2024

# An Examination of Industry Privacy Statements in Top New Zealand Websites

Sumedha Mukherjee
*Auckland University of Technology*, jjz7723@autuni.ac.nz

Jairo Gutierrez
*Auckland University of Technology*, jairo.gutierrez@rocketmail.com

# 4. An Examination of Industry Privacy Statements in Top New Zealand Websites

Sumedha Mukherjee
Auckland University of Technology, New Zealand
jjz7723@autuni.ac.nz

Jairo Gutierrez
Auckland University of Technology, New Zealand
jairo.gutierrez@aut.ac.nz

## Abstract
*This paper presents a comprehensive analysis of various website privacy statements within six distinguished industries, namely: Retail, Banking, Travel & Tourism, Government, Healthcare and Entertainment in line with the requirements of the New Zealand Privacy Act 2020. As data privacy concerns are highly prevalent in a time where data is a highly valuable asset and leveraged for organizational competitive advantage, this study seeks to evaluate the extent to which popular websites in these industries adhere to the legal requirements and industry best practices that are outlined in the latest Privacy Act using a content analysis questionnaire. This study also seeks to evaluate Government privacy statements against other industries and evaluate further the published information security practices of New Zealand websites.*

**Keywords**: Privacy Statements, Privacy Policy, Website Analysis.

## 1. Introduction
Data privacy has become cardinal to the safety of online users' personal information. The term "privacy" in the online context has evolved to include an individual's inclination to be aware of,or have control over their data despite the nature of collection, and by whom (Tjhin et al, 2016). The limitless nature of the internet has exhibited a need for individuals to provide personal information to make use of services online, and a need for organizations to collect this data to improve their services (Tjhin et al, 2016). Business integrity in the data privacy context in New Zealand is often reflected in the "privacy policy" or "privacy statement" of websites (Hooper & Vos, 2009), through contractual obligation to comply with the New Zealand Privacy Act 2020. Privacy mechanisms such as "privacy policies" and "privacy statements" are perceived to be foundational for data privacy best practices, as they inform users on the privacy practices of the online organizations (Tjhin et al, 2016). Hooper & Vos (2009) stated that the public quality of a given website is cognizant of how the organization who hosts it is appraised; and it is argued that websites serve as a representation of the backing of the organization's values, particularly with respect to privacy. Privacy statements on these websites are an example of privacy assurance to users, which disclose the nature of collection, protection, and storage of personal data from visiting individuals online (Mutimukwe et al, 2020). In recent literature, the perceived effectiveness of privacy policy statements shows an increase over other mechanisms, such as third-party seals, when examining online individual's willingness to provide their information (Fabian et al, 2017).

In New Zealand, the information privacy principles and codes of practice detailed in the Privacy Act 2020 provide a definition for the privacy rights of individuals, and therefore online customers. Hooper et al. (2007) stated that the primary criteria for evaluating privacy statements of online organizations would be the details in the privacy legislation that is pertinent to the respective country. There are other privacy legislations that may apply to New

Zealand organizations with services online, such as the EU General Data Protection Regulation (GDPR) (Mori et al, 2022). Mori et al. (2022) noted that privacy researchers observed more than 50% of organizational privacy policies in the EU did not communicate the variety of information they collected, despite this being a requirement of the GDPR. Another piece of prominent privacy legislature is the California Consumer Privacy Act (CCPA), which is debated to be the most extensive privacy law in the United States applicable to websites (Nortwik & Wilson, 2022). In a study by Chen et al. (2021), 95 privacy policies of popular websites in the United States were examined against CCPA, and the results showed that customer's privacy rights were vague when addressing their privacy rights. The motivation for this study is to assess to what level and extent, a selection of New Zealand industry privacy statements, are in line with the New Zealand Privacy Act 2020. Within the organization websites, the privacy notices are examined using a content analysis questionnaire, with the motivation to understand how certain industries in New Zealand are communicating privacy practice information to their visiting users. In numerous studies published previously, the analysis of privacy policy material was measured against the older version of the Privacy Act 2020, the New Zealand Privacy Act 1993 (Hooper & Vos, 2009).

# 2. Literature Review

## 2.1 Privacy Policies

Online privacy statements are used as a method to provide assurance to online consumers that their personal information would not be revealed, and privacy respected (Tjhin et al, 2016). It is a common belief that privacy policies are the main way that users must keep note of an organization's privacy practices (Tjhin et al, 2016). Privacy statements on websites in general are rarely read by consumers, likely due to well-known assumption detailing that policies are difficult to comprehend (Fabian et al, 2017). Results by Fabian et al. (2017) after an analysis of 50,000 privacy policies of the most popular English-speaking websites show that on average, privacy policies in general are complex to read. This complexity undermines the idea that consumers gave their explicit agreement for the collection of their data, and arguably that consent is not implied if users had a lack of understanding for the policy (Tjihn et al, 2016). Internet users usually favor third-party seals and other options that relay data privacy practices over privacy policies (Fabian et al, 2017). In addition to the level of compliance, the nature of dubious wording used within the statements can further impair the experience of informing internet users of data-handling practices (Fabian et al, 2017).

