Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

PRIVACY GOVERNANCE ONLINE: PRIVACY POLICY PRACTICES ON NEW ZEALAND WEBSITES

Iwan Tjhin
Whitireia New Zealand, iwan.tjhin@whitireia.ac.nz

Marta Vos
Whitireia New Zealand, marta.vos@whitireia.ac.nz

Satya Munaganuri
Whitireia New Zealand, satyams1084@gmail.com

PRIVACY GOVERNANCE ONLINE: PRIVACY POLICY PRACTICES ON NEW ZEALAND WEBSITES

Iwan Tjhin, Faculty of Business and IT, Whitireia New Zealand, Porirua, New Zealand, iwan.tjhin@whitireia.ac.nz

Marta Vos, Faculty of Business and IT, Whitireia New Zealand, Porirua, New Zealand, marta.vos@whitireia.ac.nz

Satya Munaganuri, Faculty of Business and IT, Whitireia New Zealand, Porirua, New Zealand, satyams1084@gmail.com

Abstract

Addressing privacy issues and concerns are important for organisations when interacting with online customers, and customers are increasingly demanding better transparency about how their personal information could be collected and used. Many organisations are informing users about their privacy practices through an online privacy notice, policy or statement. These privacy notices should reflect the privacy governance practices of the website owners as such notices are the only way online customers can be informed about the privacy practices of the organisation. This study presents a definition of privacy governance, and discusses what good governance would be in the online context. The online privacy practices of organisations in New Zealand are examined using a content analysis questionnaire, with the aim to further understand how organisations in New Zealand through their websites are informing users about their privacy practices, and whether privacy practices of the organizations align with the privacy laws set by the New Zealand government. It was found that while many New Zealand organisations are posting privacy notices, many are failing to provide a good indication of their privacy governance by omitting best practices and legislative requirements.

Keywords: Online privacy, Privacy policy, Privacy of NZ websites, Website privacy policy.

1 INTRODUCTION

The concept of privacy is one which is always changing depending on the context and personal views of the individual. The development of the internet has added complexity to the Warren and Brandeis (1890) seminal view of privacy as the "right to be left alone". Today organisations gather a large amount of data from individuals in online transactions for mainly commercial purposes, and thus our modern definition of privacy has changed to include an individual's desire to have control over their own data, no matter who has collected it, or how it has been collected (Joinson, Reips, Buchanan, & Schofield 2010; Tsai, Egelman, Cranor, & Acquisti 2007).

The Internet has become an essential part of our lives in both business and personal affairs. Website owners wanting to understand their visitors collect a range of information from them through the use of tracking software and cookies, often without users knowing this information has been collected (Wu, Huang, Yen, & Popova 2012). Further, the borderless nature of the internet means that information gathered from users can be easily stored offshore in a jurisdiction with different legislative protections from those of the user's. This has led to online user privacy becoming a public policy issue that has received substantial attention as it affects both users and organisations (Moran & Weinroth 2011). As such, with the increase of use of the Internet, many important questions are posed about the processing of information with regards to user privacy, and about how users can determine the privacy practices of websites.

Conversely, online users have increasingly realised that providing personal data may sometimes be beneficial. Many users perceive that giving detailed and accurate information will result in a higher quality of service, relevant and appropriate messages, and promotions (Yang, Cai, Zhou, & Zhou 2005). These users gain confidence from organisations providing assurances that their information will be protected, as well as being reassured by the presence of privacy legislation and regulation (Wirtz, Lwin & Williams 2007). A survey by Wu et al., (2012) found that online users were more willing to provide information online if they had been given a guarantee that this information would not be misused. However, even though users are now giving away personal data through websites in return for services, and more information is being collected by websites, many users are still unaware of how the collected information could be used. Many websites attempt to reassure users they can be trusted with personal information by posting a privacy policy statement which outlines the websites approach to privacy. Reading privacy policies or privacy statements has become an important process for users who want to reduce privacy risk when disclosing their personal information online. These statements, along with other privacy assurance mechanisms such as third party seals, assist users in trusting a website and thus their willingness to share information with that website (Bansal, Zahedi and Gefen 2015). Although Tsai et al. (2011) had shown that many users did not read online privacy policies, privacy notices informed online customers about the organisations information practices, which in return helped users to decide whether or not they wanted to provide personal information (Milne & Culnan 2004).

The provision of online privacy statements or policies by organisations can be considered to be part of the organisations governance of privacy as it supposedly reflects the processes and procedures used by organisations to manage the information they collect from the online users. However, online privacy governance is not comprehensively defined in the literature. This study provides a definition for privacy governance in the online context and tests the privacy governance practices of New Zealand websites through the use of a content analysis questionnaire. This study contributes to literature through providing a definition of privacy governance. Further, the use of the online privacy statement to test the governance of websites contributes to practice by providing a set of metrics which organisations can use to ensure best practice governance of information collected online.

