

‘Protection of privacy and New Zealand libraries: Is digital just different?’

by

Thomas Nixon

Submitted to the School of Information Management,
Victoria University of Wellington
in partial fulfillment of the requirements for the degree of
Master of Information Studies

October 2017

Abstract

With the development and uptake of digital technologies, threats to privacy change rapidly. This research measures the level of concern for privacy among New Zealand librarians in different contexts, as well as the level of confidence in libraries' current practices with regard to mitigating privacy issues surrounding digital services. Likert scale data was collected through an online survey which received 135 completed responses, and statistical analysis carried out to determine if there were differences between a) concern for privacy in offline contexts, b) concern for privacy in digital services and c) confidence in libraries' current privacy protection practices. Support was found for the hypotheses that concern for privacy was lower in the context of digital services than in offline contexts, and that in the context of digital services confidence in practices was lower than the level of concern. The findings suggest a need for changes to privacy protection practices in New Zealand libraries.

Keywords: Privacy concern, New Zealand libraries, Library 2.0, privacy protection

Introduction

Privacy rights controversies abound throughout the world. These have included the mass surveillance undertaken by the United States' National Security Agency on the communications of both US and other populations, including their social media activity (Parsons, 2015; van Dijck, 2014). Other threats stem from the prevalence of an array of tracking technologies in use on most popular websites (Fortier & Burkell, 2015).

Another area where privacy rights are potentially threatened is within libraries and through the services that libraries provide, such as the provision of internet facilities and through library 2.0 services (Campbell & Cowan, 2016). Examples of library 2.0 services with potential privacy risks include online messaging "ask a librarian"-type service type services, wikis and blogs, linking to social media sites such as Facebook, and social media type tagging applications such as GoodReads (Zimmer, 2013b; American Library Association, 2016). Privacy risks can also arise from services such as third-party provider ebooks and electronic journals, and the provision of internet access (Corrado, 2007).

Libraries have a tradition of protecting privacy that dates back at least to 1939, when the American Library Association adopted the Library Bill of Rights, seeking to protect intellectual freedom and the privacy which helps such freedom to flourish (Zimmer, 2014). In this context, "privacy" is generally taken to mean information privacy, which Westin (2003, p. 431) describes as an

individual's claim to the ability to determine what is known about himself or herself.

Privacy issues surrounding technology evolve rapidly, and little published research on the problem exists (Zimmer, 2014), creating the situation in which the current status of libraries' ability to uphold privacy rights is not known.

Librarians as a group are concerned with privacy (Zimmer, 2014), and yet when technological tools which have the potential to harm privacy are discussed in library literature, privacy issues are rarely a focus and often go unmentioned (Zimmer, 2013a). In the context of this apparent misalignment of literature output as compared to the level of concern, the present research aims to gain a picture of New Zealand librarians' and library workers' attitudes about privacy and privacy protection.

Specifically, three conditions were measured: level of concern for privacy in general (i.e. in offline contexts), the level of privacy in the context of the specified digital services, and the level of confidence in practices to mitigate privacy issues employed in relation to those specified digital services. Analysis of these three conditions was carried out to find if there are differences between them. (See under "Data collection" below for the digital services specified).

If significant differences are found between the conditions, this could be of immediate importance to the profession, as it would suggest that New Zealand librarians and library workers do not feel they have the ability to protect patrons' privacy during the provision of digital library services. Such data would be useful to the profession of librarianship in understanding current attitudes to privacy and digital services, and in planning and designing future training and awareness programmes and privacy protection solutions.

The present research aims to help guide policies of New Zealand libraries, the Library and Information Association of New Zealand Aotearoa ("LIANZA"), and education providers by helping determine to what extent librarians and library workers believe that libraries are currently equipped to uphold privacy rights in digital contexts.

Studies of privacy concern have formed a significant part of research into privacy, but a

predominance of US-based and student-centred studies means there is a need for research on different populations (Belanger & Crossler, 2011). The data collected in the present research helps to meet that need. Furthermore, these studies have tended to examine differences in levels of concern between different demographic groups or to explain the effect of privacy concern on certain behaviours (Belanger & Crossler, 2011). The present research therefore makes a unique contribution by comparing the level of concern in offline contexts with digital contexts, and by testing librarians' confidence that current practices are adequate for their level of concern.

Background

Privacy is important because “rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship” (American Library Association, 2014), and it is also guaranteed as a right under the Universal Declaration of Human Rights (UN General Assembly, 1948).

But with the advancement and popularisation of new technologies, new challenges to privacy emerge and librarians have not always met these challenges effectively (Corrado, 2007; Fortier & Burkell, 2015). Library literature on these new technologies has focused primarily on the benefits to be gained, with privacy issues being largely ignored (Zimmer, 2013a).

Privacy must be balanced with other factors, but in order for privacy rights to be protected, a person must be in a position to make an informed choice with reasonable alternatives (Campbell & Cowan, 2016). Faced with the difficulty of understanding privacy issues and a lack of reasonable alternatives, making judgements often becomes too difficult (Malaga, 2014). This can lead people to sometimes react by avoiding the issues despite concerns, and continue with un-analysed behaviours (Malaga, 2014).

Literature Review

The first scholar to extensively study privacy attitudes was Westin (2003). He describes privacy, in the context of information privacy, as “the claim of an individual to determine what information about himself or herself should be known to others” (paraphrasing Westin, 1967). He broadens this

description to include claims of groups and associations, and governments. “Privacy rights”, under this framework, are derived when these claims gain the protection of law and convention.

Privacy is a right

The Universal Declaration of Human Rights states that “No one shall be subjected to arbitrary interference with his privacy.... Everyone has the right to the protection of the law against such interference or attacks” (UN General Assembly, 1948). In New Zealand law, the right to information privacy is protected by the Privacy Act 1993. The Act does not define the term privacy, but works to regulate how, from whom and for what purpose agencies collect personal information, and establishes people’s right to access their information and to make corrections of errors.

Privacy protection is a library ethic

The centrality of privacy protection to the role of librarians is reflected by its place among the American Library Association’s (2004) Core Values of librarianship. Campbell and Cowan (2016) explore the importance of privacy in libraries and its role in intellectual freedom, with the example of members of the lesbian, gay, bisexual, transgendered, or questioning (LGBTQ) community using information resources in the process of exploring their identities and the process of ‘coming out’. They find that Big Data can present a threat to the privacy of people undergoing this process, by analysing their browsing behaviour and serving them ads which ‘out’ them to themselves at times before they have even come to a self-realisation of sexual identity. But many library offerings, such as those associated with social media, compound the threat that Big Data presents to privacy. The authors recommend the development of more privacy-friendly technologies, such as linked-data over Big Data, and that new technologies not be adopted without careful consideration of privacy implications (Campbell & Cowan, 2016).

Fortier and Burkell (2015) explore the related phenomenon of behavioural tracking and describe the various tools employed, such as HTTP cookies, Flash cookies and web beacons. The authors present tools for discovering and limiting behavioural tracking, and encourage librarians to take a role in enabling patrons to protect themselves against it.

In a multi-disciplinary literature review, Magi (2011) identifies the many benefits of privacy which have been written about in scholarly literature of many disciplines. The literature discussed highlights the fact that privacy benefits not only the individual, but also delivers many benefits to society and to interpersonal relationships.

Lamdan (2015) argues that librarians are exceptionally well placed to advocate for privacy in social media due to their history of privacy protection, their knowledge as information experts and their professional associations with common guiding principles.

New Zealand research on attitudes to privacy

Much of the descriptive research done in New Zealand has focused on behaviour rather than attitudes, but as a product of such research Lips and Eppel (2016) developed a new taxonomy of information-sharing behaviours in which all the identified classifications described people that were highly conscious of privacy.

In a study with the aim of testing theories of the underlying basis of concern for information privacy by comparing data collected in New Zealand with existing data collected from people in a different regulatory environment (the US), Rose (2006) used random sampling of the New Zealand electoral roll to select individuals to whom a survey on information privacy concern was mailed. The questions were drawn from an established survey instrument used in previous studies, known as CFIP (Rose, 2006). The large, random sample size, the use of an established survey instrument, and the data analysis techniques used make this a rigorous study yielding useful data and a well grounded conclusion. The study found support for an alternative to Westin's theory of control as the basis of privacy, Moor's control/restricted access theory.

The control/restricted access theory states that control over whether to release information is not enough to ensure privacy, but that a normative and regulatory framework must exist to ensure that access to personal data after it has been handed over remains restricted to the persons and purposes for which it was intended (Moor, 1997; Appel, 2010). Rose (2006), in the study mentioned above, argues that the New Zealand regulatory framework, under the Privacy Act 1993, satisfies this condition of restricted access in a way that the US framework does not. This more protective regulatory

environment in New Zealand may be a cause of the relative lack of aggressive defences of privacy by New Zealand librarians, compared to their US counterparts who are in a more embattled privacy environment. Many digital threats to privacy know no borders however, and in the case of the online privacy environment there may be less distinction between the two countries.

Previous research on privacy concern and librarians' attitudes towards privacy

In a review of information privacy research, Belanger & Crossler (2011) identify two well-established survey instruments that have been used in the study of privacy concern, the Concern for Information Privacy ("CFIP") and the Internet User's Information Privacy Concern ("IUIPC") instruments. A recommendation of the review is that justification should be given where these instruments are used in research, and that other instruments should be developed.

Corrado (2007) conducted a small study on librarians' attitudes entitled "Privacy and Library 2.0." The study took the form of a survey advertised through various email lists aimed at librarians, and obtained 110 responses. The great majority of responses were from the US, but a few came from other countries. A limitation identified in the study was the small sample size in relation to a large population of librarians within the US and abroad, indicating a low level of representativeness.

A finding that stood out was that 84.5% of respondents assigned a high or very high importance to privacy, but less than half of these worked in libraries with a privacy policy available online. Another was that 75.5% of respondents believe that librarians should teach patrons about issues relating to privacy (Corrado, 2007). Recommendations included that future studies attempt to achieve a more representative sample, and that age demographic information be collected.

Zimmer (2013a) undertook a content analysis of all articles discussing Library 2.0 in library related professional publications from 2005 – 2011, in order to determine the number that mention privacy, the importance placed on privacy when it was mentioned, and whether any solutions were offered (Zimmer, 2013a).

The main findings were that of 677 articles on Library 2.0, only 39 (5.8%) discussed privacy at

all, and that of these, only 14 offered solutions. This despite the fact that in articles where privacy is mentioned, over half indicated a moderate or high level of concern (Zimmer, 2013a). This appears to present a disconnect in the library literature between the level of concern about privacy, and the amount of resources devoted toward confronting the issue.

There is no published research on the privacy attitudes of New Zealand librarians. LIANZA is less vocal about the importance of privacy than the American Library Association and the International Federation of Library Associations and Institutions, but it does have a statement guiding New Zealand Library and Information professionals on how they should treat personal data to protect privacy in accordance with the Privacy Act 1993 (LIANZA, 2013).

Theoretical framework and considerations

Implicit in the present research is the assumption that attitudes and levels of concern and of confidence can be measured through a questionnaire. But no theoretical perspective on the nature of privacy or the underlying basis of privacy concern is specified. Rather, the research aims to establish whether there are differences between the three conditions of privacy in the offline context (Condition 1), privacy in the context of the specified digital services (Condition 2) and degree of confidence in library practices for mitigating privacy issues in relation to those digital services (Condition 3). On the basis of evidence that little emphasis is placed on privacy threats and their solutions when dealing with digital technologies in the literature outlined in Zimmer (2013a), seemingly in contrast with libraries' history of privacy protection, it is hypothesised that Condition 2 is lower than Condition 1, and Condition 3 lower than Condition 2. If it is found that Condition 3 is substantially lower than Condition 2, this would demonstrate that librarians and library workers do not feel they are adequately equipped to mitigate privacy threats in digital services, with implications for the traditional role of protecting citizens' privacy. Also, a finding that differences were present would provide data useful in the future study of causes of these differences.

Method

The present research applies a quantitative, rather than a qualitative, approach. The aim is to come as close as possible to an understanding of the privacy attitudes of the population of New Zealand

librarians and library workers in general, and whether there are differences between the three conditions of General Concern, Web Concern and Confidence in Practices. This aim is best served through a large sample size and the application of statistical tests which would be difficult to achieve with qualitative methods. While the characteristics to be studied would be difficult to observe directly, being attitudes and feelings such as level of confidence, such characteristics can be usefully measured using survey research (Leedy & Ormrod, 2013, p. 189).

The survey method employed was to create an online questionnaire. The survey primarily uses Likert scale questions, as these are useful for measuring responses on a continuum (Leedy & Ormrod, 2013, p. 192), but with additional nominal questions for demographic data such as gender, age, type of library, and job description, as well as a more open question calling for any further comments. The inclusion of an open question in the survey could allow the approach to be described as one of “mixed methods”, but this data was used primarily to aid in understanding responses and was not a strong focus of the research.

In order to identify appropriate digital services on which to base survey questions, an environmental scan of potentially privacy damaging services in libraries was undertaken. Ideas produced in this process were then discussed in informal interviews of librarians to check their suitability.

Research questions

The main research questions are:

1. To what extent is the level of concern librarians and library workers have for privacy in general different to their level of concern in the context of specified digital services?
2. To what extent are librarians and library workers confident that their privacy protection practices are appropriate in the context of these digital services?

The sub-questions are:

1. What is the level of concern librarians and library workers have for privacy in general?
2. What is the level of concern librarians and library workers have in the of context specified digital services?

3. What is the level of confidence librarians and library workers have that their privacy protection practices are appropriate in the context of these digital services?

Hypothesis H1: The target population has a level of concern about privacy in general that is higher than their level of concern about privacy with regard to specified digital services.

Hypothesis H2: The target population has a level of concern about privacy with regard to specified digital services that is higher than their level of confidence that their privacy protection practices are appropriate in the context of these digital services.

H1 and H2 are non-conflicting hypotheses, so it is expected that support for one or both may be found, or neither.

Null Hypothesis H0a: The first null hypothesis is that no statistically significant differences exist between Conditions 1 and 2: concern for privacy is equal in the offline and digital contexts.

Null Hypothesis H0b: The second null hypothesis is that no statistically significant differences exist between Conditions 2 and 3: within the specified digital contexts confidence in mitigating practices matches level of concern.

Sampling and population

The target population for the proposed study is all New Zealand library workers and holders of New Zealand library-related tertiary qualifications. The size of this population is difficult to estimate. According to Careers New Zealand (2016) the number of people working as librarians in New Zealand was 4,943 in 2014. The target population is clearly considerably greater than this.

As it is not feasible to obtain sample data from all members of this population, it is necessary to select a sample for study. In order for this sample to provide data upon which it is possible to base generalisations about the population, the sample must be representative (Leedy & Ormrod, 2013, pp. 206-207). Therefore an attempt should be made to ensure a sample of sufficient size.