## 2.2 The New Zealand Privacy Act

In New Zealand, the most current data privacy legislation is the Privacy Act 2020. Its purpose is to provide directions on the collection, storage, utilization and disclose of personal information and protect the privacy of individuals. The Privacy Act 2020 came into effect on the 1st of December 2020, which replaced the older Privacy Act of 1993 (Office of the Privacy Commissioner, 2013) and the older Act is frequently referenced in literature on privacy policies. Within the Privacy Act, there are thirteen privacy principles that regulate the way businesses and organizations should gather, manage, and utilize personal information (Office of the Privacy Commissioner, 2013). Principle 3 dictates the way organizations should be transparent about why they are collecting personal information and what they intend to do with it; and this includes websites (Office of the Privacy Commissioner, 2013). Office of the Privacy Commissioner (2013) states that by following this principle, the individual is informed about the purpose of collecting the personal information, and often this is through a privacy statement. The privacy statement should ensure that individuals are aware why data collection is necessary, what it will be used for, and who it will be given to, that they can access this information and correct it if required. Furthermore, Principle 5 of the Privacy Act reiterates the

requirement for storage and security of personal information, where agencies must ensure data is protected and preclude unauthorized use or disclosure of this information (Vos et al, 2020). In relation to New Zealand website content related to these principles, older literature has stated that a significant number of websites were unclear when it came to specifying the methods for the safeguard, collection, and retention of personally identifiable information with the Privacy Act of 1993 (Hooper et al, 2007). This obscurity occurred while they "retained their right to gather and exchange non personally identifiable information". Previous literature also stated that retailer websites did not provide enough information to protect consumer rights, despite privacy law in New Zealand not posing any obstacles to the growth of e-commerce (Chung & Paynter, 2002).

### 2.3 Related Work

There are several previous studies that focused on the older version of the Privacy Act in New Zealand, the Privacy Act 1993, however there is little findings of website analysis with regards to the updated Act. Mori et al. (2022) stated that analysis of legal compliance assisted by categorising the contents of a privacy statement and comparing the findings against legal standards is evident in other studies. In a paper by Hooper and Vos (2009), they examined the scope at which New Zealand websites complied with the Privacy Act 1993 to better understand the value of individuals' information privacy and the practices of handling information in New Zealand's online environment. Tjhin et al. (2016) conducted a similar study, with an analysis of privacy governance in New Zealand websites through a content analysis questionnaire. In another similar study, the privacy policies of 200 organizations within New Zealand and Facebook pages were examined by Vos et al. (2020), in which they used a content analysis questionnaire to investigate website privacy practices. The various papers noted the importance of articulating the national principles on the rights of users to privacy of their information online.

Content analysis questionnaires were used by several studies within a similar research area to thoroughly investigate privacy practices in the New Zealand online environment, and therefore comprehensively assess the components of the websites (Tjhin et al, 2016). Vorster and da Veiga (2023) conducted a research study using a quantitative data analysis methodology to examine privacy policies of websites, with the greater part of their guidelines requiring a "yes" or "no" answer. If the guideline within the questionnaire was not addressed fully, it was interpreted as not met. Mori et al. (2022) used a convolutional neural network to classify privacy policy material to evaluate compliance with legal standards. They found that legal compliance was higher in the wholesale, telecommunication, and financial industries. Finally, more than one million privacy policies were analyzed over a twenty-year period using an automated tool in a study mentioned by Vorster and da Veiga (2023). The results found that privacy statements are evolving in complexity and size, particularly lacking transparency regarding third-party data collection and tracking technologies.

## 3. Research Design and Questions

Various challenges faced by similar research studies include lack of user trust in websites and heterogeneity of industry target and range. A large amount of research on privacy statements predates social media, smartphones, and the Big Data era (Obar & Oeldorf-Hirsch, 2020). As service delivery has increased on the internet, there has been a paralleled rise in privacy concerns due to the higher potential for organization to retain, process and exploit personal information (Mutimukwe et al, 2020; Vorster & da Veiga, 2023). Concerns are rising, as a recent survey detailed over half of participants spanning 25 countries are more apprehensive regarding their online privacy than one year before (Mutimukwe et al, 2020).