2 LITERATURE REVIEW

The tracking of individual users through their online movements has become ubiquitous. According to Mathews-Hunt (2016) social media sites derived the majority of their income through such tracking, and targeted advertising directed at users based on their online movements. She found that in Australia consumers were ignorant of online privacy practices, industry regulation was minimal and data breaches were common, which was a situation likely to be mirrored in other countries. From the user perspective, Lowry et al. (2012) found that privacy concerns were a significant factor in discouraging the use of websites, and privacy notices and statements were used by organisations as a way to reassure users about the organisations online privacy practices, and the governance that surrounded them. This literature review will discuss privacy in the online environment and the definition and structure of privacy governance.

2.1 Privacy in the Online Environment

Numerous studies have looked at the relationship between privacy and trust in the online environment. Malhorta, Kim and Agarwal (2004), and Liu, Marchewka, Lu, and Yu (2004) found that a successful and positive relationship between users and an organisation depended largely on the trust of users in the organisation's online privacy policies. These studies found that trust was the mediator between privacy concerns and behavioural intentions. According to Malhorta et al. (2004) the importance of privacy policies laid in assuring users that a particular website could be trusted with their personal information. This in turn formed a view of the trustworthiness of the organisation. Online privacy policies were also used as an attempt to assure users that their personal information would not be disclosed, and that their privacy would be respected (Chellappa & Sin 2005). Furthermore, public opinion surveys found that most online customers were mainly concerned about the loss and misuse of their personal information which indicated a high level of online privacy concern (Wu et al. 2012).

Steinfeld (2016) believed that a privacy policy was one of the main ways users have to monitor a company's privacy practices. Anton et al. (2007) noted that privacy policies allowed users and organisations to negotiate the terms of their privacy practices, with users being informed of the privacy policies of the organisation. However, despite research demonstrated the value of privacy policies in informing users of the practices of the website, studies by Steinfeld (2016) and Sheng and Simpson (2014) showed that users seldom read privacy policies. Indeed, Fox News (2010) reported one instance where an online gaming site inserted an "immortal soul clause" into their privacy policy, whereby the site had an option to claim the user's souls on notice being served in fiery letters, only 12% of consumers opted to nullify this clause. Sheng and Simpson (2014) found a number of reasons users did not read privacy policies which include a lack of time and the complexity of the policy. Barriers to reading privacy policies also include the length and complexity of the policy, and the difficulty of the text given that many policies were aimed at avoiding litigation (Schermer, Custers & van der Hof 2014). Schermer et al. (2014) contended that this complexity challenges the notion that consumers consented to the gathering of their data, arguing that such consent could not be implied if users could not understand the privacy policy. They also pointed out that many websites forced users to accept the gathering of information by preventing them from using the website if they did not consent, concluding that there was an absence of realistic consent in this practice.

Organisations, however, were struggling to determine what should be included in privacy policies. Tene (2011) reported that Facebook had been condemned for including too much granularity in their privacy policy, and not enough. While Jafar and Abdullat (2009), in a readability study, found that many social media sites (with the exception of Yahoo) had increasingly complex and difficult to read privacy policies, requiring a user to have at least two years of university education before they were comprehensible.

Some studies such as Dinev and Hart (2006) and Milne and Boza (1999) further suggested that to build trust, privacy policies should not only be informative but also reassured consumers that disclosing their personal information was a low-risk proposition. A clear and credible privacy policy helps organisations build a positive and favourable reputation with consumers (Schoenbachler & Gordon 2002). Bansal et al. (2015) believed that tailoring privacy approaches to an individual's concern for their privacy assisted in persuading users to trust a website. They found that users with a high level of privacy concern preferred detailed privacy policy statements and considered an organisations reputation and the quality of their information, while less concerned users merely glanced at privacy policies and focused more on website design.

It is in the best interests of organisations to reassure users about the privacy of their information as a common response to users feeling unsafe online is that they either withhold information, or provide false information (Wirtz et al. 2007). Harris Interactive Inc. and Westin (1997) found that 60% of users who provided false information would be willing to give their real information if notice was available in the website pertaining to how this information would be used. In an experimental study, Tsai et al. (2011) found that users would pay a premium to purchase from websites they felt better protected their privacy, and recommended that websites use clear privacy information up front to users in order to gain a competitive advantage over rivals.

2.2 Privacy Legislation and Governance

Privacy governance is an area that is not well defined, partly because the term governance itself is problematic. Graham, Arnos and Plumptre (2003) believed that the terms governance and government were not synonymous. Whereas Plattner (2013) observed that the increasing popularity of the term over the previous 20 years had led to many authors using the terms synonymously. McGrath, and Whitty (2015) in a comprehensive review of the term, defined governance as "the system by which an entity is directed and controlled" (McGrath & Whitty 2015, p. 21). They also specifically excluded strategy, leadership and decision making from the term governance. Goede and Neuwirth (2013) believed that the role of governance was to steer an organisation, and that good governance added the dimension of governing according to legal (legislative) or ethical principles. Thompson, Ravindran and Nicosia (2015) discussed an Australian case study in which a lack of data governance was apparent in the inadequacy of a number of state databases. They defined data governance as providing for the management of data assets pointing out that there was little value in regulating compliance with data governance principles if there was no way of measuring whether or not organisations were actually complying.

