



Privacy of Mhealth Systems: A National Survey on User Perspectives

Biplob Ray^{1*}, Susan Hunt² and Steven Gordon¹

¹School of Engineering and Technology, CQ University, Cairns, Melbourne, Australia

²School of Nursing, Midwifery & Social Sciences, CQ Univeristy, Australia



Abstract

Background: Personal electronic health devices, such as fitness trackers, heart rate monitors, blood glucose meters, blood pressure monitors and stress level meters, and related smartphone-based health applications are increasing in usage and popularity. These Internet-based medical technologies, which this paper refers to as mHealth systems, may be prescribed by a healthcare professional or purchased over-the-counter and make it easier for an individual to collect, access and monitor information relevant to their own health and well-being. However, as with many Internet-based technologies, and especially so with sensitive, personal health information, privacy is a significant concern. Actual or a perceived risk of privacy intrusions may delay the wider adoption of mHealth systems and even generate mistrust that reduces their long-term effectiveness. This paper contributes to the understanding of users' perspectives on information privacy in mHealth systems.

Objectives: To gain an understanding of current usage patterns and how important users perceive privacy, we have conducted a national survey in Australia. Understanding consumers' preferences and expectations provide directions for developers, lawmakers and researchers in creating an improved mHealth ecosystem.

Methods: As part of the National Social Survey by Population Research Laboratory of CQ University, participants who were 18 years or older were randomly selected from across Australia for telephone interviews. The participants were asked 10 questions about usage and privacy of mobile health systems. The collected data was tabulated, cleaned and analysed using SPSS and the resultant data set contained 1,225 cases with a total of 187 variables for each case.

Results: The survey reveals users of mHealth systems have a strong desire for privacy, e.g. more than 80% rate privacy important or very important and more than 60% think no personal information should be released to developers. The survey also shows around 70% of users never or rarely reviews privacy policies, and that they perceive the significant potential impact of intrusions, including increased health insurance costs, embarrassment and financial loss.

Conclusions: While the survey results show users desire privacy and have low trust of telecommunications and IT organisations, this conflicts with the technical design of mHealth systems: in many cases application developers, device manufacturers and telecommunication companies may have access to sensitive health information. The lack of standardization and guidelines for data processing by mHealth systems, as well as ineffectiveness of privacy policies, need to be addressed to avoid users' confusion and potential invasions of privacy.

Keywords: Privacy; Mobile Health; Computer User Training; Computer Security; Mobile Applications

Introduction

The mHealth systems transmit electronic health data for a variety of purposes: social sharing (e.g. updating fitness activities on social networks), record keeping (e.g. to access and process data from any device), comparative study (e.g. compare health information of users to identify patterns), or sharing with third parties (e.g. reporting health activities to a doctor, health insurance company or advertisement agencies). The data is transmitted via public networks (i.e. the Internet), often stored in Internet-based servers and may include: physical activity records, physiological data, location-based data, personal details and preferences. Together this data can represent very

OPEN ACCESS

*Correspondence:

Biplob Ray, School of Engineering and Technology, CQ University, Cairns, Melbourne, Australia,
E-mail: b.ray@cqu.edu.au

Received Date: 31 Jul 2026

Accepted Date: 07 Sep 2026

Published Date: 09 Sep 2026

Citation:

Ray B, Hunt S, Gordon S. Privacy of Mhealth Systems: A National Survey on User Perspectives. WebLog J Comp Sci Technol. wjcs.2026.i0902. <https://doi.org/10.5281/zenodo.22846865>

ISSN 3143-1038

Copyright© 2026 Biplob Ray. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

personalised and valuable information. Unfortunately, users of mHealth systems may not be fully aware of the privacy implications of their data being collected and transmitted. For example, device manufacturers, application developers, telecommunication providers, web site operators, and other third parties (e.g. advertisers, insurance companies, and healthcare providers) may all potentially access sensitive personal health data. Despite technical controls being available (e.g. encryption, access control), due to poor or inconsistent implementation of these controls, privacy intrusions continue to occur and can be expected to increase in the future [1-3].

Users' privacy in mHealth systems is an established research area where existing literature has investigated privacy law locally and internationally [2, 4, 5], as well as privacy policies of applications, devices and web portals [3, 4, 6, 7]. There are initiatives to devise technical solutions to improve privacy and ease of use of mHealth systems to increase acceptance among users. However there have been few attempts to understand privacy issues of mHealth systems from a users' perspective. It is important to analyse users' views on usage of mHealth systems and the related privacy issues in order to develop a sustainable and acceptable solution that will lead to wider acceptance of mHealth systems.