Lack of user trust in an online organization perpetuates a reluctancy to share information (Busalim et, 2019). Detailed in the study by Vorster and da Veiga (2023), many users associated privacy statements with a lack of transparency about the processing and usage of personal information. An earlier paper by Hooper and Vos (2009) found that a primary reason people had not given up information to a website was due to a lack of trust, which led to fabricated personal information; trust has been an issue since long. Vagueness and a lack of straightforwardness within privacy statements are frequently found within privacy statements and policies. Many studies referred to by Chaudhury and Choe (2023) detailed that results show websites are influencing customer's decisions on data-sharing using deceptive user tactics, such as implied consent and nudging for data collection.

### 3.1 Research Questions

The following research questions address gaps in the recent literature and contribute insight into the nature of alignment with the updated Privacy Act:

1. Do privacy statements on the most visited New Zealand websites reflect the information privacy principles of the Privacy Act 2020?
2. Are government privacy statements closely aligned to the information privacy principles of the Privacy Act 2020 compared to other industries?
3. Is an effort made to address personal information security in New Zealand privacy statements?

The Government category is often precluded from privacy statement data collection due to assumed compliance, therefore this study addresses this gap directly. The study also provides insight into the specific addressing of information security on top New Zealand websites which can aid in assessing transparency and security efforts by various industries. This last inquiry is of interest because information security is not explicitly addressed in the New Zealand Privacy Act 2020 other than when discussing security of stored data in Principle 5.

### 3.2 Research Design and methods

*3.1.1 Research Instrument*

A content analysis questionnaire was used to conduct the research in this study. The content analysis technique, as stated by Hooper and Vos (2009), is used to evaluate, and analyze elements of communication and draw accurate conclusions based on the context of the data on the websites. Content analysis can be described as an objective and systematic method that is used to infer conclusions by recognizing specific attributes within content such as privacy statements (Salva & Martino, 2012). Through a content analysis questionnaire, the analyzed websites' established principles and intentions can be inferred accordingly, justified by the publicly available information being a representation of the values of the organization behind the website (Hooper & Vos, 2009). Strengths of using the content analysis technique include the flexibility of the method that is effective in both large sets of data and specific, smaller datasets (Salva & Martino, 2012). Content analysis as a methodology has been demonstrated as a reliable and productive method of attaining results (Salva & Martino, 2012).

The content analysis questionnaire was designed to analyze the alignment of various websites with the Information Privacy Principles in the New Zealand Privacy Act 2020. The content analysis questionnaire was developed without involving questions from Information Privacy Principles 4, 8, 10 and 13.

Principle 4 states that the collection of personal information must be lawful and seen as fair and reasonable in the circumstances. The manner of collection may vary greatly between organizations and is often an internal process that is not available publicly, rather implemented

through internal policies. “Lawful” and “fair” collection may differ between industries and individuals.

Principle 8 states that an organization must check if personal information is up-to-date, complete, relevant and not misleading when disclosing it. Internal checks of personal information are not inclined to be published in a privacy statement and would likely require actual communication with the website where information has been given. Given the limitations of the study, Principle 8 was omitted from the questions.

Principle 10 lists exceptions for the use of personal information not for the original obtained purpose. These exceptions are not often disclosed within privacy statements as they are informational restrictions for an organization's internal data collection uses.

Principle 13 sets various restrictions on assigning unique identifiers to individuals, and that it may only be done when it is necessary to its processes. Unique identifiers are seldom mentioned in privacy statements and are often only implemented in distinct scenarios, such as NHI numbers within New Zealand healthcare. Including Principle 13 may unfairly favor the developed question toward the Government and Healthcare fields, which often require a unique identifier.

The selection and omission of various IPPs from the questionnaire development was carefully considered. In addition to the reasons listed above, time, scope and resources prevented the questionnaire from exceeding 17 questions. However, the questions were designed to encapsulate the IPPs that would take little effort for organizations to disclose within a privacy statement. For example, Principle 6 states that individuals have the right to access their personal information held by the organization. This principle can be easily explicitly stated without revealing any internal processes that the organization may have and is fundamental and important information for an individual to know when accessing the website.

Various questions may address more than one IPP, and this is because there is often overlap between the content of the principles. For example, Question 2 on the content analysis questionnaire asks if the purpose of information collection is stated. This addresses both Principle 1 (organizations must only collect information for a lawful purpose connected to their functions), and Principle 3 (what to tell the individual about collection). Due to the nature of language and the expression of business activities across industries, an overlap of acknowledgement of the Privacy Act is to be expected, and this was considered when developing the questions. There were seventeen questions formed for this purpose, that were based upon one or many principles. Answers were either a “Yes” or “No” for each question. If a keyword from the question was not mentioned, or the answer was not explicitly stated, it was regarded as a “No”. The selected websites generally did not have to delve into detail to warrant a “Yes” on the questionnaire; primarily they had to acknowledge the principle in some way, with some exceptions as detailed in the Findings section.