Herold (2006) believes that an effective privacy governance program promoted customer satisfaction, as well as protecting the organisation from litigation, but did not define privacy governance. Wang and Wu (2014) described privacy governance as being the rules which governed the relationship between an organisation and its customers, either those enforced by legislation or those agreed within the community. Therefore, governance can be either legislated, or "voluntary" in nature. Wang and Wu (2014, p. 95) proposed that organisations should have a policy of "proactive privacy governance" in order to protect the privacy of online users of ubiquitous services. They described three measures to encompass privacy governance including clearly informing online customers of the organisations privacy practices, educating online customers about their own roles in protecting their privacy, and monitoring of the organisations privacy practices, alerting customers if their information is compromised. Their quantitative study found that proactive privacy practices encouraged users to disclose their information online.

Wirtz, Lwin and Willliams (2007) recommended a number of best practices to be applied to online privacy efforts, including clearly communicating changes in policies to customers, and ensuring that online marketing meets any standards set by industry, and company privacy policies. Mathews-Hunt (2016) went further, recommending an alliance regulatory efforts, including either legislation or self-regulation of online behavioural marketing, improvement to the process of allowing users to opt out of

tracking practices, education, standardisation and enforcement of industry practices. Taking an organisational approach, Anton et al. (2007) recommended organisations to consider more than just policy management, to take into account the economic and legal perspectives when developing a comprehensive privacy framework.

The presence of privacy-related legislation also acts to reassure users that their information is safe online. Wirtz et al. (2007) found that company privacy policies, the presence of third party privacy accreditation, and government legislation acted to reduce consumer concerns at providing personal information online. In New Zealand, the Privacy Act 1993 (the Act) protects the privacy of an individual. The main purpose of the Act is to guide how personal information is collected, stored, used and disclosed. This includes information gathered online. The Act covers all business operations in New Zealand with twelve privacy principles following the Organisation for Economic Co-operation and Development OECD (1981) privacy conventions.

From this literature, and borrowing from McGrath and Whitty (2015), it would be reasonable to define privacy governance as "the system by which privacy within an entity is directed and controlled". Following Goede and Neuwirth (2013), this definition can be enriched by incorporating "good governance" of privacy which would consider whether the direction and control of privacy within an organisation includes industry best practice and legislative requirements. Wang and Wu (2014) provided three measures encompassing privacy governance, two of which can be applied to the online environment through examination of an organisations posted privacy notice. Firstly, it can be determined whether the organisation informs the customer of their privacy practices through posting a privacy notice that is comprehensive and complies with industry best practice and legislation. Secondly, the education of users can be tested through the privacy notice being readable to users. A number of studies including [Withheld] used content analysis questionnaires to investigate the privacy practices of websites as detailed in the websites privacy statements, and throughly testing elements of the website itself. Such content analysis can also be used to examine aspects of good privacy governance including compliance with best practice and privacy legislation.

3 METHODOLOGY

The content analysis questionnaire used for this study was arranged to address four elements of privacy governance, with the questions detailed in the findings section.

Firstly, complying with what can be considered industry best practice, it determined whether or not the website posted a privacy notice, and what information was gathered by the website. However, if the website was a brochureware (in other words, it collected no information from the user but was merely informative), then a privacy notice was not required. The positioning of the privacy notice was also tested.

Secondly, the alignment of privacy policy notices with the New Zealand privacy laws, particularly the sections dealing with data collection and management was tested.

Third, the privacy policies were examined against principles of online privacy best practice focusing on the type of information collected by the website, whether or not individuals could control their own data, and whether or not users would be informed when the privacy policy changes.

Fourth, the readability and language of the privacy notice was tested. Readability is important to ensure users understand the privacy policy. Further, the type of language used in the privacy notices was tested to determine whether unacceptable practices were disguised through associating them with being common, cookies with being small, and the sending of marketing material associated with being valuable.

Using Kompass.co.nz, a list of top organisations in New Zealand was obtained based on financial turnover, number of employees, and importance to the New Zealand market. From this list, 100 organisations were randomly selected as the sample. This sample included both public and private

organizations, but was limited to those whose website domain names ended with ".co.nz", ".net.nz", ".govt.nz", and ".org.nz". If a selected organisation did not have a website, it was skipped and another organisation was selected.

The sample organisations' main website pages (webpages) were visited using the Google Chrome web browser, on a machine running Microsoft Windows 8.1 Enterprise Edition. Where mobile and desktop versions of the webpage were available, the desktop version was used.

For each website visited, attempts were made to locate the privacy policy notice. In order to be considered as a privacy policy statement or privacy policy notice, it needed to use a heading with the word "Privacy". Web pages that contained "Privacy" as a section heading or paragraph heading within other documents (such as "Terms and Conditions") were also considered to have a privacy policy statement or privacy policy notice. If a document was titled, for example, "Legal Disclaimer" but did not include any section heading with "Privacy", then it was not considered to be a privacy policy statement or privacy policy notice.

