issues of online privacy to the fore with claims and counter claims as to the legality or otherwise of information obtained online. An interesting area of discussion became the extent to which online data of private citizens and organisations could be hacked and used illegally. As stated by New Zealand Herald columnist Fran O'Sullivan –

[1] ALEXANDRA PETRI "The worst response to the nude celebrity photo hack" *Stuff.co.nz* (8 September 2014) <http://www.stuff.co.nz/life-style/life/10471692/The-worst-response-to-the-nude-celebrity-photo-hack>.

"Cyber attack is a major concern for New Zealand companies. In the Herald's Mood of the Boardroom election survey, chief executives rated the risk of cyber attacks among their top three international business concerns".[2]

And further

"The possibility of intellectural property being stolen is why economic and business drivers now come under the national security umbrella".[3]

This national security umbrella however doesn't extend to individual consumers who routinely use the Internet to shop for goods and services for their personal use. Online shopping is an area of rapid growth where consumers can purchase goods and services from anywhere in the world. The Dominion Post newspaper recently reported that (New Zealanders) online shopping has grown by 7% in the last year with purchases from domestic sites at 59% and from international sites has grown to 41% of total sales.[4] The exponential growth of use of the Internet has led to increased concerns regarding the privacy of individual citizens personal information. According to Solove, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] What is the role of the law in protecting personal information?

Solove further asserts that the public is reportedly as concerned about their privacy being threatened as much by business interests as by their government.[6]

In Norman Witzleb's book '*Emerging Challenges in Privacy Law'* Robert Gellman says about privacy that:

"Lawyers, judges, philosophers, and scholars have attempted to define the scope and meaning of privacy, and it would be unfair to suggests that they have failed. It would be kinder to say that they have all produced different answers."[7]

---

[2] "Fran O'Sullivan: Key wins - now let's focus on real issues" *New Zealand Herald* (17 September 2014) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11325841>.

[3] "Fran O'Sullivan: Key wins - now let's focus on real issues", above n 2.

[4] MICHAEL FOREMAN "Offshore retailers gain online marketshare" *Stuff.co.nz* (New Zealand, 1 September 2014) <http://www.stuff.co.nz/business/industries/10447282/Offshore-retailers-gain-online-marketshare>.

[5] Daniel J Solove *Privacy, information, and technology* (Aspen Publishers, New York, 2006) at 36.

[6] At 54.

In our daily interactions on the Internet we (sometimes unknowingly) release information about ourselves and our 'transactions on to the Internet. This information is then potentially used in a number of ways. Internet users receive unprompted emails from companies selling products. Banner advertisements on consumers Facebook or email home pages just happen to be promoting products of relevance to the consumer. Free offer promotions arrive at the consumers' 'home pages'. One such method is where information previously obtained by organisations is used to 'target' consumers with marketing opportunities to enable businesses to sell their products. This compilation and use of personal information according to Solove (and others) is known as '*database marketing*'[8] and provides immense marketing opportunities for business interests. Data collection techniques include often used online tools such as 'cookies', 'web bugs', 'spyware', and 'RFID' tags. Solove quotes, "According to Jerry Kang, the problem with data collection and compiling is that it is a form of surveillance that inhibits individual freedom of choice."[9] So do consumers who use the Internet as a means of transacting retain the freedom of choice as to who has access to their personal information?

The rapid uptake in use of the Internet has spawned a range of issues for law and policy makers. Chief amongst these issues is whether individual rights to privacy of their personal information can be appropriately safeguarded. The issue of online privacy is enormous and requiring of careful analysis. The purpose of this paper is to look at the rights of the online shopper only and consider whether their privacy needs are being met; are able to be met; or can not be appropriately met. To do this appropriately requires a range of comparisons with other activities occurring via the Internet so an understanding of their information privacy issues can be gleaned. This in turn can inform consideration of options for the best means of protecting the privacy of the online shopper or consumer.

The first consideration will be of the current legislation and how this assists in providing clarity on the privacy laws of New Zealand. Comparing the current New Zealand legal situation to that of near neighbours Australia, and the initiatives they

---

[7] Normann Witzleb *Emerging challenges in privacy law* (Cambridge University Press, New York, 2014) at 1.

[8] Solove, above n 5, at 185.

[9] At 193.

are implementing may provide an insight into what could be considered in the New Zealand legal context.

The second consideration will be data collection, how it takes place, how data is stored, distributed and used, and whether the current environment is helpful or otherwise to the consumers' privacy rights.

The third consideration will be a review of current technology, future opportunities and how we can work with the increasingly complex technology environment to assist the consumer with protecting their private information.

Finally consideration will need to be given to the practicalities of the current situation and future opportunities and what is the best way forward in the current and future environments for the New Zealand online consumer.

II New Zealand Privacy Law and the Internet

For privacy law to be effective it needs to have considered and understood the nature of privacy problems. In another of Solove's writings he states that, "the law struggles with comprehending how and why privacy problems cause injury."[10] This injury can be physical, financial, emotional, psychological, property, relational, and reputational. Therefore the law needs to understand both the problem and the effect.