*3.1.2 Sample and Data Collection*

120 websites were selected and measured against the above content analysis questionnaire. 96% of websites sampled contained a privacy statement and were able to be analyzed.

The content analysis was performed on a sample of the most visited New Zealand websites in July 2023, using the website Semrush “semrush.com”. The websites were selected according to the six different categories on the Semrush website: “Retail”, “Banking”, “Travel and Tourism”, “Government”, “Healthcare” and “Entertainment”.

The Top 20 websites visited in each category listed above were selected for the study. The scope for domain selection was limited to extensions of “.co.nz”, “.org.nz” and “.govt.nz”. As

the objective was to examine the privacy practices of the most visited websites in the New Zealand online environment, websites void of privacy statements were still selected for the study. If a privacy statement could not be located on the website, the data collected was a "No" for all research questions.

*3.1.3 Content Analysis*

To be regarded as a privacy statement, the body of text or hyperlink needed to be titled similar to "privacy statement" or contain the word "privacy". Alternatively, if the privacy statement was found inside the "Terms of Conditions" or similar, it was still regarded as a statement on the privacy values, and therefore considered as the "privacy statement" of the organization and was included in the study. Organizations with websites void of a body of text containing "Privacy" in the title were not considered.

To locate the privacy statement on the selected websites, several steps were taken and recorded to create reasonable judgement. Where there was a lack of direct link to a privacy statement found on the homepage of the website, the following steps were taken: 1) The terms and conditions were located and checked (if present), and 2) A search was performed in the website search bar for the world "privacy" (if present), and 3) A search was performed in Google with the website name and the word "privacy" (a check was then performed to ensure the domain was the same). Following these steps, there were no further actions to locate the privacy statement of the website, and the content analysis questions were all answered with "No". All privacy statements that were sampled for the study were subject to seventeen content analysis questions.

## 4. Findings

The highest alignment percentage of 92.5% with the Privacy Act was regarding Principle 2; *Is the information collected directly from the individual?* It was evident that most websites stated explicitly that they collect information directly from the user themselves, and many also stated the circumstances in which it was not directly collected from the individual.

Alternatively, the lowest alignment percentage of 42.5% with the Privacy Act was regarding Principle 12; *Is disclosure of personal information to an organization outside of New Zealand stated?* Most organizations did not state whether information would be disclosed overseas, rather that it would be disclosed to "third parties".

### 4.1 Information Privacy Principles: Questionnaire Analysis

17 questions were developed and designed from various Information Privacy Principles in the Privacy Act 2020. The specific IPP(s) addressed, and the data collected per question gives insight into the alignment levels of the sampled websites.

**Question 1:** *Does the website contain a privacy statement?* This question addressed Principle 3 of the Privacy Act. Approximately 96.7% of websites contained a privacy statement on their website.

**Question 2:** *Is the purpose of information collection stated?* This question addressed Principles 1 and 3 of the Privacy Act. Most websites directly addressed the purpose of which they were collecting information at 85%.

**Question 3:** Is it stated whether the data collection is compulsory or voluntary? This question addressed Principle 3 of the Privacy Act. Approximately half of websites did not state whether data collection was compulsory or voluntary, and consent was assumed.

**Question 4:** *Is it stated the consequence of not providing the information?* This question addressed Principle 3 of the Privacy Act. Approximately half of websites did not state the consequences for not providing information (48.3%), closely aligning with Question 3.
**Question 5:** *Is the information collected directly from the individual?* This question addressed Principle 2 of the Privacy Act. Most websites did state that the information was collected directly from the individual, with a large amount also mentioning the case in which it would not be directly collected.
**Question 6:** *Are the names of the collecting agencies stated?* This question addressed Principle 3 of the Privacy Act. Approximately 85% of websites stated the names of the collecting agencies.
**Question 7:** *Are the addresses of the collecting agencies stated?* This question addressed Principle 3 of the Privacy Act. In contrast to Question 6, only 59.2% of websites accompanied the name of the collecting agency with an address.
**Question 8:** *Are the names of the holding agencies stated?* This question addressed Principle 3 of the Privacy Act. Holding agencies were mentioned occasionally, however 24.2% of websites failed to disclose this information.
**Question 9:** *Are the addresses of the holding agencies stated?* This question addressed Principle 3 of the Privacy Act. The addresses of the holding agencies were mentioned by just over half of all websites selected.