All privacy policy notices located were subjected to a content analysis, against the questionnaire. A copy of the website privacy notice was retained on first visit, and used for subsequent enquiries. If a website changed its notice during the course of this study, the initial version was be used. If the links to the privacy policy notice did not work, then the website was considered to have no privacy policy.

4 FINDINGS AND DISCUSSION

Findings of the content analysis of online privacy policy notices are grouped according to the logical grouping used in the questionnaire.

4.1 Part One – Privacy Notification

The first part of the questionnaire identified whether the website was a brochureware (defined as a website that only provides information about a business, similar to a brochure), and whether the website contained a privacy policy notice. This first part also looked at how the headings and links to the policy privacy notices were phrased and positioned in the websites, as well as methods used in collecting information. Table 1 below shows the summary of findings of the privacy policy notices identification and information collection.

No.	Criteria	Yes	No
1.	Is the site 'brochure ware'?	29	71
2.	Is there a privacy notice?	79	21
3.	Is the privacy notice more than one click away from homepage?	16	63
4.	Are there links to an e-mail address, e-mail form or logon?	71	29
5.	Can job applications be submitted online?	46	54
6.	Are other means used to collect user details (e.g. inquiries, surveys, sweepstakes and contests etc.)?	25	75
7.	Can third parties send cookies or web beacons to users?	13	87

Table 1. Privacy policy notices identification and information collection.

The study found that 29 of 100 sample organisations' websites were brochureware. Only 79 websites of the total sample contained some form of privacy notification.

Most commonly used heading for privacy policy notice was “Privacy Policy” with 40 organisations using it. Headings like “Privacy Notice”, “Privacy Policy” and “Privacy Statement” were used by 15, 1, and 13 organisations, respectively. There were 10 organisations whose privacy policy notices were embedded within other headings, such as “Terms and Conditions”, “Legal Disclaimers”, “Terms of Use”, and similar.

In terms of position of the link to the privacy policy notice, the study found that while 55 organisations placed the link on the homepage, the actual location within the page varied widely. The link was found at the centre bottom (24), left bottom (15), left top (1), and right bottom (15). There were 24 organisations that placed it on a webpage other than homepage.

This reveals that the notifications were neither consistent in format and wording, nor in where there were located in a similar place within the websites. This could simply be the result of no industrial guidelines or norms to designing an effective privacy notice.

There were indications that many organisations intended to collect voluntary information from the users, with links to an email address, email forms or logins were found in 71 websites. Job applications could be submitted in 46 websites. Other means used to collect user details, such as inquiry, surveys, contests, etc. were found in 25 websites. In relation to the possibility of third parties sending cookies or web beacons to the users, 13 organisations indicated that this may occur.

Organisations that collect and use personal information should have an effective approach to informing the users using the Multi-Layered Privacy Notice recommended by (APEC 2005). This approach was outlined and recommended by the New Zealand Office of the Privacy Commissioner (n.d.) in its “10 Steps to develop a multi-layered privacy notice” as a source of detailed information.

The Office of the Privacy Commissioner (n.d.) has also published “Questions & Answers About Layered Privacy Notices”, stating that they believed a layered privacy notice could improve communication about how organisations handle personal information. It further introduces a simple process that organisations could adopt to create their own. Organisations who found themselves having challenges to provide good and effective privacy notification could consider adopting the Office’s recommendations.

4.2 Part Two – New Zealand Privacy Act

The second part of questionnaire addressed the privacy policy notice alignment with the New Zealand privacy laws. Table 2 below shows the summary of finding of the privacy policy notice alignment with the New Zealand privacy laws.

No.	Criteria	Yes	No
1.	Is the purpose of information collection outlined?	59	20
2.	Information is only collected from the individual not a third party (about the individual)?	54	35
3.	Are intended recipients listed?	10	69
4.	Is the name of collecting agency given?	3	76
5.	Is the address of the collecting agency given?	3	76
6.	Is the name of the holding agency given?	3	76
7.	Is the address of the holding agency given?	4	75
8.	Are consequences of not providing information outlined?	23	56
9.	Does the notice mention steps taken to secure transmissions between	56	23

	business and customer?		
10.	Does the notice mention steps taken to secure information stored by the business?	55	24
11.	Can the individual access their personal information?	54	25
12.	Can the individual correct their personal information?	50	29
13.	Are attempts are made to keep information up to date?	21	58
14.	Are steps in place to archive or destroy the collected information?	15	64
15.	Is information used for the purpose of collection only?	72	7
16.	Is there mention of or contact available with a privacy officer, or contact details given for a privacy matter?	39	40
17.	Is the New Zealand Privacy Act mentioned?	47	32
18.	Are other exemptions to the New Zealand Privacy Act given?	20	59
19.	Notice claims information will be released if legally required (e.g. by the Tax Act)?	51	28

Table 2. Privacy policy notice alignment with the New Zealand privacy laws.