As discussed in Leedy and Ormrod (2013, pp. 215-216), Gay, Mills and Airasian (2009) estimate that for a population size of over 5000, a sample size of 400 is sufficient.

The data collection method adopted for the present research was to create a questionnaire, using Qualtrics survey software, and to send requests for online participation by email to all the libraries

listed in the Directory of New Zealand Libraries maintained by the National Library of New Zealand. The Directory is described as providing locations and contact details of all New Zealand libraries (National Library of New Zealand, n.d.). Where the details of the library manager was given in the directory, the emailed requests were sent to these and asked recipients to consider completing the online survey and inviting their colleagues to do the same.

Finally, the survey was further promoted through the library-related email discussion groups and mailing lists NZ-Libs, PUBSIG-L, Schoollib, SLIS-NZ and TeL-SIG.

Data collection

Data was collected by means of a survey instrument designed specifically for the purpose. The instrument was based on sections of the survey conducted by the American Library Association and published in Zimmer (2014). While established and tested survey instruments for measuring concern about privacy do exist, none was found that could be readily adapted to the context of libraries. Instead, the 17-question “General Privacy Attitudes 1” section of the American Library Association survey was taken as the basis of the present survey. This section bears considerable resemblance to the CFIP instrument, notably including questions on the control, collection, intended purpose and unauthorised access of information. From this, the four questions relating to the internet were removed, leaving 13 questions whose language was localised and to which a clause specifying an offline context was added to derive Section 3 of the present survey. Sections 4 and 5 were based as closely as possible on Section 3.

The survey consists of five sections, the first two of which collected nominal data on demographic information and on relevant services offered in the respondent’s library respectively (in section 2, respondents were asked to check boxes for each of the following offered at their library: Goodreads or other social cataloguing, Facebook, Twitter or similar SNS, internet facilities, wifi, OPAC, electronic journals, ebook lending, and “ask a librarian”-type services). The remaining three sections elicited the degree to which respondents agree with certain statements, through a seven-point Likert scale.

Section 3 was identified as General Privacy Attitudes and is adapted from the survey published

in Zimmer (2014).

Table 1. General Privacy Attitudes

<p>This section relates to privacy in all aspects of life while not engaged with an internet-connected device.</p> <p>Clarification of terms: "Personal information".</p> <p>Examples of "personal information" in this section may relate to political or personal views, interests and hobbies, images and biometrics data, purchase and banking records, medical records, physical movements, content of conversations, information in contracts, personal associates, business associates etc., where these could potentially be linked at some time with the individual.</p> <p>In questions referring to libraries/librarians, examples of "personal information" may include lending records and content of inquiries etc.</p> <p>Please indicate the degree to which you agree with the following statements:</p>
1. Individuals should be able to control who sees their personal information which was generated offline.
2. I am concerned that companies are collecting too much personal information about me or other individuals engaged in offline activity.
3. I am concerned that government agencies are collecting too much personal information about me or other individuals engaged in offline activity.
4. Government agencies should not share personal information with third parties unless it has been authorised by the individual or by a court of law.
5. Librarians are actively working to prevent unauthorised access to individuals' personal information and circulation records.
6. When people give personal information to a company for a specific purpose during offline activity, their information should only be used for that purpose.
7. I do not mind if government agencies know what I have been reading offline.
8. Companies should not share personal information obtained in an offline context with third parties unless they first obtain specific permission of the individual.
9. Libraries should never share personal information or circulation records generated offline with third parties unless it has been authorised by the individual or by a court of law.
10. Companies and government agencies that collect personal information in offline contexts should take more steps to prevent unauthorised access to individuals' personal information.
11. Libraries should play a role in educating the general public about issues of personal privacy that are relevant in people's offline lives.
12. Parliament should adopt more laws that protect personal information from unauthorised disclosure in offline contexts.
13. I self-censor my offline inquiry and reading habits out of concern that my records could be misunderstood.

Adapted from the American Library Association's survey in Zimmer (2014).

Section 4 was identified as relating to Privacy in Digital Services and is adapted from Section 3. It utilised data collected in Section 2, to present only questions relevant to the respondent’s library services.

Table 2. Privacy in Digital Services (only those applications which the respondent has indicated as being offered were presented in the survey).

<p>This section relates to privacy in digital services offered by the library. Clarification of terms: "Personal information" Examples of "personal information" in this section may relate to any data knowingly or unknowingly transmitted or viewed online which may reflect such things as political or personal views, interests and hobbies, images and biometrics data, purchase and banking records, medical records, physical movements, content of conversations, information in contracts, personal associates, business associates etc., where these could potentially be linked at some time with the individual. Please indicate the degree to which you agree with the statements in this section:</p>								
1. Users of the following services should be able to control who sees their personal information:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
2. I am concerned that use of the following services results in companies collecting too much personal information about me or other individuals:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
3. I am concerned that government agencies are collecting too much information about users of the following	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi

services:								
4. E-government services should not share personal information with third parties unless it has been authorised by the individual or by a court of law.								
5. Librarians are actively working to prevent unauthorised access to personal information generated in interactions between the library and users of the following services:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
6. When people give personal information via the following service providers for a specific purpose in their interactions with the library, their information should only be used for that purpose:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
7. I do not mind if government agencies know what I have been viewing on the following services:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
8. Providers of the following services should not share personal information with third parties unless they first	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi

obtain specific permission of the individual:								
9. Libraries should never share with third parties personal information or circulation records of users who interact with the library on the following services unless it has been authorised by the individual or by a court of law:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
10. Providers of the following services that collect personal information should take more steps to prevent unauthorized access to individuals’ personal information:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
11. Librarians should play a role in educating the general public about issues of personal privacy that are relevant in using the following services:	G oodreads or other social catalogui ng	“ ask a librarian” -type service	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or similar SNS	wifi
12. Parliament should adopt more laws that protect personal	G oodreads or other	“ ask a librarian”	e book lending	el ectronic journals	O PAC	in ternet facilities	F acebook, Twitter or	wifi

information from unauthorized disclosure by providers of the following services:	social cataloguing	-type service					similar SNS	
13. I self-censor my use of the following services out of concern that my records could be misunderstood:	Goodreads or other social cataloguing	“ask a librarian”-type service	book lending	electronic journals	OPAC	internet facilities	Facebook, Twitter or similar SNS	wifi

Adapted from the American Library Association’s survey in Zimmer (2014).

Section 5 was identified as relating to privacy practices in place in the library, and is based on section 3 and 4. As with section 4, questions was tailored according to responses given in Section 2 in order to limit questions to those relevant to the respondent’s library.

Table 3. Confidence in Library Practices (only those applications which the respondent indicated as being offered were presented in the survey).

<p>This section relates to the privacy practices in place in the library.</p> <p>Clarification of terms:</p> <p>"Advice or tools"</p> <p>Unless otherwise specified, examples of “advice or tools” in this section may relate to information on the privacy implications of javascript and social media buttons, internet tracking, de-anonymisation, identity theft and intelligence organisations etc., or use of strong passwords, cookies management, privacy settings, encryption, javascript blocking and the Tor network etc.</p> <p>"Personal information".</p> <p>Examples of "personal information" in this section include any data knowingly or unknowingly transmitted or viewed online which may reflect such things as political or personal views, interests and hobbies, images and biometrics data, purchase and banking records, medical records, physical movements, content of conversations, information in contracts, personal associates, business associates etc., where these could potentially be linked at some time with the individual.</p> <p>Please indicate the degree to which you agree with the statements in this section:</p>								
1. The library provides advice or tools to users of the following services which allow them to retain control of who sees their personal	Goodreads or other social	“ask a librarian”-type service	ebook lending	electronic journals	OPAC	internet facilities	Facebook, Twitter or similar SNS	wifi

information while fully or satisfactorily utilising the service:	cataloguing							
2. The library provides advice or tools to users of the following services which allow them to prevent companies from collecting too much personal information about them while fully or satisfactorily utilising the service:	Goodreads or other social cataloguing	“ask a librarian”-type service	ebook lending	electronic journals	OPAC	internet facilities	Facebook, Twitter or similar SNS	WiFi
3. The library provides advice or tools to users of the following services which allow them to prevent government agencies from collecting too much personal information while fully or satisfactorily utilising the services:	Goodreads or other social cataloguing	“ask a librarian”-type service	ebook lending	electronic journals	OPAC	internet facilities	Facebook, Twitter or similar SNS	WiFi
4. The library provides advice or tools to users of E-government services which allow them to prevent the sharing of their personal information with third parties while fully or satisfactorily utilising the service (examples may relate to information about internet tracking, implications of javascript and social networking buttons, managing cookies, javascript blocking etc.).								
5. The library provides advice or tools to users of the following services which allow them to prevent unauthorised access to personal information generated in interactions between the library and themselves while fully or satisfactorily utilising the service:	Goodreads or other social cataloguing	“ask a librarian”-type service	ebook lending	electronic journals	OPAC	internet facilities	Facebook, Twitter or similar SNS	WiFi

6. When people give personal information via the following service providers for a specific purpose in their interactions with the library, they can be assured that their information will only be used for that purpose:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
7. The library does not provide advice or tools addressing the possibility of government agencies knowing what users of the following services have been viewing:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
8. The library provides advice or tools to users of the following services which allow them to prevent their personal information from being shared with third parties while fully or satisfactorily utilising the service:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
9. Use of the following services in interactions with the library does not result in the sharing of personal information or circulation records with third parties without the authorisation of the individual or a court of law:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi

10. The library actively advocates for providers of the following services that collect personal information to take more steps to prevent unauthorized access to individuals' personal information:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
11. Librarians are actively engaged in educating the general public about issues of personal privacy that are relevant in using the following services.	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
12. The library actively advocates for parliament to adopt more laws that protect personal information from unauthorized disclosure by providers of the following services:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi
13. The library provides advice or tools to users of the following services which allow them to make informed decisions about whether to self-censor to avoid their records being misunderstood:	G oodread s or other social catalogu ing	“ ask a librarian ”-type service	ebook lending	ele ctronic journals	OP AC	inte rnet facilities	F acebook, Twitter or similar SNS	w ifi

Adapted from the American Library Association's survey in Zimmer (2014).

Ethical considerations

The present research involved collecting data from human participants, and it was therefore necessary to gain approval from the School of Information Management Human Ethics Committee (HEC). Data was collected anonymously, but an option to provide personal details was included for those who wish to have a summary sent to them. For these cases, personally identifiable data was at no point associated with research data, and will remain confidential.

This research was conducted in accordance with the principles of the Treaty of Waitangi and with the guidelines of the HEC.

Data analysis

The 300 partial and completed responses were downloaded from the Qualtrics platform and imported into R (R Core Team, 2015), via the command `read.csv()` and with the string “NA” introduced for missing values. Of these, 106 contained no responses beyond the initial demographics sections and were not included in the analysis. A further 59 responses between 55% and 77% complete were also not included in the analysis. This left 135 completed responses for analysis, of which 129 reported at least one digital service offered by their library (the remaining six were not asked any Condition 2 or Condition 3 questions). Empty columns representing survey items not intended to be shown to participants were removed using `subset()`, and questions that used negative language were reverse coded using the `recode()` command from the `likert` package (Bryer and Speerschneider, 2016).

Cronbach’s Alpha tests were used to determine internal consistency of the questions within each condition. As described in Gliem and Gliem (2003), George and Mallery (2003) provide as a guideline that a Cronbach’s Alpha of .7 or greater can be taken to show an “acceptable” level of internal consistency. A total of 17 dataframes were created for this purpose, each containing 13 columns representing responses to 13 questions. These were made up of eight dataframes for condition 2 – one for each digital-service type, eight dataframes for condition 3 – one for each digital-service type, and a single data frame for condition 1.

The Kruskal-Wallis one-way ANOVA test was used to see if there were differences in the

medians across conditions using `kruskal.test()` in the stats package in R (R Core Team, 2015). Kruskal-Wallis one-way ANOVA tests can be used to test for differences where there are more than two conditions and where data are not normally distributed (McCrum-Gardner, 2008). As further confirmation that conditions 1 and 2 measured concern, the same test was carried out on the subsets “concern” and “importance”. Five questions in Condition 1 asked respondents to rank a statement which explicitly expresses concern, while the statements in seven questions express the importance of aspects of privacy. In the latter group, if importance is high (conditions 1 and 2) and confidence is also high (Condition 3), this does not indicate concern. But if importance is high and confidence is low, this can logically be interpreted as concern.

Wilcoxon Signed Rank Tests were selected as they are suitable for testing for differences between paired samples of ordinal data, or of interval data where the assumption of normal distribution is not satisfied (McCrum-Gardner, 2008). Medians were compared across conditions using the Wilcoxon Signed Rank Test in the stats package in R (R Core Team, 2015), `wilcox.test(paired=T, alternative = “less”)`, in order to see if there were differences in the paired conditions of Condition 1 and Condition 2, and between Condition 2 and Condition 3. This test was performed on the same 17 dataframes as were created for the Cronbach’s Alpha tests (i.e. they were performed on each digital-service type separately within Conditions 2 and 3).

Limitations

Considerations of reliability and validity must be central to any research project to ensure the utility of its results and value of its conclusions. Face validity refers to the perception of credibility of the survey among participants, and can be achieved through quality of presentation of the survey and surrounding documents as well as appropriate construction and wording of questions. In an effort to ensure face validity, care was taken to present invitations to participate professionally. The result of 300 partial or complete responses indicates a degree of success in this. Questions were based on an existing survey by a respected organisation in the first instance, and adaptations were made based on a study of literature and an environmental scan around privacy threats in libraries. Appropriateness of the questions was further tested through informal interviews with librarians. However, the need to specify distinctions between conditions, and to keep working consistent within conditions, resulted in somewhat lengthy wording. Four of the 30 respondents who wrote comments indicated that questions

were made confusing by their length or by their similarity to each other, and one respondent indicated that they thought the questions biased (they did not specify in what way). While care was taken to avoid these issues, these responses show a somewhat problematic level of face validity which is one possible contributing factor to the relatively low completion rate of 135.

Self-report data such as those collected by questionnaire research are subject to distortions (Leedy & Ormrod, 2013, p. 190). Of particular concern are construct validity and content validity, which are achieved if the quality to be studied is broken down into several measurable aspects (Andres, 2012). A section of the American Library Association survey that bears similarity to the established CFIP survey instrument was selected. The questions selected and adapted made use of established constructs underlying concern for privacy such as control, collection, intended purpose and unauthorised access of information in order to maximise the construct and content validity of the instrument.

Another aspect of reliability is known as instrumentation, and refers to the effect that the structure of questions themselves have on results (Andres, 2012). In adapting questions for Conditions 2 and 3, care was taken to keep the wording as similar as possible across conditions, to ensure that any differences measured were due to differences in the data and not in the instrument. However, in order to make the meaning of questions clear, some difference in wording was necessary. It is possible that these differences may have led to different interpretations in the different contexts.