New Zealand has no Internet privacy law as such, relying on the provisions of the Privacy Act 1993,[11] and the tort of invasion of privacy[12]. Information Privacy Principles 3 and 9 of the Privacy Act specifically deal with the collection and retention of information but as Corbett argues this has little effect with online privacy due to the domestic nature of the Act.[13] An online search of New Zealand legislation highlighted 65 references to online activity in a range of Acts thus highlighting the complexity of this situation, as there is no definitive legal direction as to the privacy of an individual's information on the Internet. Neither the OECD Privacy Guidelines

[10] Daniel J Solove *Understanding privacy* (Harvard University Press, Cambridge, Mass, 2008) at 174.

[11] Privacy Act 1993 Information Privacy Principles 3 and 6

[12] Susan Corbett "The retention of personal information online: A call for international regulation of privacy law" (2013) 29 Computer Law & Security Review 246 at 248.

[13] At 248.

nor the APEC Privacy Framework[14] include regulations requiring the deletion of personal information. Different countries throughout the Asia Pacific region have markedly different guidelines for the handling of personal information with some being very prescriptive but in the main the issue of online privacy throughout Asia Pacific is given low priority.

According to Mills "Control of personal information is the least developed sphere of privacy and the sphere with the least legal protection". [15] And -

> "Further modern technology makes this information easier to collect, easier to collate and file, and easier to disseminate. Both governmental and private entities use "data mining" for purposes ranging from advanced security to commercial gain. Thus, the level of control an individual may exercise of personal information inevitably conflicts with security and commercial interests. The need for some form of balancing becomes crucial to individual privacy concerns."[16]

Internationally there are no standards in place for the protection of an individual's personal information and there seems little appetite for achieving this. This could suggest that it's seen as too late to implement a meaningful privacy regime. More accurately it could be that there is no will to find a common solution because the question is too complex, expensive and time consuming.

Privacy commissioners worldwide are working to address legal issues surrounding privacy. As an example Asia-Pacific Economic Cooperation (APEC) member countries have established the APEC cross-border Privacy Enforcement Arrangement to assist privacy regulators to share information and assist each other in enforce laws in cross-border situations.[17]

Susan Corbett in her paper on "The retention of personal information online" comments that New Zealand's current privacy legislation only covers data or information emanating from New Zealand based sources and doesn't comply with European Union standards[18] which is therefore limiting New Zealand's trading

---

[14] At 247.

[15] Jon L Mills *Privacy* (Oxford University Press, Oxford [UK] ; New York, 2008) at 16.

[16] At 18.

[17] Witzleb, above n 7, at 43.

[18] Corbett, above n 12, at 249.

opportunities with Europe. She also believes that New Zealand's trading opportunities will continue to be limited due to domestic privacy legislation inadequately addressing the issue of data retention.[19] For New Zealand to be successful international trading partners the issue of data retention and access to private records needs to be clarified.

New Zealand's nearest neighbour Australia is currently reviewing its privacy legislation. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 came into force on 12 March 2014 and "constitutes the first step in a long and complex process to ensure that privacy remains both relevant and up to date in a changing world."[20]

From 2006 to 2008 the Australian government, via the Australian Law Reform Commission (ALRC) conducted a review of Australia's privacy framework and concluded that Australians care deeply about privacy – that they want a simple but workable system. It also found that Australians also want the "considerable benefits of the information age, such as shopping and banking online, and communicating instantaneously with friends and family around the world."[21] The work of the ALRC resulted in 295 recommendations for reform to the Australian privacy regime. These recommendations were dealt with in two stages leading up to the new legislation released this year. Of key importance is that the two previous sets of privacy principles, one for the public sector and one for the private sector, have now been replaced with one unified set of privacy provisions. These provisions now contain a number of significant changes in the areas of direct marketing and cross border information flows. This has ultimately also led to Australia's Privacy Commissioner having an enhanced range of powers including the Commissioner's ability to conduct a Performance Assessment of private sector organisations to determine how personal information is being handled under the new rules and codes.

Much of the work completed to date in Australia is considered the 'first stage' of the overhaul of privacy laws. The second stage will include data breach notifications, specifically relevant with the rapid technological advances creating massive data storage capability.[22] Currently the Australian Privacy Act does not make a distinction

[19] At 249.

[20] Witzleb, above n 7, at 31.

[21] At 33.

[22] At 44.

between data controller and data processor, leaving the issue of who 'holds' or 'controls' personal information as a question of fact to be determined on a case-by-case basis.[23] How this settles will only become clear as the new legislation is tested.