From the 79 websites that contained some form of privacy policy notice, the study found that there were 59 organisations that mentioned the purpose for which information was collected, with 54 of them stating that they collected information about an individual only from the individual and not a third party.

Only 10 organisations mentioned at least one of the intended recipients, even if it was just a term such as “We” as the owner of the website. Name and address of the collecting and holding agencies were given only in 3 of the websites.

There were 23 organisations that gave the consequences of not providing the information outlined, but most of these were related to the consequences of not accepting website cookies.

Mentions of whether individuals were able to access and correct personal information were found in 55 and 54 of the notices, respectively. A total of 72 of the notices mentioned that information is used for the purpose for which it is collected. Only 21 of the notices mentioned attempts would be made to keep information up to date.

According to New Zealand privacy laws (Office of the Privacy Commissioner 2006), when an organisation collects personal information directly from the individual concerned, it must take reasonable steps to ensure the individual is aware of the fact that the information is being collected (79 organisations had privacy notices), the purpose (59 organisations), the intended recipients (10 organisations), the names and addresses of who is collecting the information and who will hold it (3 organisations), any specific law governing provision of the information (47 organisations) and whether provision is voluntary or mandatory, the consequences if all or any part of the requested information is not provided (23 organisations), and the individual’s rights of access to (55 organisations) and correction of personal information (54 organisations). This suggests that majority of the organisations ignored, or were unaware of, at least parts of the requirements of the Privacy Act.

Privacy officer contact details for privacy matters were mentioned in only 39 of the notices in accordance with the Act. In 47 of the websites, the Act was mentioned in their privacy notices. Three websites mentioned that their privacy policy notices were in accordance with the Australian Privacy Act, even though the organisations had a “.nz” website address. Exemptions to the requirements of the Act, in the case of the organisations being legally required to release information, were mentioned in 51 of the notices. Other possible exemptions to the Act were mentioned in 20 of the notices.

Pertaining to storage and security of personal information, an organisation holding personal information must ensure that there are reasonable safeguards against loss, misuse or disclosure (Office of the Privacy Commissioner 2006). Steps taken to secure information stored by the organisations and steps taken to secure transmissions between users and the organisations were mentioned in 55 and 56 privacy policy notices, respectively. Some of the websites analysed had separate policies for security but the number for those were not recorded. Although this seems to imply that many organisations were not safeguarding information, the actual practice of these organisations remains unclear. Other organisations who did not outline these steps could possibly have internal safeguard process in place.

Another aspect of the privacy laws requires that an organisation holding personal information must not keep it for longer than needed for the purpose for which the organisation collected it (Office of the Privacy Commissioner 2006). There were only 15 organisations that mentioned steps would be taken to destroy information when it was no longer needed. This gives an indication that only a few organisations were aware of their obligation to the laws and taking proactive steps to inform their users. It is unsure, however, what the practice of the other organisations, who did not include steps in their privacy notices, in relation to destroying information.

A study by [Withheld] evaluated privacy statement of major New Zealand banks websites showed similar results. Their study found that all banks stated that customers may request correction of information, but none offered confirmation that correction had been made or that agencies to which information had been disclosed would also be informed, and the information corrected. It appears not much have changed since.

4.3 Part Three – Best Practice

The third part identified the elements of best practices mentioned in privacy policy notices. The summary of finding is shown in the table 3 below.

No.	Criteria	Yes	No
1.	Is personal information released to affiliates?	38	41
2.	Is personal information released to third parties?	27	52
3.	Is non-identifiable (or aggregated) information released either to affiliates or third parties?	17	62
4.	Is non-personally identifiable or aggregate information collected?	49	30
5.	Are promotional e-mails sent?	39	40
6.	Can individual opt out?	16	63
7.	Can the individual opt in?	4	75
8.	Does the notice say it may change?	40	39
9.	If yes, are notifications sent?	3	37
10.	Does the privacy notice include the date of the last update?	14	65
11.	Does the notice say the site use cookies or web beacons?	49	51
12.	Does the notice point out that cookies or web beacons can be disabled?	32	68
13.	Are the consequences of disabling cookies or web beacons pointed out?	29	71
14.	Notice disclaims responsibility for linked parties' privacy practices?	36	64

Table 3. Privacy policy notice best practice.

There were 38 organizations that indicated they would release personal information to the affiliates and 27 organisations would release them to third parties. These numbers were high. Moreover, none of their privacy notices mentioned the names or any other details pertaining to these third parties to whom information would be released. This would not give the users a reasonable opportunity to request access and/or correction of personal information from these third parties. Any request for correction would therefore rely heavily on the organisations that collected it at the first place to relay the updated information across to these third parties.