The validity of research can be impacted when participants tend to agree with statements for the sake of being agreeable, which is known as acquiescence bias. Negative phrasing of some survey items was employed to help counteract acquiescence bias. There is a tradeoff, however, with ease of comprehension and completion of the survey. Therefore relatively few questions with negative phrasing were used. In instances where negative phrasing was used, responses seemed to be in line with other responses, giving some indication that no strong acquiescence bias was present.

Of the 300 responses recorded, 135 were completed to the end. This is a fairly low ratio of completion which may have negative implications for the representativeness of the sample. One further possible explanation for this low ratio may be a high incidence of people having access to multiple

internet-connected devices. If a participant first looked at the survey on a work computer and then decided to complete the survey on a smartphone on the way home for example, this could have resulted in a partial response being recorded as well as a complete one.

The sampling method employed was a form of self-selection sampling. This will inevitably affect the representativeness of the sample. Furthermore, the sample size (135) fell short of the number thought desirable (approximately 400, as mentioned above) for representativeness of a large population, limiting the level of confidence with which inferences can be made to the whole population.

The design stage of this study did not have the benefit of consultation with experts in digital security, privacy, data analysis, digital surveillance etc. An ideal survey instrument would reflect very accurately the most pressing privacy threats and the best strategies for mitigating these. A review of the literature was undertaken to identify these as well as could be managed. However, it is possible that the wording used and the examples given in questions may have had an impact on results, and indeed one participant left a comment describing the questions as “biased” (without describing in what way).

Reading level and unequal access to the internet have been cited as impediments to accurate data collection through questionnaires, but with the target population being those working in libraries neither of these limitations are likely to have been serious (Leedy & Ormrod, 2013).

Results

The Cronbach’s Alpha test on Condition 1 gave a Standard Alpha of 0.78. The same test repeated for each digital-service type within Condition 2 gave Standard Alphas ranging from 0.74 to 0.87. For each digital-service type within Condition 3, Standard Alphas ranged from 0.93 to 0.96. These results indicated that the conditions had a level of internal consistency in the acceptable range or higher, and were therefore suitable for further testing.

A Kruskal-Wallis one-way ANOVA test across the three conditions gave a chi-squared of 2932.2, with a p-value of less than 0.001. This result shows to a high degree of certainty that there were shifts in the distributions of the conditions. The same test conducted on the subset of questions focusing on

“importance” across the 3 conditions gave a chi-squared of 2456, with a p-value of less than 0.001.

Results of the Wilcoxon Signed Rank Test on Conditions 1 and 2, run separately for each digital-service type within Condition 2 (that is, with the median of Condition 1 responses being compared with the median of Condition 2 responses relating to ebooks and then to the median of Condition 2 responses relating to wifi, and so on), gave a V ranging from 9349 to 103250 with p-values ranging from 0.019 to less than 0.001. This showed that concern for privacy in general was higher than concern for privacy in the context of all of the specified digital services. For the same tests run on each digital-service type within Condition 2 and its counter-part in Condition 3, results ranged from V = 6019.5 to V = 93992, with p-values all less than 0.001, showing that the level of concern for privacy in the context of each of the digital services was greater than the level of confidence in privacy protecting practices for those same services.

Table 4. Wilcoxon Rank Sum Test results

	V	p-value
Cond. 1, Cond. 2 (GoodReads)	9349	<0.001
Cond. 1, Cond. 2 (wifi)	103180	<0.001
Cond. 1, Cond. 2 (Facebook)	36458	0.019
Cond. 1, Cond. 2 (computers)	103250	<0.001
Cond. 1, Cond. 2 (OPAC)	69132	<0.001
Cond. 1, Cond. 2 (e-journals)	38145	<0.001
Cond. 1, Cond. 2 (e-books)	39542	<0.001
Cond. 1, Cond. 2 (Ask-a-librarian)	49554	<0.001
Cond. 2(GoodReads), Cond. 3 (GoodReads)	6019.5	<0.001
Cond. 2(wifi), Cond. 3 (wifi)	83116	<0.001
Cond. 2(Facebook), Cond. 3 (Facebook)	14370	<0.001
Cond. 2(computers), Cond. 3 (computers)	87650	<0.001
Cond. 2(OPAC), Cond. 3 (OPAC)	93992	<0.001
Cond. 2(e-journals), Cond. 3 (e-journals)	52547	<0.001
Cond. 2(e-books), Cond. 3 (e-books)	51454	<0.001
Cond. 2(Ask-a-librarian), Cond. 3 (Ask-a-librarian)	69854	<0.001

The type of library reported by respondents is listed in Table 5, with public libraries being the most numerous.

Table 5. Library type

	number of responses
Public	43
School	30
Academic	27
Special	24
Other	11

Table 6 shows reported job descriptions, with the greatest number being “Librarian”.

Table 6. Job description

	number of responses
librarian	84
library paraprofessional or library worker	7
Graduate of a librarianship or related programme	8
library volunteer	2
library administrator (management)	26
library administrator (staff level)	1
other library related role	7

Of the digital services offered by the libraries of the 135 respondents who gave complete responses, the most common were wifi, In-library computers and an online public access catalogue (OPAC), as shown in Table 7.

Table 7. Digital services offered

	Number of responses
GoodReads or other social cataloguing	34
Wifi	120
Facebook, Twitter or similar SNS	64
In-library computer with internet access	119
OPAC	117
Electronic journals	83
E-book lending	91
“Ask a librarian”-type service	90
None of these	6

Discussion

The present research investigated the level of concern that New Zealand library professionals have in online and offline contexts, as well as their level of confidence that their libraries' privacy-protecting practices in online contexts are appropriate. In particular two non-conflicting hypotheses were proposed: H1, that concern in Condition 1 was greater than that in Condition 2, and H2, that concern in Condition 2 was greater than confidence in practices in Condition 3.

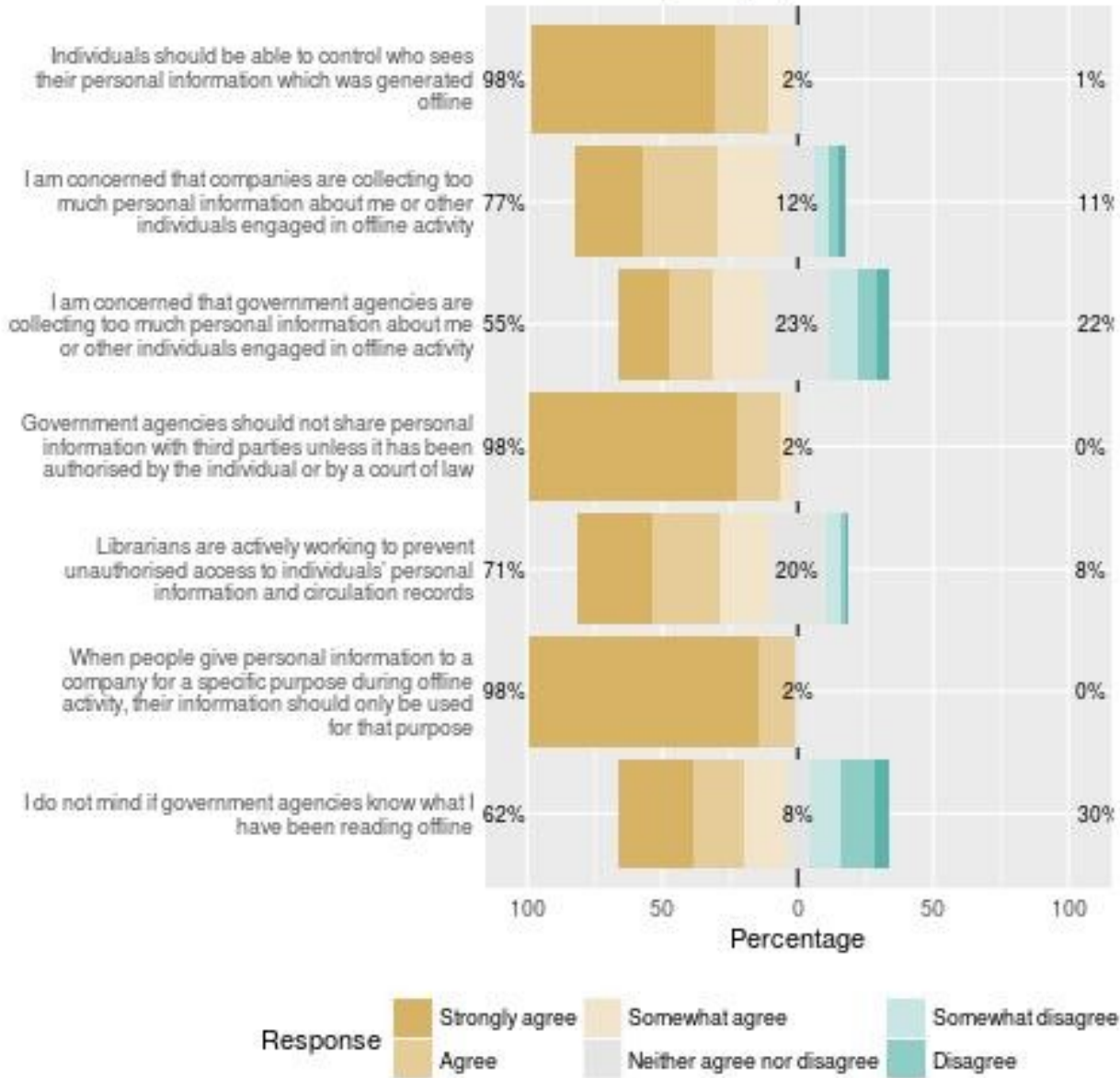
Analysis of the data provides a basis for rejecting the null hypotheses H0a and H0b of no difference between Conditions 1 and 2, and between Conditions 2 and 3. Support is found for both hypotheses H1 and H2, that concern for privacy in digital contexts is less than concern in offline contexts, and that in digital contexts confidence in mitigating practices is less than concern.

In order to answer the research questions of the preset research, three subquestions were posed: what are the levels of a) offline privacy concern b), privacy concern in digital services, and c) confidence in practices. From the seven-point likert scale data gathered, where 1 was "strongly agree" and 7 was "strongly disagree", the mean values of these three conditions were 2.24, 2.69 and 4.19 respectively (means across all service types were taken for Conditions 2 and 3). This shows that concern is high in both the offline and the digital services contexts, and that confidence is relatively low.

The two research questions posed were: a) to what extent does offline privacy concern differ from online privacy concern, and b) to what extent does online privacy concern differ from confidence in online privacy protection practices. The results show that offline and online privacy concern differ only slightly, and that online concern differs considerably from confidence in online privacy protecting practices.

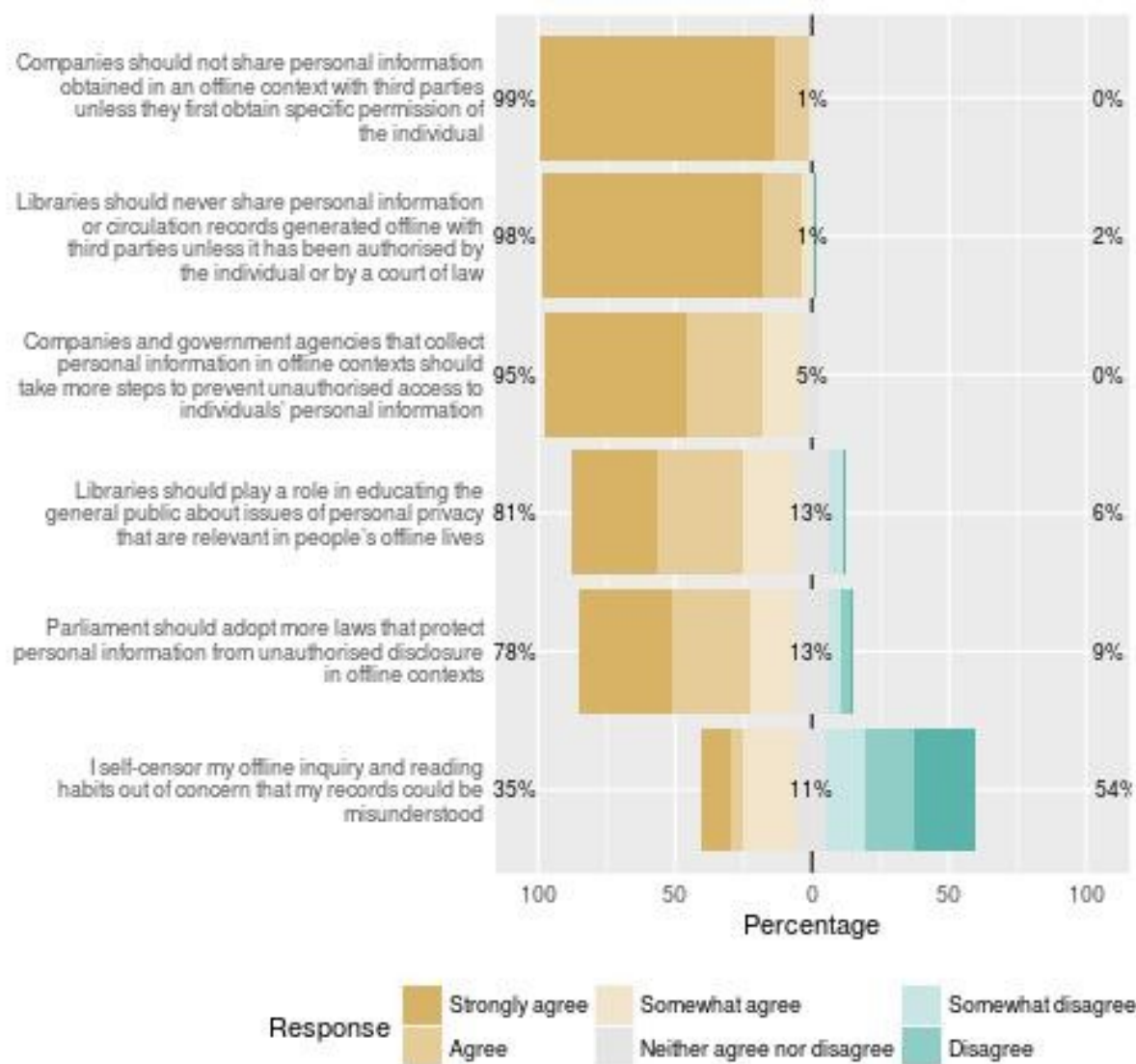
In the offline context, in questions 1, 4, 6, 8 and 9 respondents showed a very high level of support for the right to control over one's personal information, and for the idea that personal information should not be shared or used for secondary purposes without authorisation, with well over ninety percent indicating agreement (that is, either "strongly agree", "agree", or "somewhat agree")..

Condition 1 (1 of 2), questions 1 - 7



Results for questions 10 and 12 indicate concern, with 95% agreeing that more work should be done to ensure such practices, and 78% agreeing that additional legislation should be adopted. (Note that question 7 in the figure about has been reverse coded).