| QUESTION NO. | PRINCIPLE NO. ADDRESSED | QUESTION | YES | NO | % "YES" |
|---|---|---|---|---|---|
| 1 | 3 | Does the website contain a privacy statement? | 116 | 4 | 96.7% |
| 2 | 1, 3 | Is the purpose of information collection stated? | 102 | 18 | 85% |
| 3 | 3 | Is it stated whether the data collection is compulsory or voluntary? | 59 | 61 | 50.8% |
| 4 | 3 | Is it stated the consequence of not providing the information? | 62 | 58 | 51.7% |
| 5 | 2 | Is the information collected directly from the individual? | 111 | 9 | 92.5% |
| 6 | 3 | Are the names of the collecting agencies stated? | 102 | 18 | 85% |
| 7 | 3 | Are the addresses of the collecting agencies stated? | 71 | 49 | 59.2% |
| 8 | 3 | Are the names of the holding agencies stated? | 91 | 29 | 75.8% |
| 9 | 3 | Are the addresses of the holding agencies stated? | 73 | 47 | 60.8% |
| 10 | 11 | Has the website stated the purpose for disclosing information to other agencies? | 82 | 38 | 68.3% |
| 11 | 5 | Are there safeguards in place to prevent loss or misuse of information collected? | 97 | 23 | 80.9% |
| 12 | 3,6 | Can people request access to their personal information? | 106 | 14 | 88.3% |
| 13 | 6 | If there are restrictions to accessing personal information, is the reason stated? | 50 | 70 | 58.3% |
| 14 | 3,7 | Can people correct their personal information? | 105 | 15 | 87.5% |
| 15 | 9 | Is the length of retention time of personal information for the purpose stated? | 58 | 62 | 48.3% |
| 16 | 12 | Is disclosure of personal information to an organization outside of New Zealand stated? | 51 | 69 | 42.5% |
| 17 | 3 | Is the Law under which personal information is required to be collected explicitly stated? (e.g. Tax Act) | 67 | 53 | 55.8% |

**Table 1.** Privacy Act Questions and Corresponding Answers from Most Visited New Zealand Websites

**Question 10:** *Has the website stated the purpose for disclosing information to other agencies?* This question addressed Principle 11 of the Privacy Act. A lower number of websites at 68.3% addressed the purpose for disclosing information to other agencies. Often there was only observed to be a statement on which third parties would be disclosed such information, however no reason accompanied.
**Question 11:** *Are there safeguards in place to prevent loss or misuse of information collected?* This question addressed Principle 5 of the Privacy Act. 80.9% of websites addressed that there were security measures in place, however most websites did not state any specific safeguards.
**Question 12:** *Can people request access to their personal information?* This question addressed Principle 3 and 6 of the Privacy Act. Approximately 88.3% of websites explicitly stated that personal information can be accessed, usually accompanied by an email or address.
**Question 13**: *If there are restrictions to accessing personal information, is the reason stated?* This question addressed Principle 6 of the Privacy Act. Almost half, 41.7% of websites did not state if there were restrictions to accessing personal information.
**Question 14:** *Can people correct their personal information?* This question addressed Principle 3 and 7 of the Privacy Act. Most websites detailed that personal information could be corrected, usually stated in line with Question 12.
**Question 15:** *Is the length of retention time of personal information for the purpose stated?* This question addressed Principle 9 of the Privacy Act. Over half of websites did not address retention time of personal information (51.7%).
**Question 16:** *Is disclosure of personal information to an organization outside of New Zealand stated?* This question addressed Principle 12 of the Privacy Act. Most websites, 57.5%, did not state whether personal information would be disclosed overseas for any reason.
**Question 17:** *Is the Law under which personal information is required to be collected explicitly stated? (e.g. Tax Act).* This question addressed Principle 3 of the Privacy Act. A low number of websites addressed the Privacy Act 2020 at all, and there were several websites that addressed it incorrectly due to a variety of reasons.

The number of websites that aligned with the principles is shown to be generally varied with each question asked, with particular questions, such as Question 16, having a high misalignment with the accompanying principle (IPP 9). The answers show clear priorities in being explicitly aligned with the Privacy Act, while lacking in addressing other areas.

### 4.2 Discussion

Further analysis was performed to compare the six different industries targeted in this research: Retail, Banking, Travel and Tourism, Government, Healthcare and Entertainment. Question 17 on the questionnaire is detailed: *Is the Law under which personal information is required to be collected explicitly stated? (e.g. Tax Act).* If the New Zealand Privacy Act was not mentioned, it was regarded as a "No", even if other Laws were mentioned, as the website is still subject to the Privacy Act as an organization operating in the New Zealand online environment. Similarly, if the correct year was not mentioned, or there was no year listed at all, it was also regarded as a "No".