The study found that 49 organisations mentioned they would also collect non-identifiable or aggregated information. Intention to send promotional emails was mentioned by 39 organisations who mainly claimed that the purpose of collecting information was to send marketing related information. Only 16 organisations allowed users to opt-out if they were not interested in receiving promotional information like emails or even the placement of cookies on their devices, and only 4 organisations used an opt-in approach, suggesting that information collection by most organisations was largely mandatory. This practice by itself is not against the privacy laws if the organisation collecting the information believes on reasonable grounds that it is not prejudicing the interests of the individual concerned, or it is necessary for a public sector agency to collect the information to uphold or enforce the law, or, the information will not be used in a form in which the individual concerned is identified (Office of the Privacy Commissioner 2006). Best practice suggests that organisations should elect to use opt-in approach, in the interests of building better trust with their users. Nonetheless, the Unsolicited Electronic Messages Act 2007 (Parliamentary Counsel Office 2013) prohibits unsolicited commercial electronic messages with a New Zealand link. The intention by 39 organisations to send promotional and marketing related information through emails, with only 16 of them allowed the users to opt-out, does not appear to be a fair practice, or good governance.

Privacy policy and practice could change along with the organisations strategic and operational direction. The study found that 40 organisations mentioned that their privacy policy notices may change, but only 3 of them said that they would send notifications should it occur. The findings were concerning. Furthermore, 76 organisations stated that it was the user's responsibility to check the websites to determine whether any changes were made to the privacy policy. Moreover, only 14 of privacy policies actually had the date of last update on the notices. It is reasonable to expect that an organisation would notify their users should these changes occur. Putting the date of last update is the least an organisation could do to inform their users of any possible changes to their privacy notices.

The study found that 49 organisations mentioned the use of cookies for recording user's online activities within their websites. However, this did not mean that these organisations would actually use them. There were 32 organisations that mentioned that cookies or web beacons could be disabled, but only 29 organisations pointed out the consequences of disabling them. Disclaimers of responsibility for linked parties' privacy practices were made by 36 organisations. TRUSTe (n.d.) suggests that the more notification is given and the less information is actually collected, the more users will trust the organisation. Personal data collected from the users should be minimal and only enough to either provide them with products or services, or let them interact on the website. Findings in this study indicated that organisations in New Zealand seemed to generally adhere to this suggestion when it comes to data collection using cookies and web beacons.

Many organisations failed, however, to take extra steps to inform users about how their information would be used. This pertains particularly to indications that many organisations intended to collect voluntary information from the users, with links to an email address, email forms or logins, job applications that could be submitted online, and other means used to collect user details, such as inquiry, surveys, and contests. When information was collected from the users and/or from user-profiling technologies like cookies, log files and web beacons, organisations should not only notify users about them in the privacy notice, but also disclose their use of all personally identifiable information in order to comply with the privacy laws (Office of the Privacy Commissioner 2006).

Further, almost all of the organisations who indicated that they would release personal information to the affiliates and/or to third parties made disclaimers of responsibility for linked parties' privacy practices. This includes the possibility of third parties sending cookies or web beacons to the users.

4.4 Part Four - Readability

The fourth part measured the readability of privacy policy notices, and the summary of finding is shown in table 4 below.

No.	Criteria	Yes	No
1.	Is privacy notice easy to read?	0	79
2.	Are legal terms used (eg. confidentiality, enforcement, exigent, edicts etc.)?	7	72
3.	If yes are they explained?	3	4
4.	Are IT terms used (eg. cookie, IP, log files, data mining etc.)?	52	27
5.	If yes, are they explained?	49	3
6.	Are information sharing practices associated with carefully selected, trustworthy, reputable, responsible or similar?	14	65
7.	Is the sending of marketing material associated with occasional, information that is thought to be of value, or interesting to the user?	11	68
8.	Are cookies and/or web beacons associated with small or common usage?	19	60
9.	Are there generic disclaimers used in the notice (e.g. "except as otherwise stated", "use of this website implies consent" etc.)?	40	39

Table 4. Readability of privacy policy notices.

The study found that legal terms were used sparingly, with only 7 organisations using them extensively. The use of IT terms was more common, with 52 organisations using them in their privacy policy notices, and 49 organisations explained the IT terms they used. Generic disclaimers used by organisations in privacy policy notices were apparent in 40 websites.

Graber, D'Alessandro, and Johnson-West (2002) believed that online health notices should have a level of no more than US 8th grade (NZ year 9) to be easily readable. In comparison, the privacy notices tested had an average readability score of 13 using the Flesch-Kincaid grade level. This indicates a minimum requirement of the equivalent of a New Zealand year 13 education level. All organisations in this study failed to provide notices that were easy to read. This was further compounded by the use of legal and IT terms in the notices. The use of generic disclaimers by organisations found in this study could in fact be counterproductive in establishing trust, as some studies found it produced a largely negative emotional effect (Ata, Thompson, & Small 2013). Organisations in New Zealand have room for improvement in providing online privacy policy notices to their customers that are better tailored and easy to read.