Condition 1 (2 of 2),
questions 8 - 13



Regarding privacy with importance did not necessarily mean respondents felt their openness impinged, however, as much as 35% agreed that they self-censor in reading and inquiry, with 54% disagreeing. This represents a considerably higher degree of self-censorship than that found in the two US surveys of librarians reported in Zimmer (2014), however. Those showed between 15% and 21% agreeing, and between 66% and 76% disagreeing to a similar “I self-censor” statement.

The data indicate that concern for privacy is high in both offline and digital contexts, which shows that in general New Zealand library attitudes towards privacy are in line with those espoused by

the American Library Association and the International Federation of Library Associations and Institutions. This lends support to the traditional idea that libraries can and should be involved in protecting privacy.

Although the difference was relatively small, the concern for privacy in digital services was found to be significantly less than in the offline context. It is beyond the scope of the present study to determine the reasons driving this difference. However, two possible reasons that may explain a lower level of concern in the online context are that, firstly, a need may be seen to trade-off privacy against other benefits or, secondly, there may be a sense of an inevitability of reduced privacy online which invites acceptance.

It will be important for the profession to note this difference, and to come to an agreement about its significance. If the causes for the difference are deemed to be justified, a somewhat reduced notion of privacy rights should be accepted and defined for the digital context. If the causes are deemed to be rooted in a lack of knowledge or resources to enable protection of privacy in digital contexts, efforts should be made to reduce this deficit. Some support for this latter explanation of the cause of the difference found between Conditions 1 and 2 may be present in the data showing such a large deficit in Condition 3 as compared to Condition 2. Zimmer (2013a) found that professional journal articles put far less emphasis on privacy solutions than the level of concern seemed to require. Likewise, the present study shows less confidence in practices for protecting privacy than would seem desirable given the level of concern. The cause of discrepancy in both cases may well be the same: it may be that the necessary expertise is not present in the profession.

Other causes for the difference in Conditions 2 and 3 may include a lack of control over privacy due to the parent organisation being responsible for IT infrastructure, a lack of control over the data collection practices of third-party providers, a desire to resist privacy protections in order to safeguard law enforcement, a lack of resources for privacy protection and privacy education, and it may be that individual library policies do not permit privacy protecting practices to be carried out to an extent in agreement with the level of concern of staff.

While it is not within the scope of the present research to determine the appropriate responses to

the many privacy challenges faced by libraries, the results do indicate that librarians believe that efforts should be made to improve practices. It is fortunate that there are a number of organisations which offer advice to libraries on this topic, and a summary of some these may be of use here. The advice varies in ease of implementation and in applicability to individual libraries, and some may be more or less controversial. The situation is complicated by the fact that in some instances it is the parent organisation or its IT department, rather than the library itself, which has direct control of many of the systems that impact privacy. Therefore, it is important that individual libraries, library associations and library education providers find ways to open channels of communication on the topic of privacy both internally and amongst themselves, as well as with parent organisations and more broadly.

For this to be effective, individuals will need to be familiar the challenges and potential solutions. Many useful resources for this purpose are offered by organisations such as the American Library Association, the Library Freedom Project and the Electronic Freedom Frontier. Rich as these resources are, however, they do have a focus on the US, with its different regulatory environment. Libraries in New Zealand would benefit if a resources such as the American Library Association's "Privacy Toolkit" (2007) were adapted for local applicability.

The Privacy Toolkit recommends that libraries' approach to privacy include maintaining a privacy policy and designating a privacy officer, conducting of privacy audits, advocacy and education, all of which are relevant to the concerns indicated by the present research (American Library Association, 2007).

A privacy audit should include the library's data collection and retention practices, as well as those of third-party service and content providers. The information should be shared with patrons and staff, and should be considered in future decisions on the provision of services (Farkas, 2015). Similarly, careful consideration of privacy implications should given to any new content or services providers. Disclosure of data collection and storage practices should be required of any potential provider and, if the service is adopted, these practices should be communicated to patrons and staff. Two of the participants in the present research wrote comments indicating a lack of knowledge about what privacy protections were in place, suggesting that greater privacy auditing and communication of the results is required in some cases. A list of areas to check for personally identifiable information in a

privacy audit is given in the Privacy Toolkit (American Library Association, 2007), with many of the items being relevant to the concerns found in the present research.

It can be assumed that any unencrypted information transmitted over the internet or on a local network will be “intercepted and used”, according to Breeding (2016). Libraries can address this issue by ensuring that third-party providers’ and their own websites and OPAC are encrypted with HTTPS, by installing the HTTPS Everywhere browser plug-in from the Electronic Freedom Foundation on their public-facing computers and by encouraging patrons to do the same on their devices and to be aware of this issue.

It can be difficult for individual libraries to exert much influence over the data collection and encryption practices of third-party providers, as was pointed out in comments left by two participants of the present research. It may be possible to increase this bargaining power if libraries are able to act together in negotiations, perhaps coordinated by library organisations. In the case free applications such as social media applications this appears even more difficult. As one participant commented, a cross-sector approach involving the library sector, the technology, NGOs and government working together may be necessary for this. A finding of this research, that 67% of respondents believe that more laws should be adopted to protect privacy in the context of digital services (taken as an average across service types), suggests that there may be considerable support for this idea.

While snooping of unencrypted data can be expected anywhere on the internet, the risk is even more pronounced over wifi hotspots (Breeding, 2016). An even more serious risk is that fake wifi hotspots can be run by malicious actors within the vicinity of legitimate hotspots and with similar names, seeking to fool victims into connecting in order to steal sensitive information or deploy malware. Posters or information sheets could be provided to inform patrons of the correct name of a library’s legitimate wifi service and to caution users about accessing sensitive information over wifi to address this. Breeding (2016) provides discussion of the options available to libraries that choose the greater convenience of an open wifi network, or the greater security of an encrypted network.

While important, and likely sufficient for many purposes, the kinds of practices mentioned above can help to provide confidentiality in a way that has been likened to using an envelope to post a letter

rather than sending a postcard which can be read by anyone—their aim is not to provide anonymity, but simply to prevent data from being needlessly broadcast to unrelated parties. Macrina (2015), citing evidence of a chilling effect upon writers as a result of NSA surveillance, argues that the protection of intellectual freedom and privacy for all members of society requires that the ability to use the internet anonymously must be afforded, and that libraries can contribute to this by providing and promoting the tools for anonymous web browsing Tor and the Tor Browser. Libraries serve vulnerable groups such as immigrants that may come from oppressive regimes and domestic abuse victims who may be in special need of anonymity online. Given that 38% of respondents in the present research indicated some level of agreement that they self-censor on digital services (averaged across digital services), it is likely that the most vulnerable groups in society experience an even stronger chilling effect. This suggests that intellectual freedom may indeed be improved by the provision of the Tor Browser in public-facing computers.

With developing technologies, threats to privacy also develop along with the opportunities. More important than any individual solution to current threats is that librarians, libraries, library training institutions and library organisations engage with the issues to best equip themselves to manage current and future challenges (Gressel, 2014). This should involve education of staff and the public, care in procurement decisions or in negotiating these decisions with parent organisations, development of tools and information packs for staff and for the public and advocacy and outreach to build greater awareness and better outcomes for privacy.

Conclusions

Privacy is an important aspect of the health of a society, necessary for the preservation of democracy and intellectual freedom, the protection and promotion of which has long been associated with libraries. The present research found evidence that the challenge of protecting privacy in the context of rapidly evolving technologies has meant that concern about privacy has come to outweigh confidence in privacy protecting practices of libraries.

Significant differences across the conditions measured were found, with offline privacy concern being the highest and online privacy concern also being high, and confidence in privacy-protecting practices being relatively low.

Whatever the reasons for the differences, it is clear that New Zealand librarians and library workers believe that privacy should be protected and that more ought to be done. Furthermore, there is evidence that the various digital services offered by libraries themselves, often through third parties or parent organisations, do not currently provide a level of protection that matches those beliefs. The level of advocacy and education for privacy undertaken by libraries is also seen by respondents as being less than it should.

Resources for privacy protecting practices were pointed to, and some solutions discussed. The creation of localised privacy resources, greater privacy related education and awareness-raising for library staff and for patrons, and the development of avenues for cooperation in negotiations and advocacy for privacy were recommended.

Further research

There is much research to be done in the field of digital privacy and libraries. Qualitative studies could look at the causes of the lower level of confidence in privacy protection practices found in the present research, by interviewing librarians about their attitudes and competencies with regard to privacy and digital technologies. Privacy policies in place in libraries could be examined to find out the proportion of libraries that display these online or within the library. Content of the policies could be analysed for comprehensibility and practices covered. Data collection and retention practices of libraries could be examined for compliance with regulations and policies. A study of library websites and websites associated with e-governance could be made to discover and analyse any privacy harming technologies such as tracking cookies, web beacons and social media buttons that may be present. A survey of libraries and government agencies could be conducted to discover the existence or frequency of requests for patrons' or customers' information by government agencies, and the information sharing regulations cited in these requests.

Acknowledgements

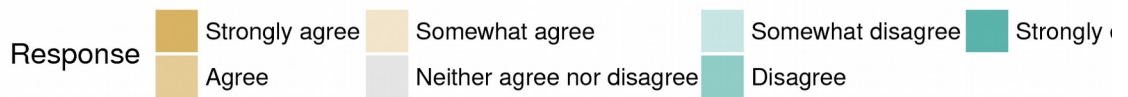
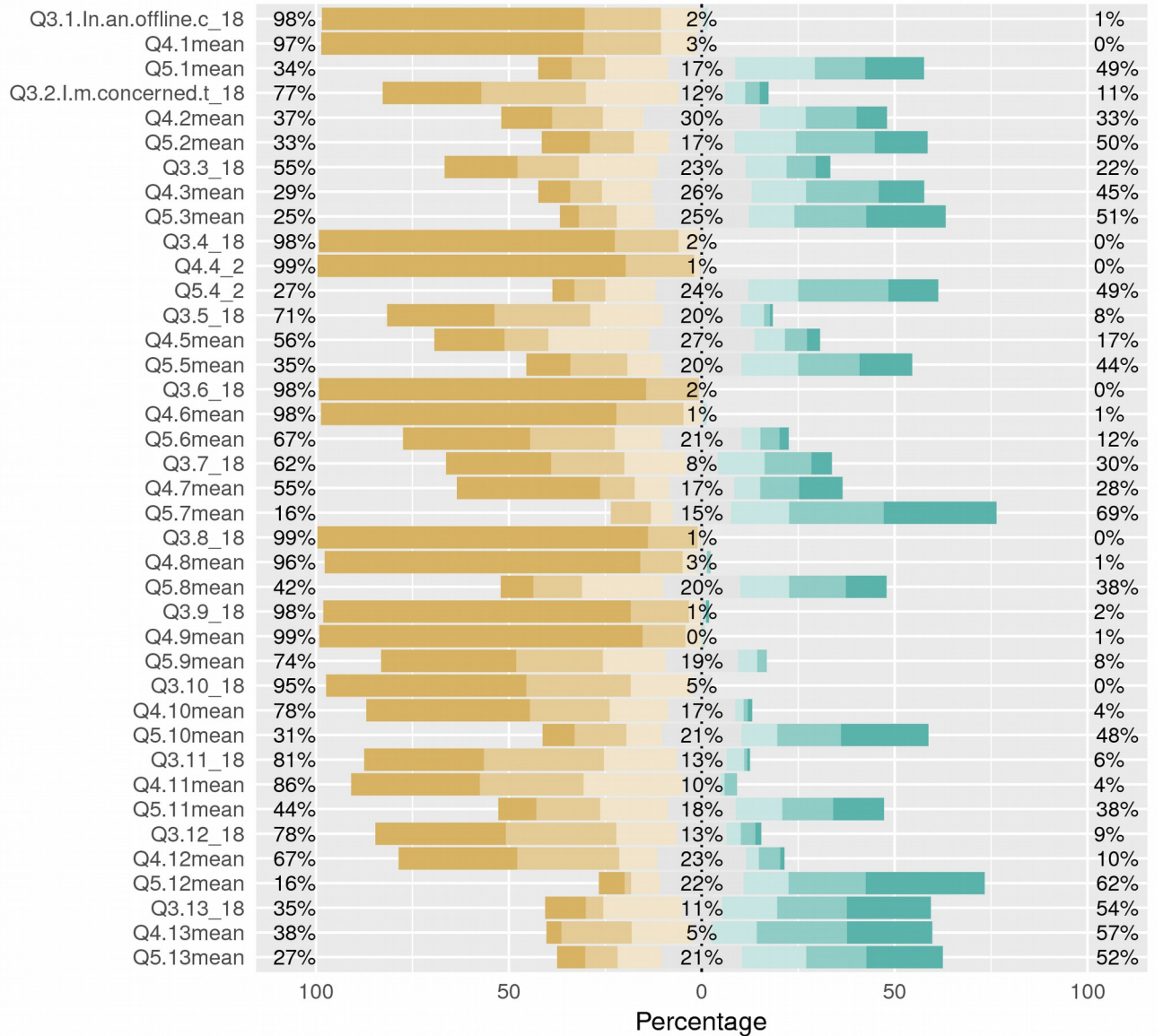
I would like to thank my sister, Dr Jessie S. Nixon, for a great deal of support, both moral and technical, for which I am very grateful.

Thanks also to Dr Philip Calvert, my supervisor for this project, for much encouragement and advice, as well as a good deal of patience.