In order to understand users' view on usage and privacy of mHealth systems, we conducted a national survey in Australia. The survey aimed to find the usage of mHealth devices and applications, as well as users' perspectives on who they trust with the data collected and what value they place on privacy. This paper reports results and analysis from one of the few national surveys addressing mHealth privacy, and contributes insights on users' perspectives. This is a step forward to developing a user centric solution to provide better privacy protection of users for mHealth systems to boost users' confidence.

Background and Significance

Literature in the field of mHealth privacy and usage patterns can be classified into three main categories: privacy law [2, 4], privacy policy [2, 4, 6, 7] and identification of privacy risks [5, 8, 9]. There is also literature on users' views on wearable devices in health monitoring [1] in China and on electronic transmission of patient medical information [3, 10] across institutions in United States. This section discusses relevant literature to highlight the current state-of-the-art and the significance of our work.

In the articles of [2, 4], the issues related to mobile health application's regulation, safety, privacy and quality are discussed. The authors of these articles pointed out that there is no established standard privacy law to specifically protect the privacy of users of mobile health applications.

BinDhim NF, Trevena L [2] reviewed characteristics of the Apple iPhone Health app, including the app rating, privacy policy and functionality. They raised concerns about the lack of standardization of how mobile health applications present data, as well as the validation of that data by certified medical practitioners. They concluded that malicious intent of developers and sponsors can create serious privacy risks, and health related apps present a significant danger to users due to the sensitive nature of the information involved.

A number of papers [2, 4, 6, 7] have investigated the impact and standardisation of privacy policies for mHealth applications. Most investigations found that privacy policies of mHealth applications were either confusing or did not exist. McCarthy M [4] identified,

that despite efforts by the government to educate consumers and to provide guidance to developers, confusion persists amongst consumers due to large gaps in policies with respect to information access, security, and privacy. Sunyaev A *et al.*, [6] identified that the majority of health apps (70%) do not have a privacy policy, and for those that do, few focus on the app itself (rather on the company and website). According to [6] most of the available policies do not make information privacy practices transparent, require college-level literacy and are often too wordy to understand for general users. The authors suggested the need to develop international regulations for mobile health information collection, storage and privacy. The article [7] focused on mobile health apps for diabetes and again found that many of these apps do not have a privacy policy. They point out that users might mistakenly believe that health information entered into an app is private, particularly if the app has a privacy policy, but that generally is not the case. Worryingly, many of these mHealth apps access various services of mobile devices that are not related to their functionality, such as camera access or modifying the content of external USB devices. According to the study by [7], most apps share information with third parties that are not directly under the developers' control, such as data aggregators or advertising networks.

It is important to note that the sharing of sensitive health information by apps is not exclusively prohibited by the Privacy Act of Australian Privacy Principles [11] and there is no clear guideline about sharing information by apps with third parties in Australian Privacy Principles [11]. Therefore, sharing of information with third parties poses a significant privacy risk, as there are no legal protections against the sale or disclosure of data from medical apps to third parties.

The articles of [5, 8, 9] have studied the privacy risk level of mHealth apps and devices. Safavi S and Shukur Z [9] investigated existing models of Personal Health Record (PHR) for wearable devices and applications using Health Insurance Portability and Accountability Act (HIPAA) principles and six security properties (namely Confidentiality, Integrity, Availability, Authenticity, Authorization and Non-repudiation). Based on their investigation, the article has identified a need of universal standard for interpretability, user centric security control, improved data security and privacy. This finding motivated them to design and propose an improved security and privacy framework which considers client control over data and provides a comprehensive checklist for developers. The authors recommended that the framework should be adopted as a law to protect the privacy of mobile health information.

Mense A *et al.*, [8] analysed the technical capabilities of mHealth applications with respect to privacy risks. The authors simulated network transactions of actual mHealth applications, identifying when encrypted communications were used, and the possibility that data could be intercepted by third parties. The authors argue that a standard test framework to assess security and privacy of mHealth applications is important. At the same time, raising awareness among mHealth app developers and users around privacy issues through education is of critical importance.

Ratnayake H [5] analysed functionalities of mHealth applications to understand the level of privacy risks they pose to users. The thesis also investigated existing privacy laws to protect user's privacy. The investigation has identified that many of the apps create high degree of risk towards user's privacy. Existing European Union (EU) laws, which are facing a dilemma of harmonizing with laws from other

parts of the world, are inadequate to protect privacy expectations of the users. The author proposes a privacy risk assessment strategy and argues that it is one strategy to harmonize the EU laws, industry interests and actual privacy expectations of the users from health and wellbeing apps.