5 CONCLUSION

This research defined privacy governance and gauged the privacy governance practices of New Zealand websites using a content analysis questionnaire applied to the organisations online privacy

notices. Although a reasonable numbers of New Zealand website contained privacy notices of some form, many of these notices were deficient in indicating the organisations online privacy practices and governance. While most organisations took reasonable steps collect only pertinent information from users, there was little effort made to inform users about how this information might be used by third parties. The use of disclaimers about how third parties might use information was also worrying as this indicated a lack of concern on the part of collecting organisations for third party privacy practices and governance.

Many organisations which had a privacy notice failed to address all the criteria of the New Zealand Privacy Act, particularly around notification of changes to the policy, and the ability of users to correct their information. Of particular note is that few organisations gave contact details of the collecting agencies, or listed recipients of information collected. Given the disclaimers about third party use of information, users should at least be able to determine which third party would be receiving their information so they can check the governance practices of those organisations. According to Wang and Wu (2014), one of the primary measures of privacy governance was to clearly inform users about the organisations privacy practices. The practice of not informing users of third party practices, and disclaiming responsibility for them, clearly infringed this element of good privacy governance. Furthermore, the high reading level required to read and understand the studied privacy notices was also concerning, as this not only failed to clearly inform users of the organisation's privacy governance, it also negatively affected users' trust. In many cases, the privacy notices associated information sharing with being common, and marketing material stated to be of value. These phrases were designed to minimise the effect of potentially unpalatable practices, and it could be argued that organisations using this practise were failing in their governance by using language to conceal their practices.

In terms of best practice, many websites did not allow users to opt-out of information gathering, in contravention of established best practice. Most privacy notices also failed to contain the date of last update, and of those that did, expected the users to check the privacy notices to see if any changes had occurred, in contradiction to recommendations by Wirtz, Lwin and Williams (2007). The prevalence of these practices is of concern as they indicate that website owners had not considered basic best practice when it came to online information gathering and user notification.

In informing users of legislative requirements, many of the organisations examined described the purpose for which they gathered information. However, details in respect of where the information was held, or how it could be accessed or changed were found to be less common. Good privacy governance would imply this information should be readily accessed by the reader of the policy.

This study has found that the online governance practices of some New Zealand websites, while being adequate in terms of providing privacy notices informing users as to the privacy practices of the website, were not providing users with enough, easily readable information, to fit the criteria for being "good governance". Given that the only way online users have to discover the privacy governance practices of websites was to read the online privacy notice, these notices should fit the criteria of good governance by being easy to locate, comprehensive in nature and readable for the average member of the public rather than someone with a year 13 reading age (in the US this would be the end of high school education).

Wang and Wu (2014) found that strong privacy governance, communicated through privacy notices enhanced users' trust and therefore encouraged users to transact with the organisation. Therefore, a connection can be established between privacy governance, user trust and transactions with the organisation. It would only be to the advantage of organisations to maintain good online governance practices through informing users of the privacy practices. However, despite being able to identify good privacy governance practices many questions still remain. For example, Tsai et al. (2011) found that users frequently did not read privacy policies. Therefore, what would a good governance require? Should organisations just accept that mere presence of a privacy notice is enough, whatever the policy says? Perhaps, should good governance require a tailored approach to privacy where each individual is

able to select the amount of information they share with each website? These are all questions that could be addressed in further research, in order to fill in the picture of what good privacy governance should look like in the online environment.

6 LIMITATIONS

There were 502,170 organisations in New Zealand as of February 2015 (Statistics New Zealand 2015). Content analysis from a sample of 100 organisations in this study could not draw conclusive and definite findings as to the practices of all New Zealand organisations.

This study was also limited by the inability to match privacy policy notices posted by organisations with reality in practice. As noted by Kuzma (2011), organisations could not assume that the posting of a privacy notice guaranteed that the organisation would comply with existing legislation. Similarly it could not be tested whether or not the organisation actually practised what was posted in the privacy notice. It is not unrealistic to suggest that some organisations might not practice their own stated policies, either deliberately or otherwise. It is also possible that some organisations might have better privacy practices than what they claimed on their websites.

7 FUTURE WORK

Future work from this study could include tracking privacy policies over time through a longitudinal comparison. Further, an attempt could be made to match posted privacy policies with the reality of organisational behaviour. Sample size could also be extended to cover a broader range of organisational demographics, by also taking into account the smaller organisations. Other potential further study may also include comparative study between and/or among countries, longitudinal study, and more.

References

Anton, A. I., Bertino, E., Li, N., & Yu, T. (2007). A Roadmap for Comprehensive Online Privacy Policy Management. Communications of the ACM, 50(7), 109-116.

APEC (2005). Multi-Layered Notices Explained. Retrieved from http://mddb.apec.org/documents/2005/ECSG/DPM1/ 05_ecsg_dpm1_003.pdf

Ata, R. N., Thompson, J. K., & Small, B. J. (2013). Effects of exposure to thin-ideal media images on body dissatisfaction: Testing the inclusion of a disclaimer versus warning label. Body image, 10(4), 472-480.