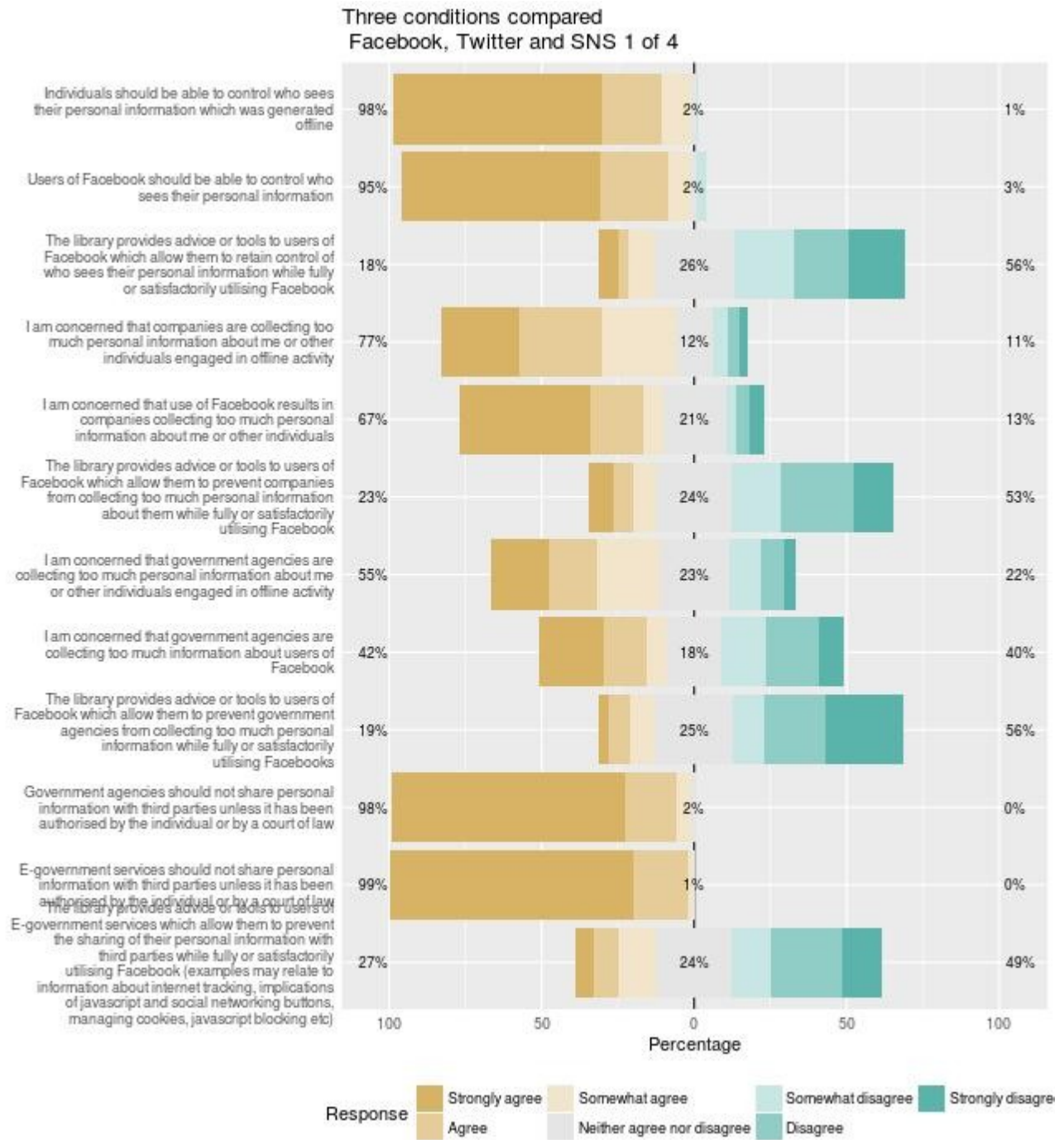
Appendices

Appendix 1. Question by question comparison of Conditions 1 -3 (means of digital-service types)

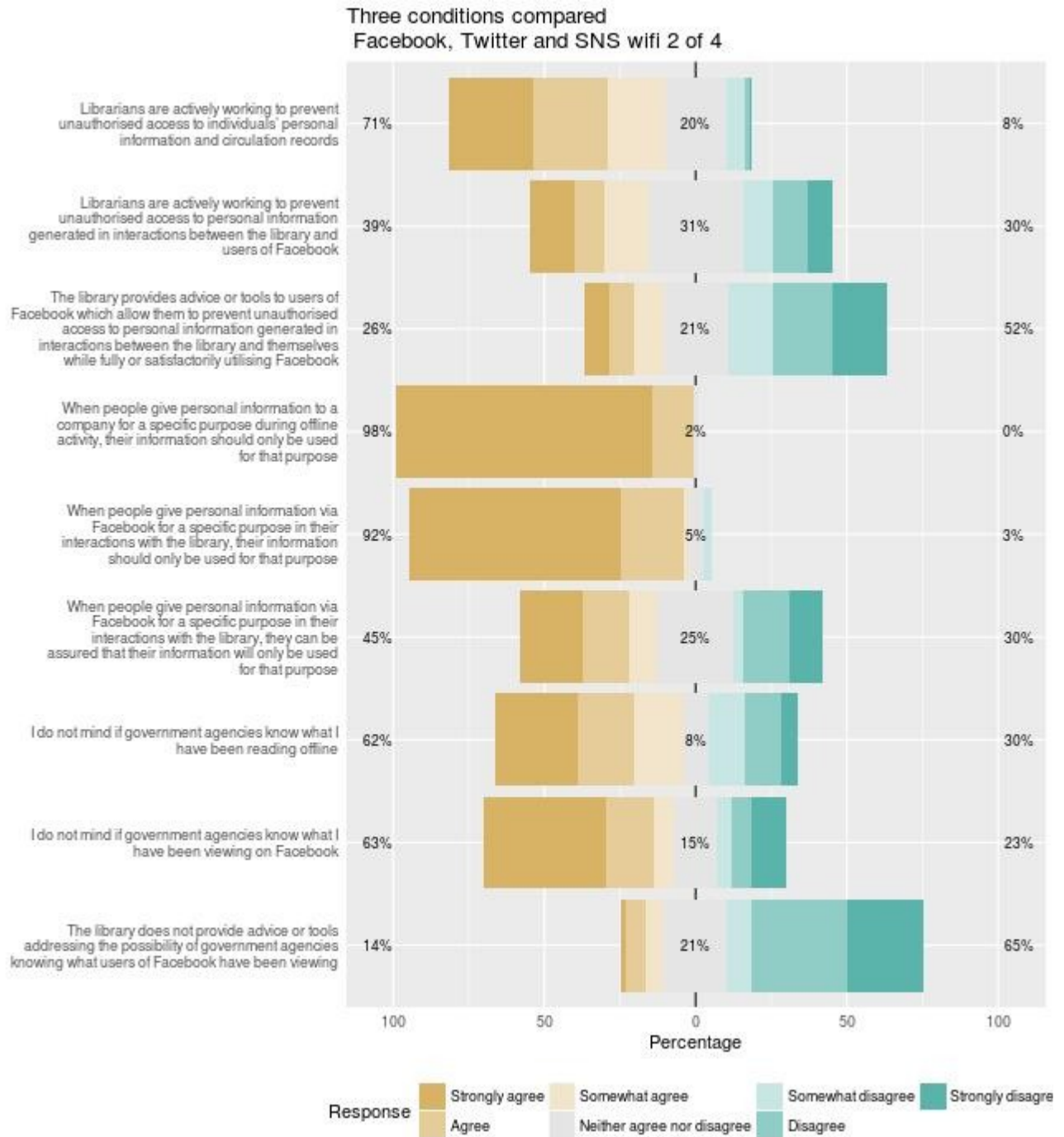
(Note that questions 7 have been reverse coded).



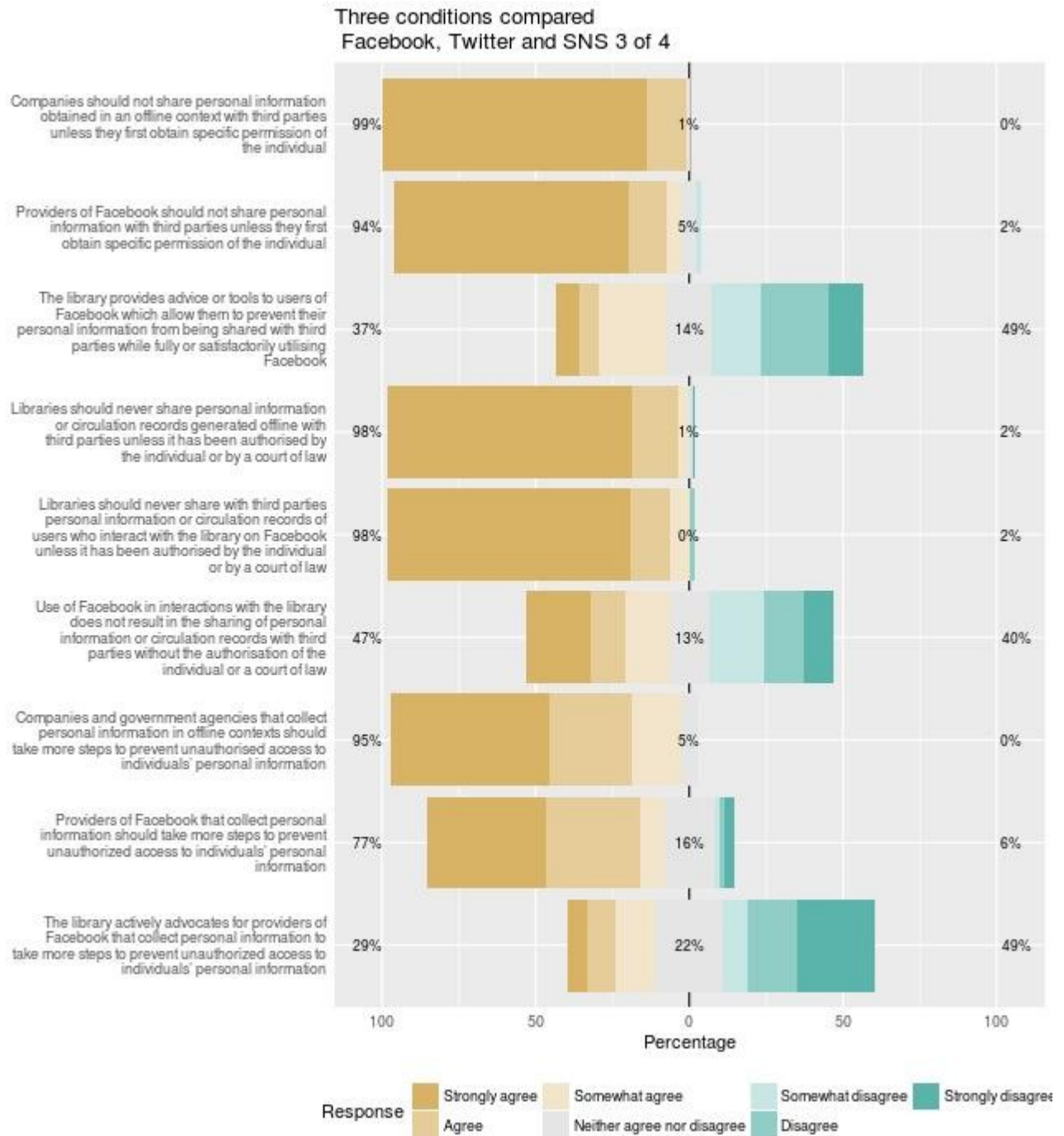
Appendix 2. Question by question comparison of Conditions 1 -3 (Facebook, Twitter and SNS 1 of 4)



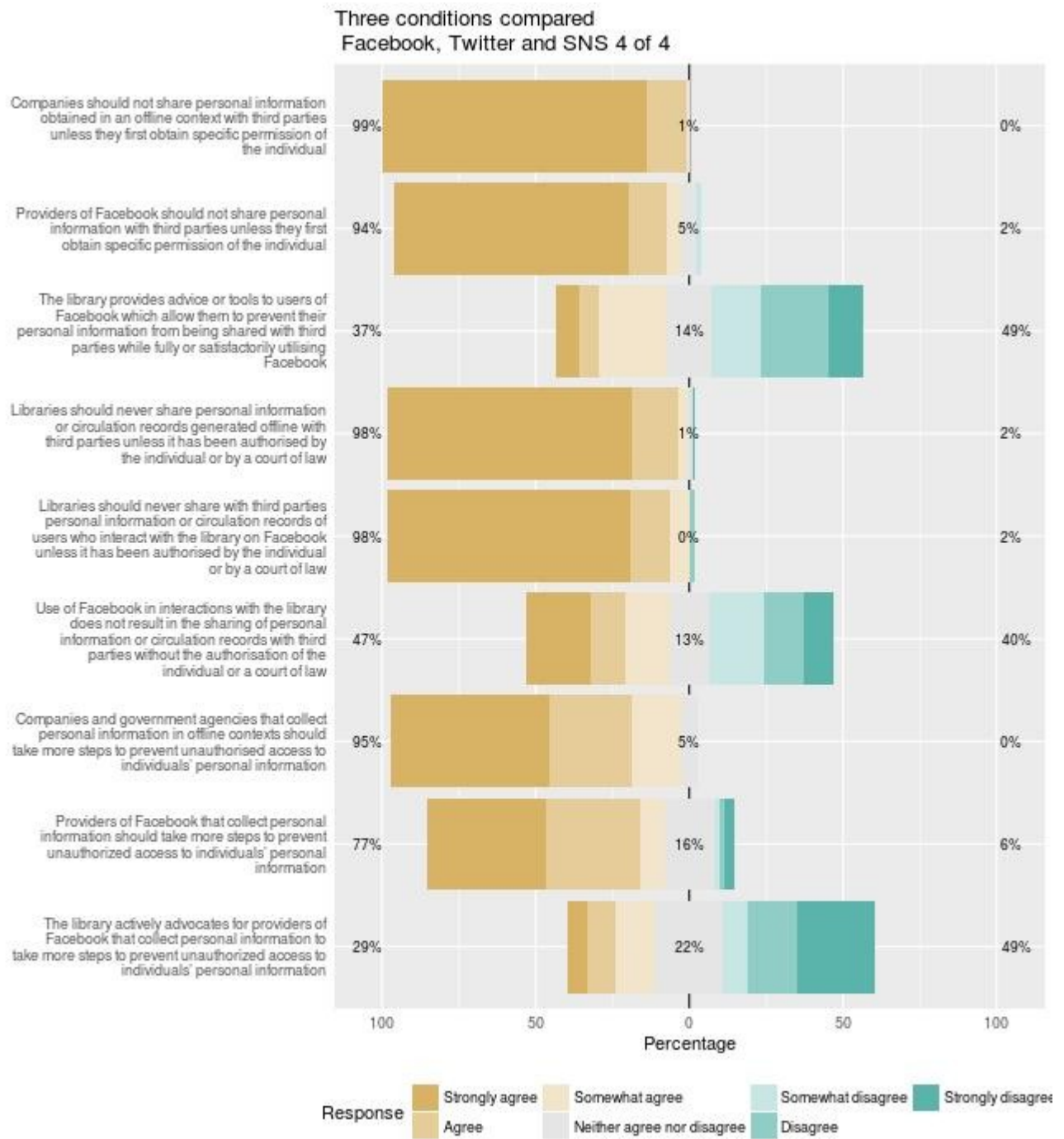
Appendix 3. Question by question comparison of Conditions 1 -3 (Facebook, Twitter and SNS 2 of 4)
 (Note that questions 7 have been reverse coded).