Question 17 was not addressed or addressed incorrectly by 44.2% of all selected websites. Websites that earned a "No" answer on the questionnaire for Question 17 were split up by Reason in Table 2. This table shows the percentage of websites that did not comply with this subsection of Principle 3 of the Privacy Act and the reasons observed.

52.8% of these websites did not address the Privacy Act 2020 at all, and various other reasons for earning a "No" for Question 17 include addressing the old Act (Privacy Act 1993), no year

stated and stating other laws such as GDPR but lacking a statement on New Zealand privacy legislation. An interesting observation about Question 17 is the lack of explicit statement of the New Zealand Privacy Act 2020. Many websites fail to mention the Act, but rather would state “relevant privacy legislation”, “New Zealand legislation”, or simply “Privacy Act”. Many of the privacy statements had not been updated since the release of the new Act that replaced the old Privacy Act of 1993. The selected websites seem to portray the acknowledgement of the word "privacy" as an organization with a New Zealand domain as enough regard for the Act itself. The explicit statement of New Zealand privacy law is an area requiring improvement.

Question 11 addressed Principle 5: *Are there safeguards in place to prevent loss or misuse of information collected?* The websites (80.9%) that contained a statement on safeguards were analyzed further on the level of specificity their statement contained. Figure 1 shows the percentage of privacy statements against two criteria:“Specific” and “Non-Specific”. Websites were classified as having “Specific” safeguards if they stated any detailed security processes or protocols, for example, encryption methods, internal procedures, or physical security measures. Otherwise, a generic statement earned a “Non-Specific” in the data collection.

| REASON FOR “NO” | COUNT OF “NO” | % OF “NO” |
|---|---|---|
| **NOT ADDRESSED** | 28 | 52.8% |
| **ANOTHER LAW ADDRESSED** | 12 | 22.6% |
| **OLD NZ ACT ADDRESSED** | 9 | 16.9% |
| **NO YEAR STATED** | 4 | 7.5% |

*Note.* The count of “NO” is derived from n=53 expressed in Question 17.

**Table 2.** Reasons for Failure to address Question 17

Information security is not specifically addressed in the New Zealand Privacy Act 2020; there is no legal requirement stated on how specific organizations need to be when disclosing the safeguards put in place to protect personal information. The 5$^{th}$ principle states that information should be protected “by such security safeguards as are reasonable in the circumstances to take”, which in its articulation, lacks a distinctness that is essential when addressing security. The Privacy Act states that reasonable security safeguards must be in place to prevent loss, access, use, modification, disclosure that is not authorized by the organization. Most websites directly quoting the Privacy Act were ambiguous, using statements such as “We will take reasonable steps to ensure personal information is protected from loss, misuse, disclosure or modification.”.