Customers' perspectives towards privacy and use of mHealth data has been studied in the past. The articles of [1], [10] and [3] have looked into customers' perspective towards usages and privacy of mHealth data.

Wen D *et al.*, [1] looked into user's perspective on usage of wearable devices. The data of [1] shows that 59.8% of users in China are discouraged to use health applications due to the privacy concerns. The paper by [3] identified that older adults place greater emphasis on provider as opposed to personal access for managing their mHealth data and privacy. At the same time, younger adults are highly likely to withhold information in mHealth system out of concerns for privacy and security. O'Donnell HC *et al.*, [10] looked into consumers' attitudes towards health information exchange between institutes and personal mHealth devices. The article has concluded that mHealth applications need to address consumer's security concerns and disparities in standards for health information exchange.

As detailed above, users of mHealth systems are concerned about the privacy of their data and confused about current security protection measures and relevant privacy laws. This shows the need of a user centric approach to address privacy issues of mHealth systems. As a step towards this, we have collected and analysed users' views of usage and privacy of mHealth systems.

Methods

This paper reports on data collected from 2016 National Social Survey (NSS-2016). NSS-2016 was conducted in November 2016 by the Population Research Laboratory at CQ University. The survey aims to obtain public opinion on a range of topics held by a random sample of Australian residents.

Telephone interviewing was used with 50% of the sample contacted *via* landline telephone, with geographically proportionate landline samples drawn to cover each of the 8 Australian states and territories, and 50% contacted *via* randomly selected mobile telephone numbers (which have no geographical marker). Telephone numbers were obtained *via* SampleWorx Pty Ltd, which selects random numbers using postcode parameters and removes known non-residential and non-working numbers. For each selected landline telephone number, one eligible person (18 years or older, usual place of residence) was selected as the respondent for the interview. Households were pre-selected as either a male or female household. For each mobile telephone number selected, the eligible respondent was deemed to be the person who received the phone call (if they confirmed an age of 18 or older).

A cluster sampling approach with Australian states and territories as clusters has been used to select the total of 1225 sample from the whole Australian population who are 18 years of age or older. The sampling units were selected completely on random basis from each cluster to ensure the equal chance of every unit in the population to be picked in the sample. Therefore, the sample used in this study can be assumed to be representative to the population. For further check of how well the sample ($n=1225$) generalized to the population ($N=20337681$) in terms of the distribution of Australian residents

(18 years or older) across all the states and territories, a one-sample chi-square test was conducted. Results indicated that the sample proportions of residents by states and territories were not significantly different from the population proportions by states and territories (χ^2 ($df=7$, $\alpha=0.05$) = 6.628, $p=0.469$).

Interviews were conducted by trained and supervised staff and supported using a Computer Assisted Telephone Interview system. Interviewing began on 2 Nov 2016 and completed on 29 Nov 2016, and performed between the hours of 10:30 am to 2:30 pm Monday, Wednesday and Friday, 4:30 pm to 8:30 pm, Monday through to Friday, and between 12:00 pm and 4:00 pm on Saturday and Sunday. Unsuccessful call attempts resulted in a minimum of 5 callback attempts.

The survey comprised a standard introduction, demographic and core health questions, as well as questions on specific topics. The questions were pilot-tested on 83 randomly selected households with interviewer and sponsor feedback used to create the final questionnaire. The average interview duration was 25 minutes and consisted of approximately 85 questions. Ten of the questions were on consumer perspectives of personal electronic health privacy - this paper reports on the answers to those ten questions as well as demographics questions.

With a total of 187 variables for each case, the NSS-2016 data set contained 1,225 cases. The survey response rate was 35%. The estimated sample error, at the 95% confidence interval, is ± 2.8 percentage points. Several questions were used for quality assurance. On a scale of 1 (very poor) to 10 (excellent), the quality of the interview had a mean score of 8.6. Almost all respondents (96%) found the survey questions very easy or mostly easy to understand (4-level Likert scale).