There are 13 new Australian Privacy Principles or APPs promulgated in this legislation replacing the two previous separate groups of private and public sector privacy principles. The new APPs can be divided into five categories of principles –

1. Organisations being required to consider the privacy of personal information when designing information systems (1,2)
2. The receipt of personal information including the receipt of unsolicited information by organisations (3,4,5)
3. Governance of the use and disclosure of personal information including direct marketing, use of government related identifiers and disclosure of personal information to recipients outside Australia (6,7,8,9)
4. The integrity quality and security of personal information (10,11)
5. Requests for access to and correction of personal information (12,13)[24]

The principle most relevant to consideration of the privacy of consumer information is the new privacy legislation principle known as Australian Privacy Principle number seven or APP 7. This APP creates certain conditions by which personal information can be used for direct marketing. The principle states:

> "If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing."[25]

The statute goes on to include a range of situations where personal information, not being sensitive information, can be used for the purposes of direct marketing. Most importantly for the individual item 7.6 of APP 7 provides the ability for an individual to request not to receive direct marketing communications. As stated by Witzleb - "The conditions are complex and their effect uncertain, although the intention is to

[23] At 48.

[24] Ben Allen and Hamish McNair "Reforms to Australian privacy legislation will have major impact for both public and private sector" (2012) 64 Keeping Good Companies (14447614) 690.

[25] c=AU; o=Commonwealth of Australia; ou=Attorney-General's Department; ou=Office of the Australian Information Commissioner "Privacy fact sheet 17: Australian Privacy Principles Office of the Australian Information Commissioner - OAIC" <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>.

ensure that, in most circumstances, individuals are offered an 'opt-out' opportunity, and that their choices must be respected".[26]

This new legislation has not been 'tested' yet but it is hoped that this new principle may have struck the right balance to please consumers and suppliers. As stated by Allen and McNair –

> "The Act also introduces an APP specifically dealing with direct marketing (APP 7) which requires greater accountability from organisations to record the source of personal information used for direct marketing. APP 7 also enables individuals to request an organisation not to use or disclose their personal information to facilitate direct marketing by other organisations. Organisations that presently disclose customer data to, or receive customer data from, other organisations, will need to carefully review their practices to ensure compliance."[27]

Australia has completed extensive research and analysis of its privacy legislation and now is in the process of implementing the amended Privacy Act. The next period may well see extensive 'testing' of this legislation as businesses, organisations, government agencies and private consumers work to understand how this legislation applies to them.

By way of contrast New Zealand has the Privacy Act 1993 which was most recently reviewed in 2011. In this review the authors looked at the 12 privacy principles contained in the original legislation and recommended that the basic structure of all of the principles remain unchanged.[28]

As a brief summary of New Zealand's Privacy Principles –

- Principles 1 – 4 cover the collection of personal information
- Principle 5 relates to the storage and security of information
- Principle 6 deals with an individual's ability access to personal information about them that has been stored by an agency
- Principles 7 – 8 pertain to the correction and accuracy of personal information

[26] Witzleb, above n 7, at 53.

[27] Allen and McNair, above n 24, at 691.

[28] New Zealand *Review of the Privacy Act 1993 review of the law of privacy, stage 4* (Law Commission, Wellington, NZ, 2011) at 76.

- Principle 9 explains how long personal information could reasonably be kept by an agency
- Principles 10 – 11 place limits on specific use of and/or disclosure of personal information
- Principle 12 outlines requirements regarding the use/non use of unique identifiers[29]

(Note that principles 2, 3, 6, 10 and 11 all have exceptions in them that alter the way each principle could be interpreted.)

One of the key features of the Privacy Act 1993 as explained in the New Zealand Law Commission review in 2011 is what is described as the "open textured principles" which the writers observed gives the language the "virtues of flexibility and capacity to move with the times".[30] This review document makes reference to direct marketing where it states –

"Direct marketing is a recurring topic in discussions of privacy. Intrusive marketing practices can upset people. In our view this is as much a matter of consumer law as of privacy. We are attracted to the idea of putting the "do not call" register currently operated by the Marketing Association on a statutory basis, and suggest that the Ministry of Consumer Affairs should progress this work. It seems to us that an amendment to the Fair Trading Act would be the appropriate vehicle."[31]

Later in the Law Commission review with regard to the influence of technology on access to personal information the authors state -

"On the whole, we think that the privacy principles and the Privacy Commissioner's current functions and powers are adequate and sufficiently flexible to respond to the challenges posed by new technologies. Nevertheless, that landscape is dynamic and will need to be kept under regular review to ensure that this remains the case."[32]

And further –

[29] At 74.
[30] At 11.
[31] At 20.
[32] At 250.

"It will therefore be important that subsequent reviews of the Privacy Act ensure that the Act continues to adequately deal with technology issues and to reflect international responses to those issues that may be developed in the future through global cooperation and consensus."[33]

An interesting submission to the reviewers referred to whether the Privacy Act was the most appropriate legislation to deal with Internet privacy issues stating -

"In relation to privacy issues between citizens that arise through Internet publication, Professor Roth's submission, drawing from his academic article, was that these issues are better covered by other causes of action such as defamation and the privacy tort and criminal offences such as computer misuse, rather than the Privacy Act."[34]

It is interesting to note that throughout the review there is reference and comparison to the Australian privacy review.