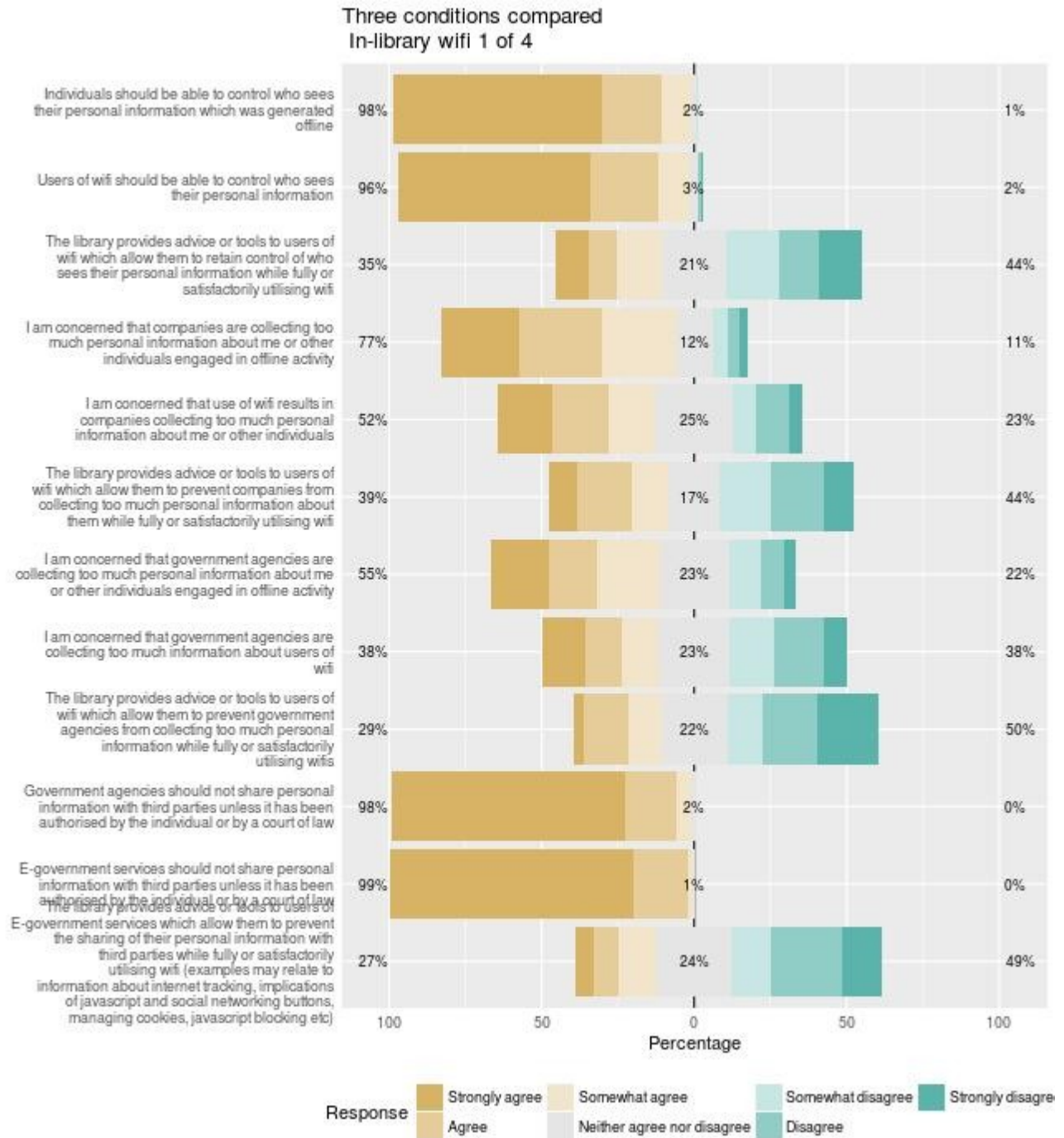
Appendix 4. Question by question comparison of Conditions 1 -3 (Facebook, Twitter and SNS 3 of 4)



Appendix 5. Question by question comparison of Conditions 1 -3 (Facebook, Twitter and SNS 4 of 4)

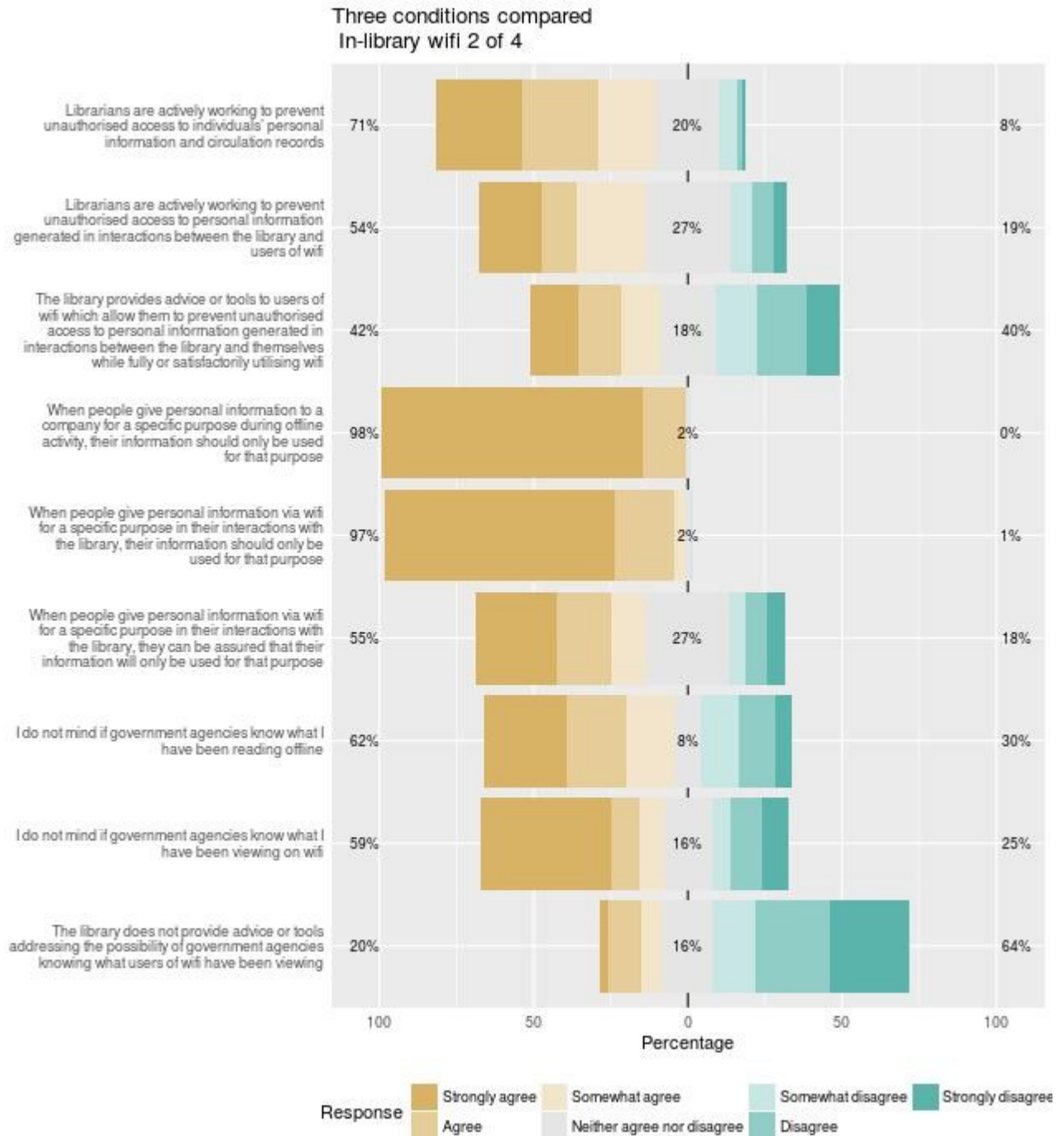


Appendix 6. Question by question comparison of Conditions 1 -3 (wifi 1 of 4)

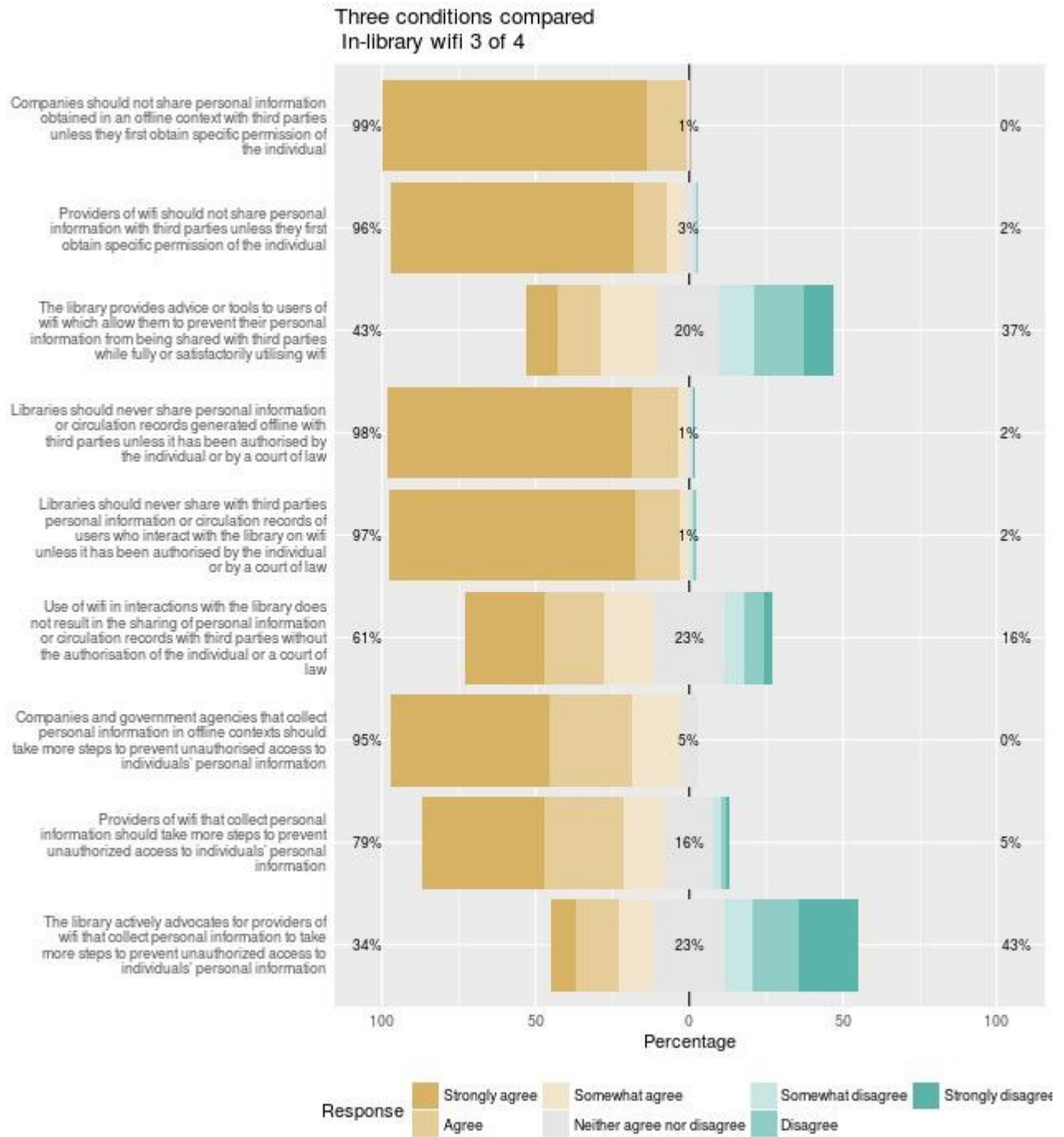


Appendix 7. Question by question comparison of Conditions 1 -3 (wifi 2 of 4)

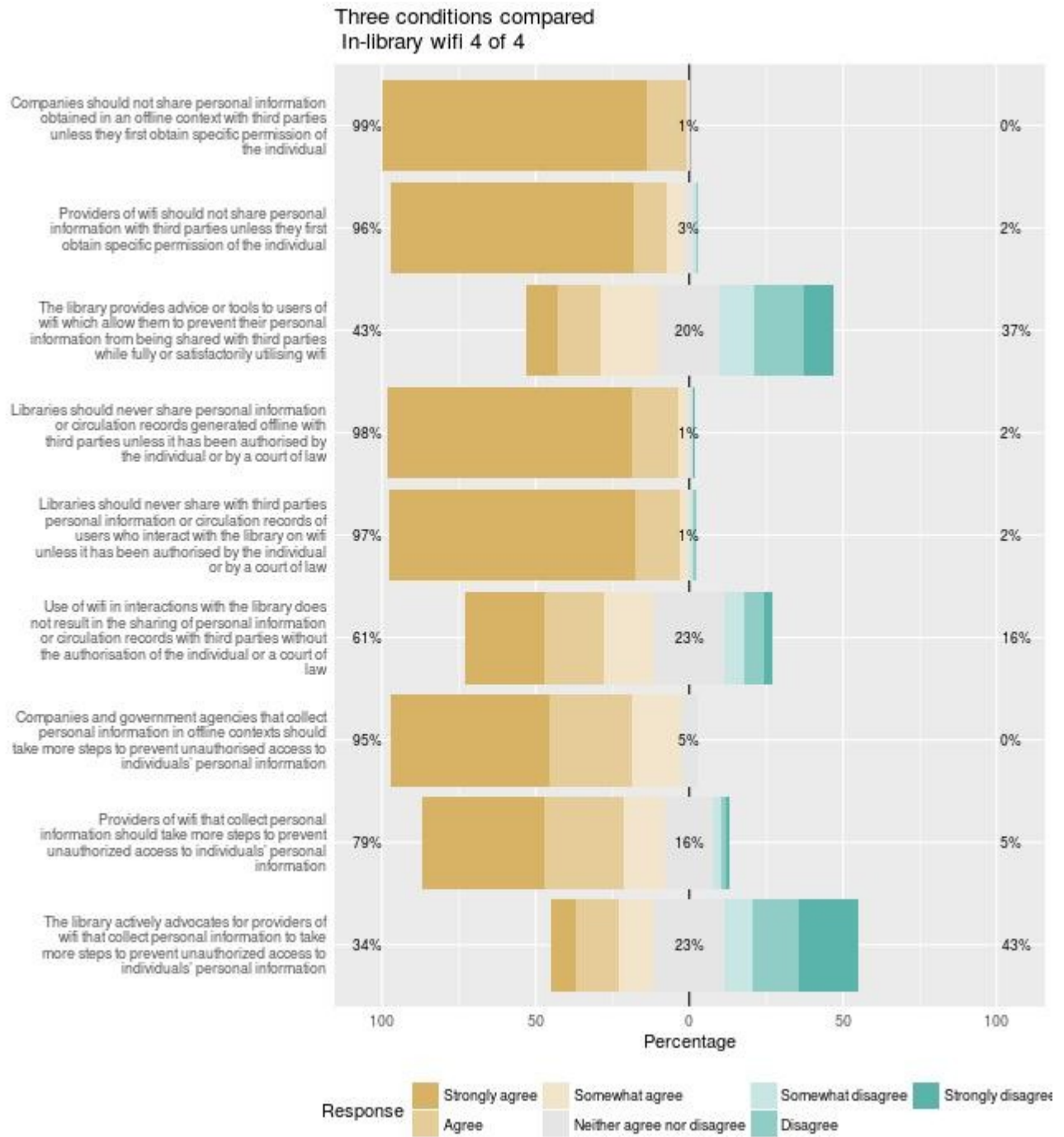
(Note that questions 7 have been reverse coded).