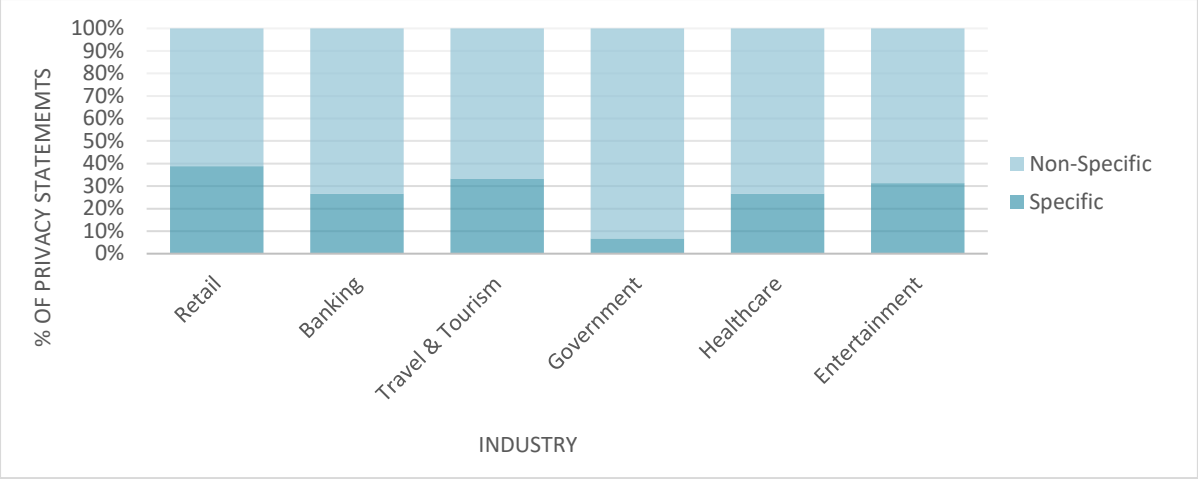


**Figure 1.** Specificity of Personal Information Safeguards

In Figure 1, we observe that 70 out of 97 of selected websites that had a safeguard statement, did not state what specific safeguards were in place to protect personal information. This indicates that around 71% of websites did not specify information security best practices such as encryption methods, employee training or security of servers storing information. Rather, user blame was high amongst all selected websites; emphasis was placed on the user's responsibility in protecting their information and displacing responsibility onto the user of the website if any security breach were to occur. The largest number of non-specific safeguards mentioned in privacy statements was from the Government sector, followed by the Healthcare and Banking industries. However, all industries were observed to have poor details of their actual security practices.

The assumption that government websites, particularly New Zealand government websites (that primarily have an extension of ".govt.nz") are more trustworthy and transparent in their respective privacy statements is challenged within the results of the study. Figure 2 displays the spread of "Yes" vs. "No" responses to all seventeen questions in the content analysis questionnaire in the Government industry.

Figure 2 shows that only Questions 1 and 5 were fully addressed by the selection of Government websites. Question 16, which is regarding the disclosure of personal information to overseas agencies, is a poorly addressed area in the Government sector. This is closely followed by Question 13, regarding restrictions to accessing personal information. This is arguably an important question to address, as government websites receive a wide variety of personal information, such as employment, immigration, criminal, and financial data. If there are restrictions to accessing such sensitive information about individuals, it should be explicitly stated. The Government sector was observed to have the greatest number of websites that did not state *specific safeguards* for protecting personal information. The statements were noted to be generic and ambiguous if any were stated at all.

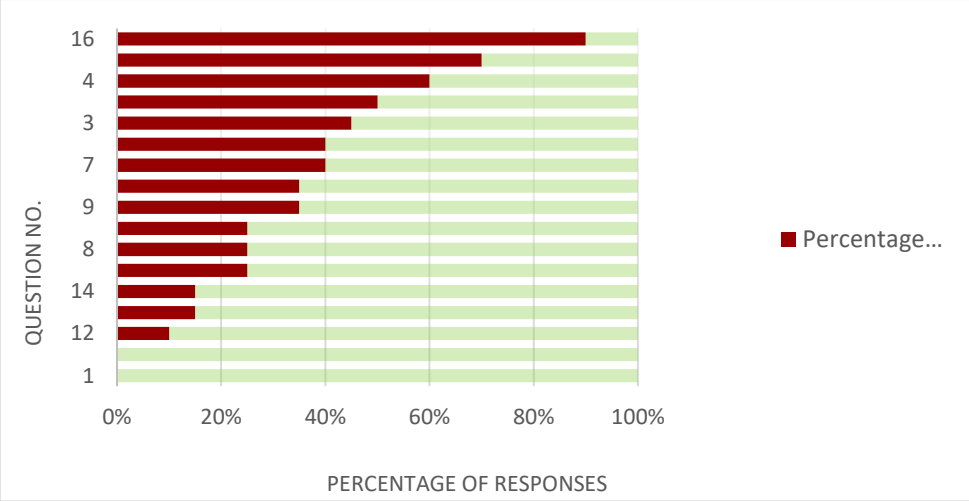


**Figure 2.** Government Privacy Statements: Bridging the Gap in Perception

## 5. Conclusions

The purpose of this study was to research the extent of alignment of a sample of New Zealand websites' privacy statements with the Privacy Act 2020. The Privacy Act defines the principles of privacy for users in the New Zealand online environment, and therefore provides an accurate basis for the content analysis questionnaire used in this study. The first research question addressed whether privacy statements on the most visited New Zealand websites can reflect the privacy principles in the latest New Zealand Privacy Act. This was not supported by the data collected, due to the fluctuating nature of explicit content. None of the questions were addressed by 100% of the examined sites, however in addition, the percentage of non-coverage was sometimes as low as 40%.

The second research question addressed whether the Government sector contained privacy statements that are closely aligned to the Act compared to other industries – and this was also not supported. The Government sector consistently assumed that the user could refer to the Privacy Act itself, and these sites also had a high level of non-coverage for multiple questions on the questionnaire. The third research question addressed whether efforts were made to specify personal information security. Little to no effort was made by most websites to address the security of personal information in detail, and the ambiguity of their statements point toward the generalized statement in the Privacy Act itself. Improvements are needed to ensure that users are aware of how their information will be protected.

### 5.1 Limitations and Future Work

A sample of the Top 120 New Zealand websites were selected for the study. Limitations include that the findings from these websites could not draw definite and conclusive results that represent all New Zealand websites with privacy statements. A bigger sample size would need to be obtained to represent the population of privacy statements more accurately in New Zealand. Another limitation is that the representation of industries was limited to only six: Retail, Banking, Travel & Tourism, Government, Healthcare and Entertainment.