Both Australian and New Zealand authorities have recognised the need to review their privacy legislation. Interestingly the two reviews have yielded quite different approaches with the changes to the Australian legislation preferring quite prescriptive principles and references to online information, direct marketing and the control of information contained or sourced from the Internet. The New Zealand review by contrast has continued to prefer the open textured principles from the original 1993 legislation and the ability to be flexible with the capacity to move with the times. The New Zealand review also placed more emphasis on the ability to utilise 'other causes of action' rather than the Privacy Act. Potts in his 2011 book entitled *Cyberlibel* drew references from the New Zealand tort of invasion of privacy when he said –

"Holding the balance fairly between plaintiffs and defendants in this field is not likely to be easy. The law should be as simple and easy of application as possible in the interests of those who have to make decisions about what and what not to publish"[35]

This reinforces the Law Commission reviewers' perspective about having the legislation flexible and open to interpretation. But does this make the legislation easier to apply or harder to apply?

---

[33] At 257.

[34] At 264.

[35] David A Potts *Cyberlibel* (Irwin law, Toronto, Ont, 2011) at 381.

As with all legislation the strength and value of the legislation will be seen in how individual issues or cases are dealt with over time. Interestingly the New Zealand situation by the very nature of the approach taken creates far more opportunity for the Privacy Act 1993 to be interpreted very widely on a case by case basis thus opening the way for very broad interpretations with regard to online situations as they develop over time.

III Data Collection

Large volumes of data are collected retained, accessed and used online through a variety of data collection methodologies. One of the single biggest issues with regard to the rights of individuals, consumers, organisations or groups is that this information often ends up resident in a country away from where the information originated. The movement of this data from source of origin in New Zealand to an overseas-based repository has implications for the privacy of this data. This data may go to a country, which either doesn't have a privacy framework, or has a privacy framework that is incompatible with New Zealand's.

New Zealand's Privacy Act was amended in 2010 to give the Privacy Commissioner the power to intervene in situations involving international data transfers.[36] Unfortunately the benefit here is more for data being transferred through New Zealand and not for data originating from New Zealand. Interestingly a number of New Zealand's government departments already have their own legislation to deal with the transfer of New Zealand domiciled data internationally and the general consensus in the review is that while the Privacy Act does provide protection for data leaving New Zealand, the principles relating to this issue are cumbersome and could be streamlined over time.[37]

The implications for online consumers is difficult to fully comprehend. If a New Zealand based consumer was to exercise their right to have their personal information withheld whom would they address their requirement to? Which country's privacy framework would be applied and what rights would the New Zealand consumer have

[36] New Zealand, above n 28, at 275.

[37] At 278.

in that particular framework. The reality is that once a consumer's information is moved from its base in New Zealand it could within seconds be domiciled in any number of databases anywhere in the world. This wouldn't necessarily become clear until a direct marketing initiative targets that consumer from this consumers own information.

There are a variety of data collection systems now in place worldwide that have received international acceptance and are used specifically to safeguard and protect personal information. One such example is a global system now in place to safeguard the use of credit card payments to protect against fraud, theft and other criminal activity pertaining to the use of credit card systems.

This credit card data security system is known as the Payment Card Industry Data Security System or PCI DSS which administers a worldwide standard for the security of payment data thus protecting the privacy of individuals, their payment data, purchasing data and banking data. As stated by Fakhry and Nicho[38] "The objective of the standard was to enhance the security of the cardholder through protection of cardholder data and thus help facilitate global adoption of consistent data security measures". This situation is unique because it came about due to agreement being reached between the worlds five largest payment card organisations who identified not only the opportunity to consolidate their work into one efficient system but also to provide a level of security for their financial transactions that would give confidence to their customers that online financial transactions using credit cards are safe.

A similar system could be developed to protect consumers' personal information but this would raise international issues as to who would initiate, fund, coordinate and lead this work. Further, the myriad of consumers and suppliers now using the Internet is such that creating a secure system, implementing it and achieving compliance would already be next to impossible.

Another issue of concern for personal information privacy is how long personal information could/should be retained by a collecting agency. As Corbett says in her

[38] Hussein Fakhry and Mathew Nicho "An integrated security governance framework for effective PCI DSS implementation" (2011) 5 International Journal of Information Security and Privacy 50+ Academic OneFile at 50.

article[39] this also raises the issue of not only how this data is to be removed using a variety of technological options but how legislation can be designed to accommodate this as a requirement.