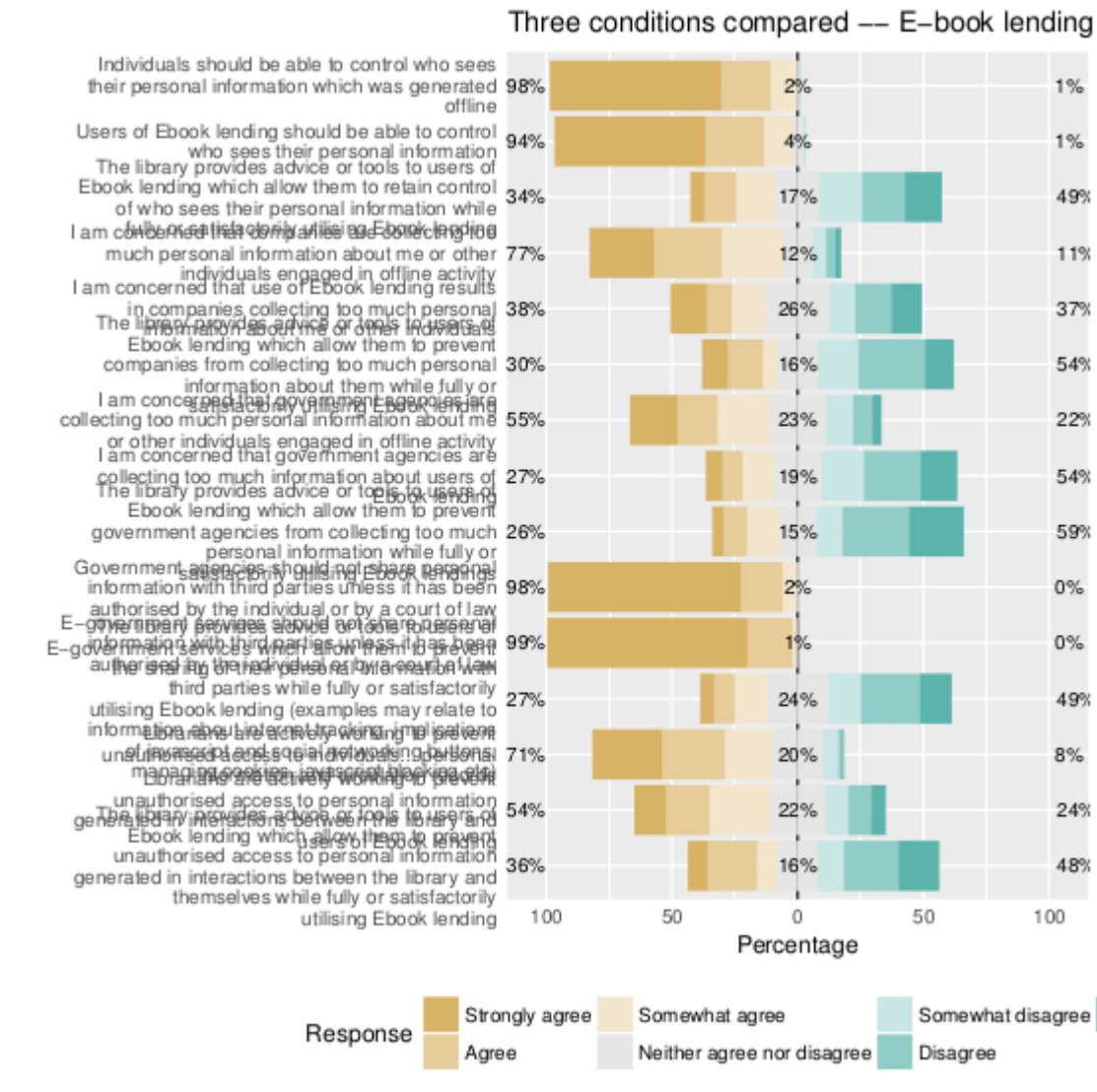
Appendix 8. Question by question comparison of Conditions 1 -3 (wifi 3 of 4)



Appendix 9. Question by question comparison of Conditions 1 -3 (wifi 4 of 4)

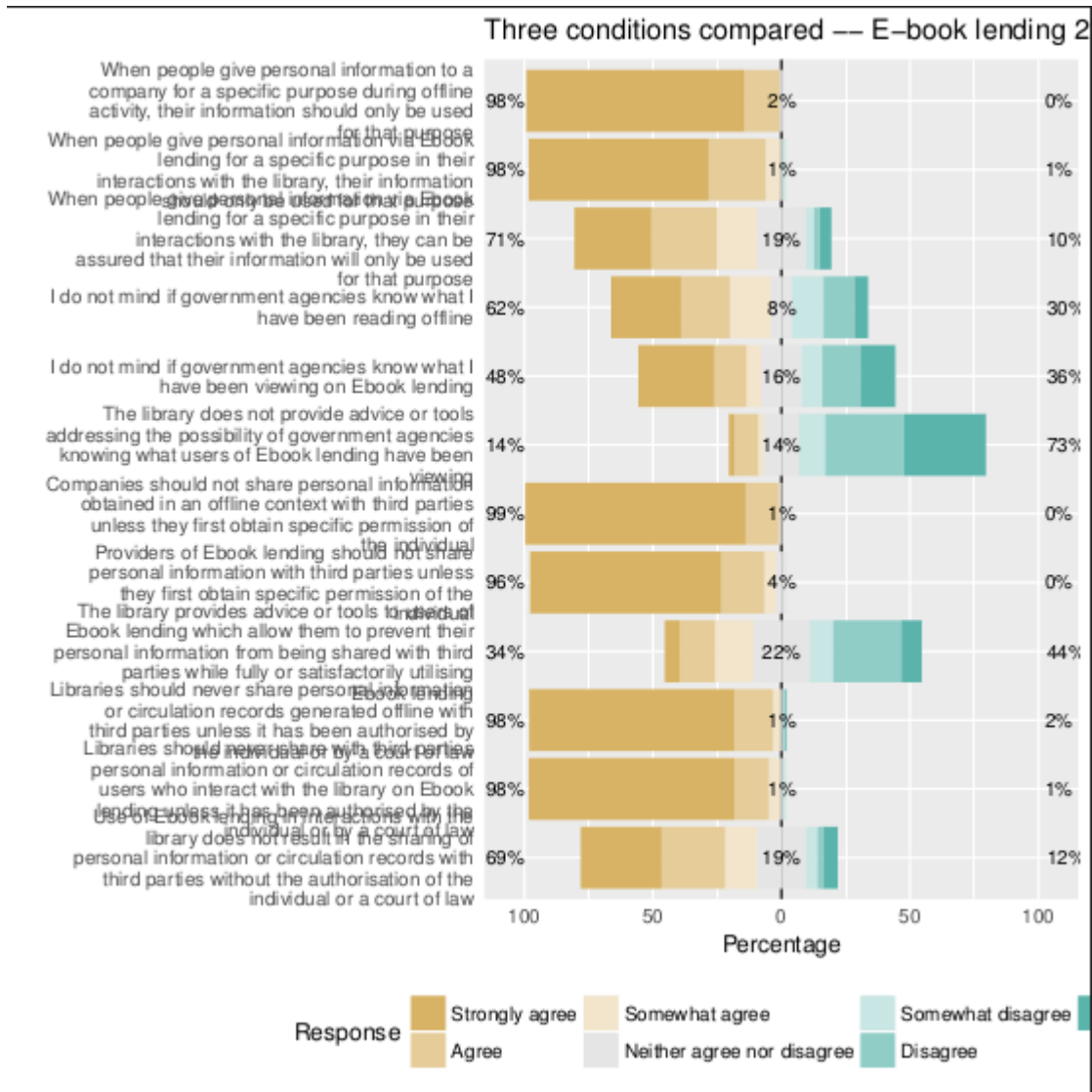


Appendix 10. Question by question comparison of Conditions 1 -3 (E-books 1 of 3)

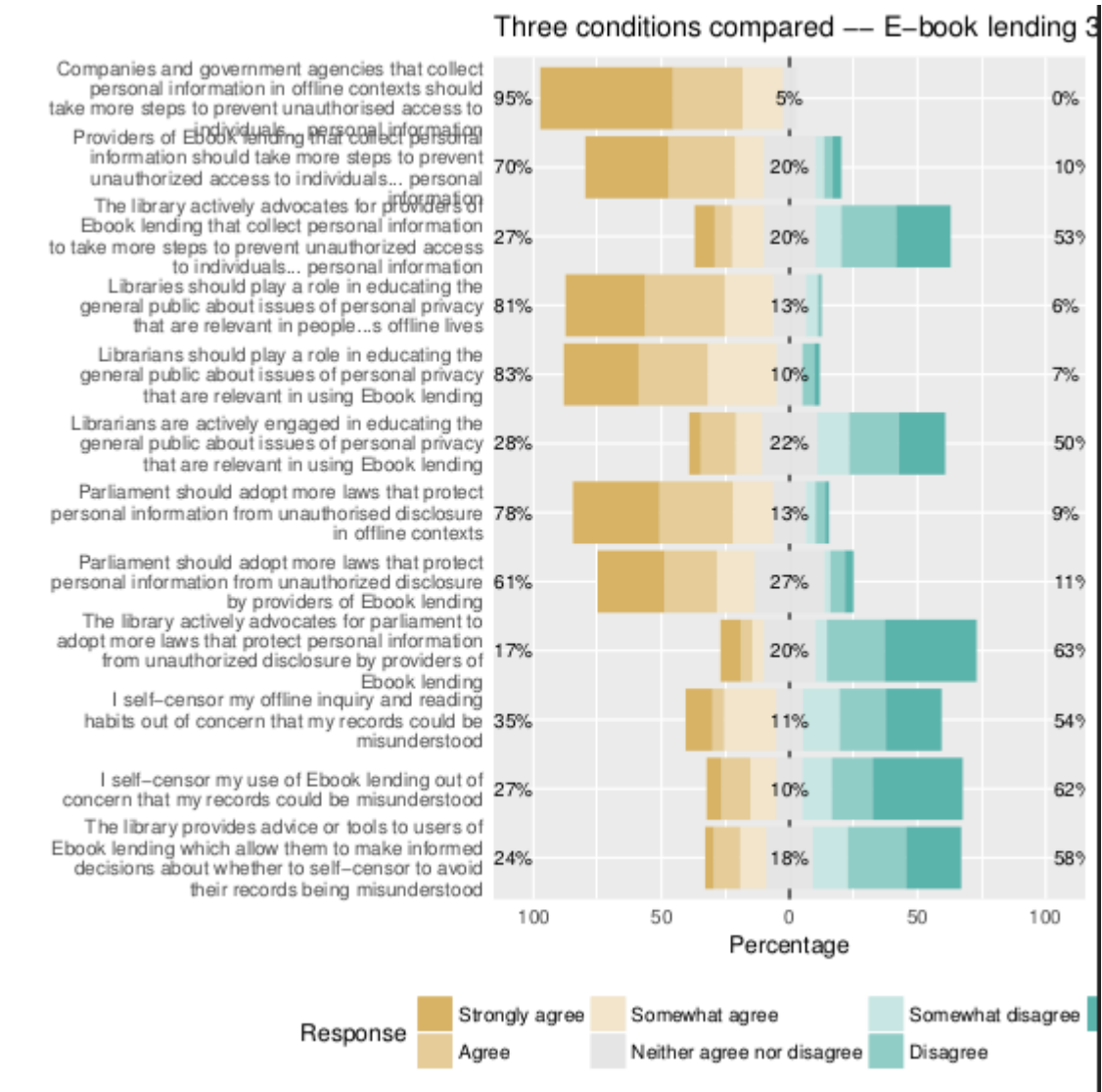


Appendix 11. Question by question comparison of Conditions 1 -3 (E-books 2 of 3)

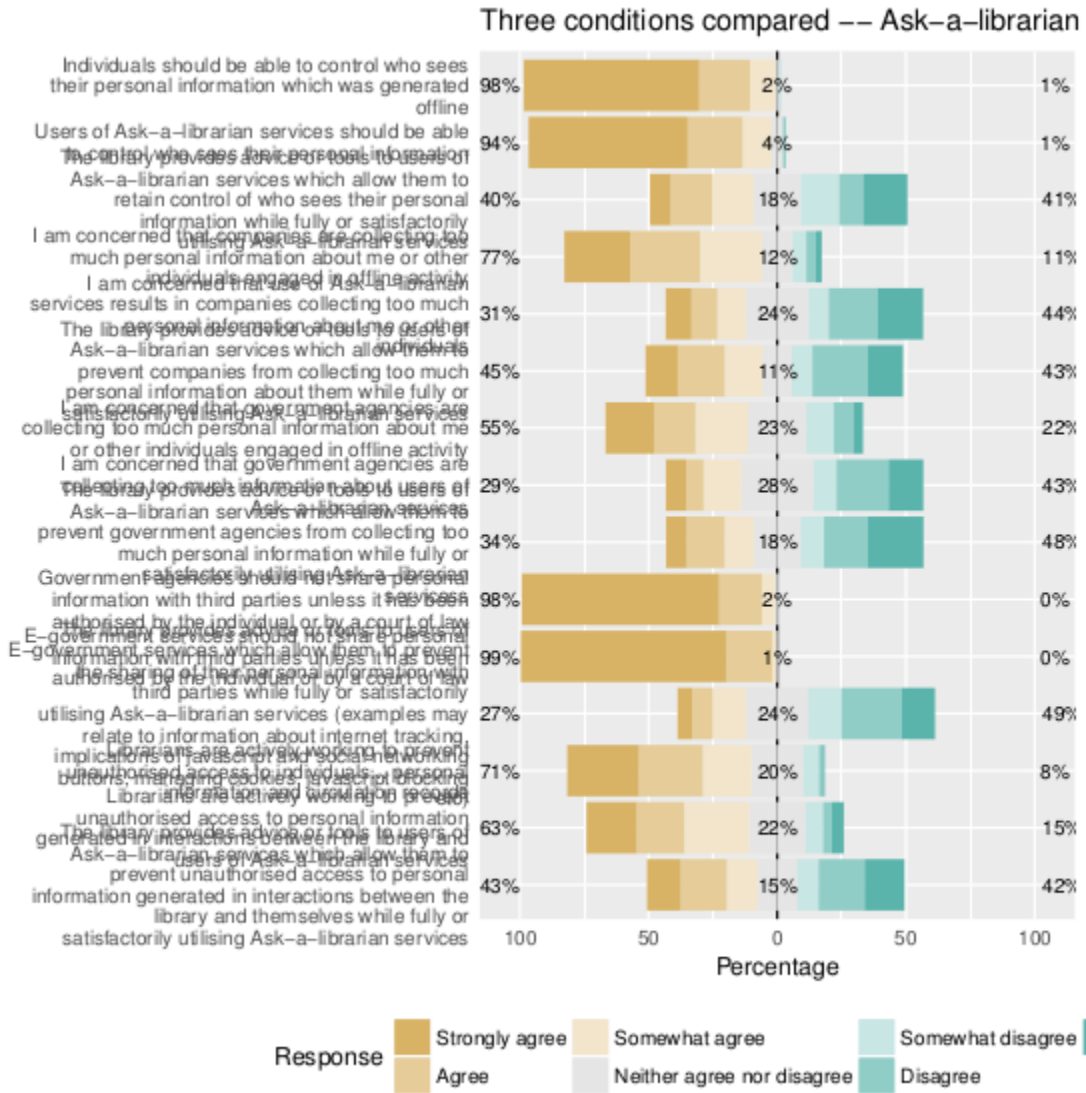
(Note that questions 7 have been reverse coded).