Privacy statements that model the Privacy Act 2020 and any future Acts need to have a profile of elevated prominence for users to observe them more and raise user trust in organizations.

From the findings of this study, it is evident that even the most visited New Zealand websites have not established a strong correlation between articulated content in their privacy statement and its potential to guide customer behavior through the promotion of their privacy values. A positively framed privacy statement that avoids user blame and displaced security responsibility may be a good starting area for improvement. Future work could include assessing governmental privacy statement practices against the non-profit industry in attempt to draw insights into the private and public sector relationships with New Zealand privacy legislation. Further research into published privacy statements against the organizations' real practices would be a significant insight into the importance of how privacy legislation needs to be refined.

## References


Busalim, A., Hussin, A., & Iahad, N. (2019). Factors influencing Customer Engagement in Social Commerce Websites: A Systematic Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research, 14*(2), 1-14. https://dx.doi.org/10.4067/S0718-18762019000200102

Chaudhury, R. D., & Choe, C. (2023). Digital Privacy: GDPR and Its Lessons for Australia. *Australian Economic Review*, *56*(2), 204-220. https://doi.org/10.1111/1467-8462.12506

Chen, R., Fang, F., Norton, T., McDonald, A. M., & Sadeh, N. (2021). Fighting the fog: Evaluating the clarity of privacy disclosures in the age of ccpa. *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, 73-102. 10.1145/3463676.3485601

Chung, W., & Paynter, J. (2002). Privacy issues on the Internet. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 1-9. https://doi.org/10.1109/HICSS.2002.994191

Dehling, T., Gao, F., & Sunyaev, A. (2014). Assessment Instrument for Privacy Policy Content: Design and Evaluation of PPC. *Proceedings of the Pre-ICS Workshop on Information Security and Privacy*, 1-16. https://papers.ssrn.com/abstract=2646460

Fabian, B., Ermakova, T., & Lentz, T. (2017). Large-scale readability analysis of privacy policies. *Proceedings of the International Conference on Web Intelligence*, 18-25. https://doi.org/10.1145/3106426.3106427

Hooper, A., Bunker, B., Rapson, A., Reynolds A., & Vos, M. (2007). Evaluating Banking Websites Privacy Statements – A New Zealand Perspective on Ensuring Business Confidence. *PACIS 2007 Proceedings.* https://aisel.aisnet.org/pacis2007/25/

Hooper, T., & Vos, M. (2009). Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices. *Online Information Review*, *33*(2), 343-361. https://doi.org/10.1108/14684520910951258

Mori, K., Nagai, T., Takata, Y., & Kamizono, M. (2022). Analysis of Privacy Compliance by Classifying Multiple Policies on the Web. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1734-1741. https://doi.org/10.1109/COMPSAC54236.2022.00276

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behaviour. *Government Information Quarterly*, *37*(1). https://doi.org/10.1016/j.giq.2019.101413

Nortwick, M., & Wilson, C. (2022). Setting the Bar Low: Are Websites Complying with the Minimum Requirements of the CCPA? *Proceedings on Privacy Enhancing Technologies*, 608–628. https://doi.org/10.2478/popets-2022-0030

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Office of the Privacy Commissioner. (2013). Privacy Act 2020 and the Privacy Principles. https://www.privacy.org.nz/privacy-act-2020/privacy-principles/

Privacy Act 2020. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html

Savla, P., & Martino, L. D. (2012). Content Analysis of Privacy Policies for Health Social Networks. *2012 IEEE International Symposium on Policies for Distributed Systems and Networks*, 94-101.10.1109/POLICY.2012.20.

Tjhin, I., Vos, M., & Munaganuri, S. (2016). Privacy Governance Online: Privacy Policy Practices on New Zealand Websites. *Pacific Asia Conference on Information Systems.* https://www.semanticscholar.org/paper/Privacy-Governance-Online%3A-Privacy-Policy-Practices-Tjhin-Vos/4a2dc7fac576b8f9d7523c0f5de2036eec866c22

Vorster, A., & da Veiga, A. (2023). Proposed Guidelines for Website Data Privacy Policies and an Application Thereof. *Human Aspects of Information Security and Assurance, 674,* 192-210. https://doi.org/10.1007/978-3-031-38530-8_16

Vos, M., Hu, M., & Du, B. (2020). Privacy on Facebook Brand Pages: A Content Analysis Study of New Zealand Organisations. *ACIS 2020 Proceedings.* https://aisel.aisnet.org/acis2020/53/