The rapid rate of change in information storage is highlighted by Witzleb who says:

> "In our modern world of cloud computing, portable storage devices, electronic databases and hackers, the parameters around data security and document storage have shifted immeasurably. All it takes is a single careless incident to cause a massive data breach. The 2011 Sony data breach involved the personal information of up to seventy-seven million people worldwide. A data breach on this scale would have been inconceivable when the Privacy Act was introduced."[40]

The collation, retention, dissemination and removal of data via the Internet is a global issue. There are examples where interventions have been created to protect data in specific situations and the PCI DSS example listed above is one. For the consumer who simply wants to go online and shop they can have a certain level of comfort that some of their personal data, such as their credit card details and transactions, is safe but this guarantee does not extend to all of their personal information leaving them open to approaches through direct marketing schemes.

IV Cloud Computing and New Technology

In addition to the traditional issues associated with Internet privacy Krutz talks about how the rise of '*cloud'* computing presents a newer and more challenging situation with regards to privacy. Cloud computing allows data to be physically stored anywhere in the world and accessible 24/7 without the need to have expensive software and hardware resident with the client or user. This raises issues regarding which country or countries legislation is binding to the cloud based company. In this environment it could be where the Internet Company is based, which country holds the data, or where a client or customer is based when they gain access to data via the '*cloud*'. As explained by Ogigau-Neamtiu [41] the security issues around data include who can create the data, where is it stored, who can modify and access the data, how

[39] Corbett, above n 12, at 247.

[40] Witzleb, above n 7, at 41.

[41] Florin Ogigau-Neamtiu "Cloud Computing Security Issues" (2012) 3 Journal of Defense Resources Management 141 at 145.

the data is deleted, backed up or transferred. These issues are all part of what Ogigau – Neamtiu describes as the data security lifecycle and while it is exactly the same as in the classic Internet configuration the nature of cloud computing makes this lifecycle much more complex. Ogigau-Neamtiu goes on to highlight the lack of international standards for cloud computing[42] giving rise to a plethora of '*standards'* organisations creating a great deal of confusion for potential cloud customers.

The rate of technological change is now so rapid that in the time it takes to draft any privacy legislation the whole Internet environment could have evolved. No one can be sure what the next direction is for the Internet but rapid and constant change is expected. We are very close to a situation where we may have no idea at all what is happening to our personal data, where it is being stored, who has access to it, how it is protected, how legislation can protect it and whether it is stored on Planet Earth. The legal and policy implications of future technological advances are immense and uncertain thus fuelling hesitancy on behalf of law and policy makers.

V Privacy of Personal Information

Privacy is seen as a human right. As Witzleb states "I have no doubt that, innately, people continue to feel strongly about their right to have their privacy protected. That is why privacy is recognised as a basic human right enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR)"[43]

However privacy is not an issue for all consumers. According to Jeff Sweat[44] in 2001 most companies walk "the same fine line between knowing and serving customers well and violating their privacy". Further in the same article he asserts "only a fraction of consumers are so concerned about privacy that they refuse to share information with companies and expect none to be collected about them".[45] Paul Rosenzweig in a 2012 article asserted that:

[42] At 145.

[43] Witzleb, above n 7, at 32.

[44] Jeff Sweat "Privacy" [2001] 851 InformationWeek 30 at 30.

[45] At 31.

> "Even if we wanted to create greater online privacy the trend of technology is making that increasingly impossible to achieve – at least in the classic sense that privacy advocates mean, where a user is in complete control over data about himself".[46]

In a 2013 study by Rebekah Pure on privacy expectations one of her key findings was that privacy expectations differed markedly dependent on what area the personal information was being used in. People have different privacy expectations pertaining to law enforcement than they do for marketing. Further her study found that people think differently about privacy of their information dependent on what information they think is observable and by whom.[47]

On the subject of people's privacy Mark Zuckerburg, the founder of Facebook, is quoted by Witzleb as saying –

> "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. You have one identity… The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to and end pretty quickly… Having two identities for yourself is and example of a lack of integrity."[48]

A recent review of the privacy of data in the European Union by Koponen and Mangiaracina added a further perspective on the retention and use of data when they said that –

> "The European Commission noted that many online services rely on data and are free only because of the information people supply. In some ways data has become currency and it has proven to be a valid business model."[49]

Koponen and Mangiaracina go further to discuss how the retention of individuals' personal data may create an environment that gives an unfair competitive advantage

---

[46] Paul Rosenzweig "Whither Privacy?" (2012) 10 Surveillance & Society 344 at 344.

[47] Rebekah Abigail Pure "Privacy Expectations in Online Contexts" (PhD, University of California, Santa Barbara, 2013) at 98.

[48] Witzleb, above n 7, at 32.

[49] "IBA - Competition Law International October 2013" <http://www.ibanet.org/Article/Detail.aspx?ArticleUid=a48b9a27-aff4-4328-9a01-887cb333e5fa#6> at 7.

to a supplier or a group of suppliers leading to situations where control over data can be a means of 'excluding' rivals.[50] Presumably then the use of personal information as a means of 'currency' in online marketing needs to be carefully monitored to ensure that the consumer's welfare and privacy is safeguarded.