Appendix 12. Question by question comparison of Conditions 1 -3 (E-books 3 of 3)

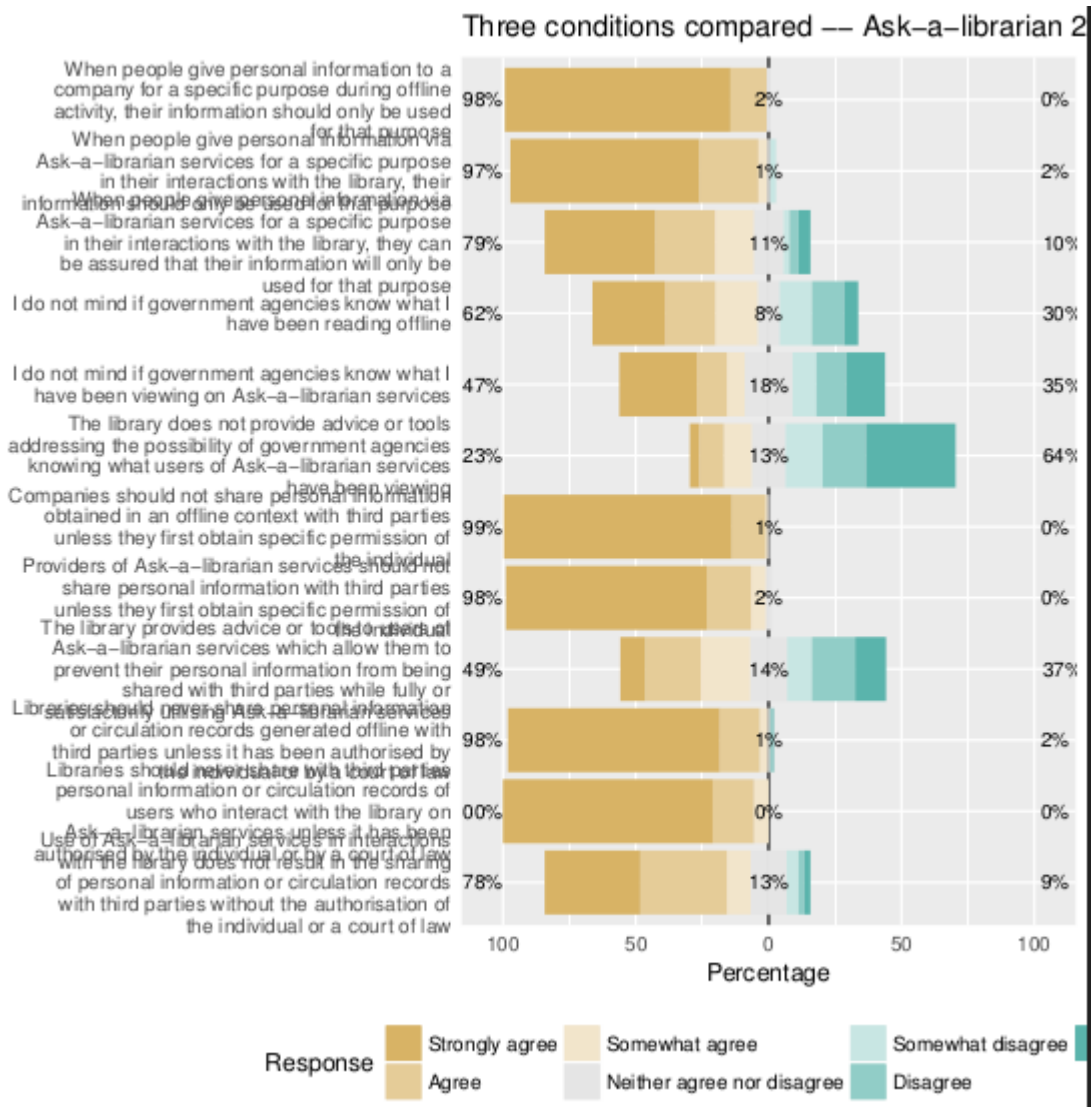


Appendix 13. Question by question comparison of Conditions 1 -3 (Ask-a-librarian 1 of 3)

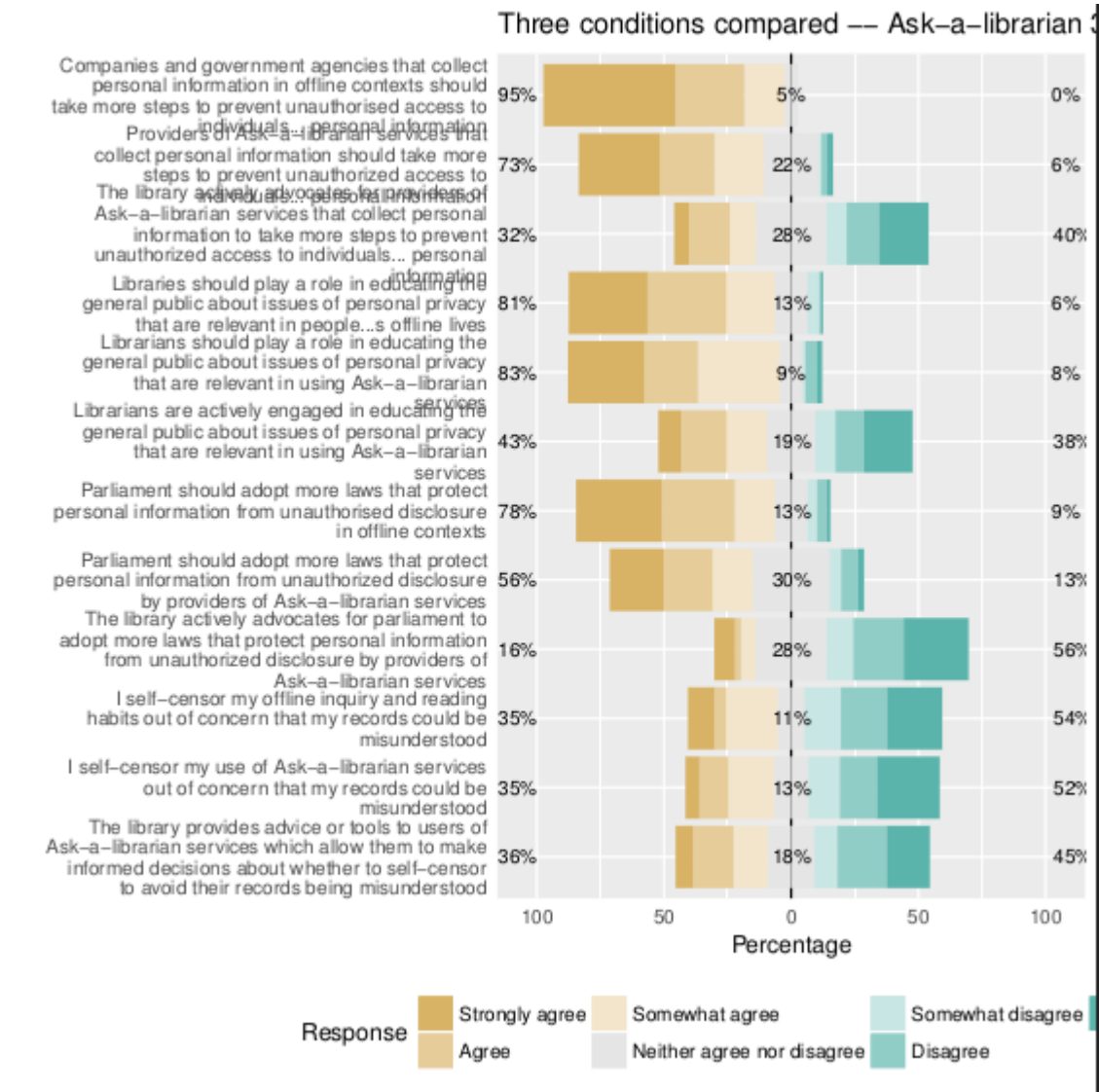


Appendix 14. Question by question comparison of Conditions 1 -3 (Ask-a-librarian 2 of 3)

(Note that questions 7 have been reverse coded).



Appendix 15. Question by question comparison of Conditions 1 -3 (Ask-a-librarian 3 of 3)



References

- American Library Association. (2004). Core values of librarianship. Retrieved November 2, 2016, from <http://www.ala.org/advocacy/intfreedom/statementspols/corevalues>
- American Library Association. (2007). Privacy Toolkit. Retrieved September 7, 2017, from <http://www.ala.org/advocacy/privacy/toolkit/policy>
- American Library Association. (2014). Privacy. Retrieved November 1, 2016, from <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>
- American Library Association. (2016). Library privacy guidelines for library websites, OPACs, and discovery services. Retrieved November 1, 2016, from <http://www.ala.org/advocacy/library-privacy-guidelines-library-websites-opacs-and-discovery-services>
- Andres, L. (2012). *Designing & Doing Survey Research*. London: SAGE Publications, Ltd.
- Appel, F. (2010). Revisiting Moor's Towards a theory of privacy in the information Age. *SIGCAS Computers and Society*, 40(2), 31–34. <https://doi.org/10.1145/1839994.1839999>
- Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4).
- Breeding, M. (2016). Issues and technologies related to privacy and security. *Library Technology Reports*, 52(4), 5-12,3.
- Bryer, J. & Speerschneider, K. (2016). likert: Analysis and Visualization Likert Items. R package version 1.3.5. <https://CRAN.R-project.org/package=likert>
- Campbell, D. G., & Cowan, S. R. (2016). The paradox of privacy: Revisiting a core library value in an age of big data and linked data. *Library Trends*, 64(3), 492–511. <https://doi.org/10.1353/lib.2016.0006>

- Corrado, E. M. (2007). Privacy and Library 2.0: How do they conflict? In *Sailing into the future : charting our destiny : proceedings of the Thirteenth National Conference of the Association of College and Research Libraries*. Baltimore: Association of College and Research Libraries. Retrieved from <http://codabox.org/12/>
- Cullen, R., & Reilly, P. (2007). Information privacy and trust in government: A citizen-based perspective from New Zealand. *Journal of Information Technology & Politics*, 4(3), 61–80.
- Farkas, M. (2015). More important than ever: privacy in the internet age. *American Libraries*, 46(11-12), 31.
- Fernandez, P. (2009, March). Online social networking sites and privacy: Revisiting ethical considerations for a new generation of technology. *Library Philosophy and Practice*, 1–9.
- Fortier, A., & Burkell, J. (2015). Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology & Libraries*, 34(3), 59–72.
- Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education. Retrieved from <http://scholarworks.iupui.edu/handle/1805/344>
- Gressel, M. (2014). Are Libraries Doing Enough to Safeguard Their Patrons' Digital Privacy? *The Serials Librarian*, 67(2), 137–142.
- Heiberger, R. M., & Holland, B. (2015). *Statistical Analysis and Data Display*. New York, NY: Springer New York.
- Kemp, R., & Moore, A. D. (2007). Privacy. *Library Hi Tech*, 25(1), 58–78.
- Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy an analysis of the privacy policies of digital content vendors. *Proceedings of the Association for Information Science and Technology*, 52(1), 1–9. <https://doi.org/10.1002/pr2.2015.145052010044>
- Leedy, P. D. & Ormrod, J. E. (2013). *Practical research: Planning and design (10th ed)*. Boston: Pearson.

- LIANZA (2013). Privacy statement for the sector. Retrieved August 29, 2016, from <http://www.lianza.org.nz/sites/default/files/Privacy%20Statement%20for%20the%20Sector.pdf>
- Lips, A. M. B., & Eppel, E. A. (2016). Understanding and explaining online personal information-sharing behaviours of New Zealanders: a new taxonomy. *Information, Communication & Society*, 1–16. <https://doi.org/10.1080/1369118X.2016.1184697>
- Macrina, A. (2015). The Tor browser and intellectual freedom in the digital age. *User Services Quarterly*, 54(4), 17–21.
- Malaga, R. A. (2014). Do web privacy policies still matter? *Academy of Information and Management Sciences Journal*, 17(1), 95–99.
- McCrum-Gardner, E. (2008). Which is the correct statistical test to use? *British Journal of Oral and Maxillofacial Surgery*, 46(1), 38–41. <https://doi.org/10.1016/j.bjoms.2007.09.002>
- Moor, J. H. (1997). Towards a theory of privacy in the information age. *SIGCAS Comput. Soc.*, 27(3), 27–32. <https://doi.org/10.1145/270858.270866>
- National Library of New Zealand. (n.d.). Directory of New Zealand libraries.. Retrieved October 31, 2016, from <http://natlib.govt.nz/directory-of-new-zealand-libraries>
- Nichols Hess, A., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. *The Journal of Academic Librarianship*, 41(1), 105–114.
- Parsons, C. (2015). Beyond privacy: articulating the broader harms of pervasive mass surveillance. *Media and Communication*, 3 (3), 1–12.
- Privacy Act 1993. Retrieved from http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html?search=ts_act_Privacy+Act+1993_reselel_25_a&p=1
- R Core Team (2015). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>.
- Revelle, W. (2017) psych: Procedures for Personality and Psychological Research, Northwestern

University, Evanston, Illinois, USA, <https://CRAN.R-project.org/package=psych> Version = 1.7.5.

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, 43(3), 322–335.

UN General Assembly. (1948). *Universal declaration of human rights* (217 [III] A). Paris.

van Dijck, J. (2014). Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197-208.

Victoria University of Wellington. (2016). Human ethics policy. Retrieved November 1, 2016, from:<http://www.victoria.ac.nz/law/pdf/human-ethics-policy.pdf>

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431–453. <https://doi.org/10.1111/1540-4560.00072>

Williamson, K. (2013). Quantitative data analysis. In K. Williamson & G. Johanson (Eds), *Research methods; information, systems and contexts* (pp. 395–416). Tilde University Press.

Zimmer, M. (2013a). Assessing the treatment of patron privacy in Library 2.0 literature. *Information Technology & Libraries*, 32(2), 29–41.

Zimmer, M. (2013b). Patron Privacy in the “2.0” Era: Avoiding the Faustian Bargain of Library 2.0. *Journal of Information Ethics*, 22(1), 44–59.

Zimmer, M. (2014). Librarians’ attitudes regarding information and internet privacy. *The Library Quarterly*, 84(2), 123–151.