Bansal, G., Zahedi, F. & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. European Journal of Information Systems. 24, 624-644.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6(2-3), 181-202.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.

Fox News (2010). 7,500 Online Shoppers Unknowingly Sold Their Souls. Retrieved from http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html.

Goede, M. & Neuwirth, J. (2014). Good Governance and Confidentiality: A Matter of the Preservation of the Public Sphere. Corporate Governance, 14(4), 543-554.

Graber, M. A., D'Alessandro, D. M., & Johnson-West, J. (2002). Reading level of privacy policies on internet health web sites. Journal of Family Practice, 51(7), 642-642.

Graham, J., Amos, B. & Plumbtre, T. (2003). Principles for Good Governance in the 21st Century, Policy Brief, Institute on Governance, Ottawa, Ontario.

Harris Interactive, Inc., & Westin, A., 1997. Commerce, Communication and Privacy Online. New York: Louis Harris & Associates.
Herold, R. (2006). Building an effective privacy program. Information Systems Security. 15(3), 24-35.
Jafar, M. J. & Abdullat, A. (2009). Exploratory analysis of the readability of information privacy statement of the primary social networks. Journal of Business and Economics Research. 7(12), 123-142.
Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. Human–Computer Interaction, 25(1), 1-24.
Kuzma, J. (2011). Empirical study of privacy issues among social networking sites. J. Int'l Com. L. & Tech., 6, 74.
Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2004). Beyond concern: a privacy–trust–behavioural intention model of electronic commerce. Information & Management, 42(1), 127-142.
Lowry, P. B., Moody, G. D., Vance, A., Jensen, M., Jenkins, J. L., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. Journal of the American Society for Information Science and Technology. 63(4), 755-766.
Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). Internet users' Information privacy concerns (IUIPC): The construct, the scale and a causal model. Information Systems Research, 15, 336-355.
Mathews-Hunt, K. (2016). Cookie consumer: Tracking online behavioural advertising in Australia. Computer Law and Security Review. 32, 55-90.
McGrath, S. K., & Whity, S. J., (2015). Redefining governance: From Confusion to Certainty and Clarity. International Journal of Managing Projects in Business, 8(4), 1-36.
Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing, 13(1), 5-24.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy statements. Journal of Interactive Marketing, (18:3), pp15-29
Moran, T. J., & Weinroth, J. (2011). Invasion Of Privacy On The Internet: Information Capturing Without Consent. An Ethical Background As It Pertains To Business Marketing. Journal of Business & Economics Research (JBER), 6(7).
OECD (1981). Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data 1981. Retrieved from http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.
Office of the Privacy Commissioner (n.d.). Effective website privacy notices. Retrieved from https://www.privacy. org.nz/news-and-publications/guidance-resources/ effective-website-privacy-notices/
Office of the Privacy Commissioner (2006). Information Privacy Principles. Retrieved from http://www. privacy.org.nz/news-and-publications/guidance-resources /information-privacy-principles
Parliamentary Counsel Office (2013). Unsolicited Electronic Messages Act 2007. Retrieved from http://www.legislation.govt.nz/act/public/2007/0007/latest/096be8ed80cda4af.pdf.
Plattner, M. F. (2013). Reflections on "governance". Journal of Democracy. 24(4), 17-28.
Schermer, B. W., Custers, B. & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. Ethics in Information Technology, 16, 171-182.
Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. Journal of Interactive marketing, 16(3), 2-16.
Sheng, X. & Simpson, P. M. (2014). Effects of perceived privacy protection: Does reading privacy notices matter? International Journal of Services and Standards, 9(1), 19-36.
Statistics New Zealand (2015). New Zealand Business Demography Statistics: At February 2016. Retrieved from http://statistics.govt.nz/browse_for_stats/businesses/business_characteristics/BusinessDemographyStatistics_HOTPFeb15.aspx

Steinfeld, N. (2016). “I agree to the terms and conditions”: (How) do users read privacy policies online? An eye tracking experiment. Computers in Human Behaviour. 55, 992-1000.
Thompson, N. Ravindran, R. & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. Government Information Quarterly, 32, 316-322.
Tene, O. (2011). Privacy: The new generations. International Data Privacy Law. 1(1), 15-27.
Tsai, J. Egelman, S., Cranor, L., & Acquisti, A. (2007). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. 6th Annual Workshop on “Economics and Information Security” (WEIS 2007), Pittsburgh PA, 7-8 June 2008.
Wang, S-C. & Wu, J-H. (2014). Proactive privacy practices in transition: Toward ubiquitous services. Information and Management. 51, 93-103.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 193-220.
Westin, A. (1967). The right to privacy. New York: Athenaeum.
Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy control. International Journal of Service and Industry Management. 18(4), 326-348.
Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 28(3), 889-897.
Yang, Z., Cai, S., Zhou, Z., & Zhou, N. (2005). Development and validation of an instrument to measure user perceived service quality of information presenting web portals. Information & Management, 42(4), 575-589.