In the USA recent research indicates that the majority of consumers don't want their information collected and used by advertisers.[51] The Federal Trade Commission (FTC), a body charged with protecting the rights of consumer recommended that businesses limited the tracking of consumers' personal information in an attempt to protect the consumers' privacy. These recommendations included the use of a mechanism to allow this information to not be tracked, calling it a 'Do Not Track' mechanism.[52] The FTC reported that not all bodies have entered into the 'Do Not Track' recommendations and some have actually designed their own form of regulations in an attempt to appease concerned consumers. The FTC reports push back from advertising organisations including the Digital Advertising Alliance (DAA) opposed to these recommendations. Further the FTC reports work by both Microsoft and Google on creating 'opt-out' mechanisms that give consumers the ability to have their personal information not included as part of online tracking for advertising and marketing.[53]

As stated by Erica Scott in her research into protecting consumer data, online behavioural advertising has become an increasing concern for privacy rights activists in both the USA and the European Union where 'opt-out' tools have been extensively researched. A key consideration is the development of an international browser level opt-out tool that engages the consumer explicitly, advises them that their data is being 'mined' and presents them with transparent options to allow the consumer to decline data collection.[54] One example of how control of data can be quickly lost is an issue now known as 'data leakage' and is is one area of concern for both researchers and legislators. Data leakage generally happens when online data is transferred from a

[50] At 11.

[51] Angelica Nizio "Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a Do Not Track Mechanism" (2014) 2014 U Ill JL Tech & Pol'y 283.

[52] At 285.

[53] At 285.

[54] "Comment: Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?" [2013] at 285.

first party site to a third party server that may not be known to the user.[55] This data transfer is done by a range of tools available online. Further complicating the environment is the knowledge that the methods available with which to search, store, analyse, 'deanonymize' and transfer data is growing rapidly as new technologies develop. At the current rate of development, technology innovation is occurring faster than legislation can be promulgated or policies can be implemented.

The following view from the same research validates this -

> "Because the Internet increasingly ferries vast amounts of sensitive information, such as medical or financial records, tracking all online activity represents more than just effective advertisement and increased revenue. Tracking such detailed movement online implicates consumer 'privacy, security and dignity.' Advertisers, however, have come to rely on this cornucopia of consumer data and attempting to end that reliance legislatively might be a losing battle."[56]

And further –

> "Additionally, a complete end to behavioral tracking is not necessarily a desirable solution. As was discussed above, advertisements pay for the Internet and consumers, generally, are interested in free services, content and the convenience of a personal web cannot be understated. Rather, a more practicable solution is establishing the rights of online consumers to be notified if their data is collected, to choose how much and what information to reveal, to be able to obtain a copy of their personal data or request that it be discarded, and to know how secure their data is when stored by websites and ad servers."[57]

[55] At 292.

[56] At 297.

[57] At 297.

VI Conclusion

The issue of online privacy of information is hugely complex and constantly evolving in an effort to try and keep pace with the rapid growth of the Internet and the uptake of technology across the world. Many countries have enacted legislation and/or enabled policy and regulatory reform in an attempt to provide appropriate privacy provisions, relevant in this day and age, for their citizens. Countries have also commenced working together to provide privacy solutions that meet their specific needs with the European Union being a good example where a cluster of countries is working collaboratively on privacy issues. New Zealand's office of the Privacy Commissioner has established working relationships with Privacy Commissioners throughout its geographic region to work together to collaborate and develop privacy solutions that are appropriate for this region.

The key issues identified in this paper have included:

- The relevance and effectiveness of domestic privacy legislation, policies and regulations
- Cross border collaboration in the development of legislation, policies and regulations
- The rapid evolution of online technology and the difficulty in developing legislation, policies and regulations at a pace that matches the development and uptake of new technology with the ensuing privacy issues they bring
- The complexity, accountability, and cost of implementing workable privacy solutions internationally
- The dichotomy of privacy concerns by private citizens both domestically and internationally across borders
- The lack of enthusiasm from business suppliers to commit to the cost, time and effort of creating an effective privacy legislation to cover all privacy needs of private citizens
- The aversion of many businesses to giving up access to the wealth of consumer data they currently access and the marketing benefits they currently employ
- The increasing trend of individual businesses providing their own privacy guarantees to their consumers

- The development of technology solutions that will assist individual consumers to make choices about how their personal information is used and/or accessed in specific situations
- The increasing awareness by marketers and suppliers that promoting or enabling privacy options for consumers can be a positive marketing tool

New Zealand's law and policy position on the Internet is not clear. Despite New Zealand legislation containing numerous references to online activities no one single piece of legislation caters specifically for computer/technology based activities. The Privacy Act 1993 (and torts) provides some clarity pertaining to New Zealand domiciled information but does not address the issue of international access to and retention of data. Globally there is little coordinated effort to bring together law and policy that can cross international borders to provide protection to consumers.

By comparison with nearest neighbours Australia, New Zealand's privacy laws are worded to allow for more flexibility in interpretation and application. Australia's recently re-drafted privacy laws on the other hand are considerably more prescriptive and narrowly focused on a specific set of privacy issues and circumstances. The recent review of New Zealand's legislation has revealed little appetite for changing the manner in which privacy law is enacted in New Zealand and will continue to rely on individual cases over time to 'test' and 'tighten' the application of the legislation in the online environment.

In the New Zealand situation whether legislation to protect consumers online privacy is enshrined within privacy laws or consumer based legislation would seem to be of less concern than the ability of the legislation to be flexible and able to be interpreted according to each situation that arises. Therefore the current privacy legislation is probably sufficient for New Zealand's 'domestic' needs given this previously stated intent. This does leave unanswered the question of how to deal with the international implications on consumer privacy given the frequent cross border flow of this information.

The collection, storage, modification dissemination and deletion of data is problematic as technological advances create new data capture systems providing businesses with new opportunities to capture and utilise data. There are examples available internationally that show coordinated efforts being made to secure the privacy of data in specific business applications with the PCI DSS system utilised by

the payment card industry being the one example cited in this paper. That the payment card industry has been successful in creating a secure environment for online card payments indicates what is possible with international cooperation.

The payment card industry was able to achieve this for two very important reasons. Firstly the five main corporations funded the work, committed to it and ensured that a robust system capable of engendering confidence from consumers was developed and mandated internationally for the benefit of all consumers. Secondly these corporations recognised the marketing benefits of creating a safe online payments system for consumers worldwide. They identified that if a safe online payment system wasn't created this would cause considerable harm to their business interests. Adapting to the growth of online shopping and the ease of access for consumers was seen as crucial to the survival of the payment card industry and consumer confidence in online payment facilities was correctly identified as central to the success of the payment card industry.

The growth of cloud computing has added layers of complexity to the issue of online privacy as this platform further stretches the global reach of the Internet and confuses legislative boundaries. Not knowing what is next on the technology horizon makes the role of legislators and policy makers virtually impossible. Add to this the reality that privacy expectations differ greatly depending on the business, social and political context in which it is being considered. Research shows that consumers are divided as to the importance of privacy with views ranging from those who are truly concerned about all aspects of consumer privacy to those who are ambivalent at best. Research also shows consumers to be happy for their details to be freely available as they enjoy the notion of products and services being promoted to them with no effort required on their behalf.

The notion of reaching an agreed position either domestically or internationally on the privacy of consumer information is potentially far from achievable. Research has shown that businesses don't necessarily want to conform to a uniform standard for privacy. Many are of the view that they can offer their consumers a higher level of confidence in the privacy of the data retained by them through proprietary systems they have developed specifically to benefit their consumers. These businesses see this type of offering as a unique selling point for the organisation and are cautious about giving away this sort of advantage. In short privacy is now seen as a potential selling advantage by organisations.

The intention of this paper was to consider whether privacy should be more fully enforced and regulated on the Internet to protect the privacy rights of individual consumers on the Internet or whether the opposite could be more beneficial. This research shows that the issue of Internet or online privacy is problematic due to the complex legislative environment both domestically and internationally, the exponential growth in data management globally, the uncertainty created by rapid technological advances, the varying concerns of the individual Internet users, and the approach of businesses to how they support and promote privacy for individual consumers.

The views of consumers as to the use or otherwise of their personal data are central to consideration of the best way forward. These views range from those who want their personal information completely private and not available for marketing purposes by online suppliers, to those who are happy for their details to be available for marketing purposes as they like to see what products and services are offered up to them online. Extensive research is underway evaluating the ability for consumers to 'control' the use of their data through 'opt-out' tools or browser level screening of data mining. Many marketing companies routinely offer an 'opt-out' option or 'unsubscribe' button in their promotional material as a means of allowing the consumer to control their contact with the marketer.

If we are to take the position that the current environment is very complex and with rapid advances in both Internet use and technological platforms then a reasonable conclusion could be that it is already too late to create, implement, enforce and audit a prescriptive regulatory regime to protect consumer data both domestically and internationally. It may be that we have no choice but to consider the second alternative – letting the Internet users, both the buyer and supplier sides, work towards a model where they create their own model of self-regulation based on open market forces.

Dirk Helbing in his 2013 economic study considered the traditional economic models and whether they are still relevant, as these models are considered complex and often punitive.[58] But globalisation and technological advances have created new levels of interdependencies with the "ability to destabilise our current techno-socio-economic-

[58] Dirk Helbing "Economics 20: The Natural Step towards a Self-Regulating, Participatory Market Society" (2013) 10 Evolutionary and Institutional Economics Review 3 at 31.

environmental systems on a global scale".[59] He says the existing economic models are considered to be top down and would potentially "endanger privacy, socio-diversity and innovation" and further that there would be "major risks that personal data will sooner or later be misused".[60] Further in his research he concludes that "decentralised self-organisation and self-regulation approaches can deliver solutions for complex dynamical systems that are far superior to our existing way of designing and operating systems". And finally Helbing states, "efficient ICT enabled reputation systems and 'qualified money' might support self-regulation."[61]

Helbing states that the digital revolution is re-shaping our economy and there is a major trend towards decentralisation. This decentralisation allows more people to be involved in social, economic and political affairs.[62] This rapid change in people's activities is leading to more creativity, social involvement and innovation thus creating an environment where self-regulation could prosper.

Given the complexities raised in the body of this paper a next step would be to consider the means by which the Internet "market" could be encouraged to self-regulate its privacy practices. In a self-regulated environment businesses would decide for themselves exactly the value that privacy of information has for them, their product and their clients. The customers would have the ability to choose if they wanted their information available and could either opt-in or opt-out of online transactions accordingly.

Research and trialing is currently underway with new technology enablers to assist customers to regulate the release of their own data as and when they decide that it is appropriate to do so. Some countries have already considered the option of having this facility as a mandatory element in its online environment. In due course this could also be considered by New Zealand. However with 41% of all online shopping transactions performed by New Zealanders being with off shore websites[63] the issue is not capable of being resolved simply through New Zealand legislation. Can international cooperation be achieved to strengthen consumer control? Is it possible for legislation to be enacted that appropriately meets all global needs?

---

[59] At 31.

[60] At 31.

[61] At 33.

[62] At 34.

[63] FOREMAN, above n 4.

When New Zealand enacted its Privacy Act in 1993 the Internet was a relatively new communications medium well behind the then rise of the mobile telephone. The Internet has not only become a widely accepted part of daily life but it has effectively bought the whole world close together and created a global market place. Legislation, regulation and enforcement can not keep up with this phenomenon. The best way forward for consumers may well be for them to take control of their position by exercising the right to say no or to opt out until or unless they are satisfied with the service they are receiving. Any other solution may well be beyond us already.

Bibliography

Mills, Jon L *Privacy* (Oxford University Press, Oxford [UK] ; New York, 2008).

New Zealand *Review of the Privacy Act 1993 review of the law of privacy, stage 4* (Law Commission, Wellington, N.Z, 2011).

Potts, David A *Cyberlibel* (Irwin law, Toronto, Ont, 2011).

Solove, Daniel J *Privacy, information, and technology* (Aspen Publishers, New York, 2006).

Solove, Daniel J *Understanding privacy* (Harvard University Press, Cambridge, Mass, 2008).

Witzleb, Normann (ed) *Emerging challenges in privacy law* (Cambridge University Press, New York, 2014).

Allen, Ben and McNair, Hamish "Reforms to Australian privacy legislation will have major impact for both public and private sector" (2012) 64 Keeping Good Companies (14447614) 690.

Corbett, Susan "The retention of personal information online: A call for international regulation of privacy law" (2013) 29 Computer Law & Security Review 246.

Fakhry, Hussein and Nicho, Mathew "An integrated security governance framework for effective PCI DSS implementation" (2011) 5 International Journal of Information Security and Privacy 50+.

Helbing, Dirk "Economics 2.0: The Natural Step towards a Self-Regulating, Participatory Market Society" (2013) 10 Evolutionary and Institutional Economics Review 3.

Nizio, Angelica "Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a Do Not Track Mechanism" (2014) 2014 U Ill JL Tech & Pol'y 283.

Ogigau-Neamtiu, Florin "Cloud Computing Security Issues" (2012) 3 Journal of Defense Resources Management 141.

Rosenzweig, Paul "Whither Privacy?" (2012) 10 Surveillance & Society 344.

Sweat, Jeff "Privacy" [2001] 851 InformationWeek 30.

"Comment: Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?" [2013].

Pure, Rebekah Abigail "Privacy Expectations in Online Contexts" (Ph.D., University of California, Santa Barbara, 2013).

c=AU; o=Commonwealth of Australia; ou=Attorney-General's Department; ou=Office of the Australian Information Commissioner "Privacy fact sheet 17: Australian Privacy Principles Office of the Australian Information Commissioner - OAIC" <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>.

"IBA - Competition Law International October 2013" <http://www.ibanet.org/Article/Detail.aspx?ArticleUid=a48b9a27-aff4-4328-9a01-887cb333e5fa#6>.

FOREMAN, MICHAEL "Offshore retailers gain online marketshare" *Stuff.co.nz* (New Zealand, 1 September 2014) <http://www.stuff.co.nz/business/industries/10447282/Offshore-retailers-gain-online-marketshare>.

PETRI, ALEXANDRA "The worst response to the nude celebrity photo hack" *Stuff.co.nz* (8 September 2014) <http://www.stuff.co.nz/life-style/life/10471692/The-worst-response-to-the-nude-celebrity-photo-hack>.

"Fran O'Sullivan: Key wins - now let's focus on real issues" *New Zealand Herald* (17 September 2014) <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11325841>.