Results

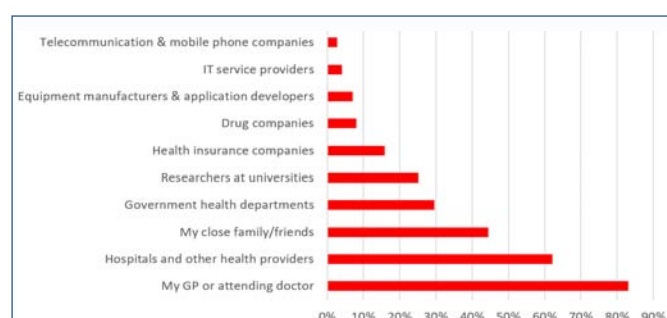
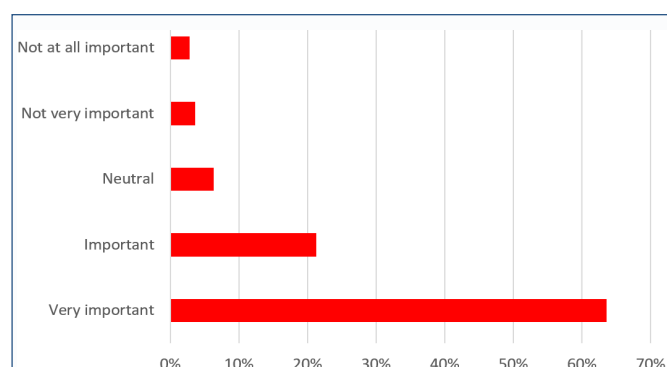
In this section, we present statistical analysis of our survey results. Selected tables and figures of the results are included, with additional data included in Appendix A. Although the survey data includes many different participant characteristics (e.g. income, education, age, gender), for brevity we present results group by three age categories (18-39, 40-64, and 65-101 years) and two gender categories (male and female).

We asked participants which methods they use to record or share their health information, allowing them to select from options such as journals, websites, devices and applications. As presented in Table1, approximately one third of participants were using at least one of the methods listed. The majority of participants were not using any methods listed in Table 1 to record or share their health information, with men and older people more likely not to do so. The most common method used by younger people was smartphone apps; by middle-aged people was electronic health devices; and by older people was a written health journal. Older people and women were generally more likely to use a written health journal. Younger men were more likely to use social media. Younger participants were more likely to use private health insurance and government websites and electronic health devices. Younger and middle-aged participants were more likely to use health or fitness websites, and smartphone apps.

We surveyed how likely participants are to use an electronic health monitoring device if offered by a healthcare provider. The most common response from people of all ages except older women,

Table 1: Methods used by participants to record or share health information (n (%)).

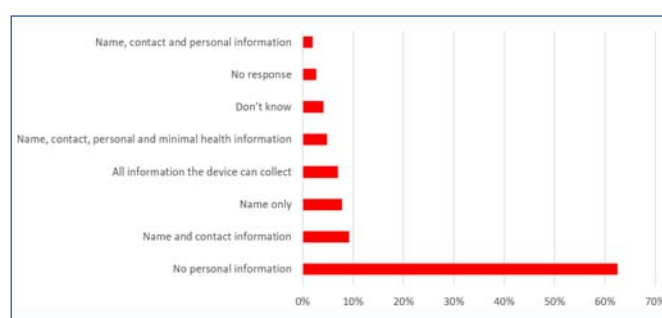
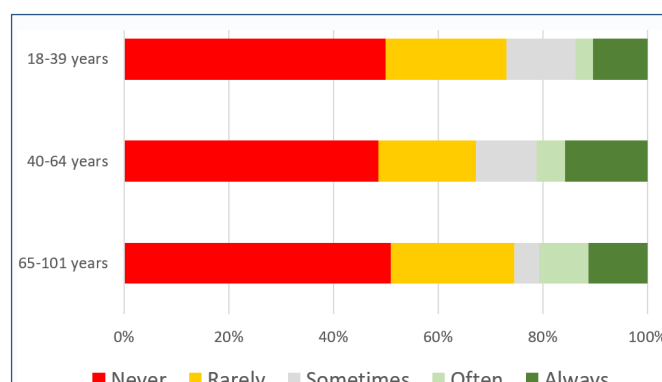
	18-39 years (N=291)		40-64 years (N=551)		65-101 years (N=383)	
	Men (N=149)	Women (N=142)	Men (N=273)	Women (N=278)	Men (N=162)	Women (N=221)
Written health journal	5 (3.4)	13 (9.2)	12 (4.4)	26 (9.4)	17 (10.5)	24 (10.9)
Online health journal	3 (2.0)	8 (5.6)	5 (1.8)	8 (2.9)	5 (3.1)	2 (0.9)
Social media	9 (6.0)	4 (2.8)	4 (1.5)	9 (3.2)	2 (1.2)	4 (1.8)
Private health insurance website	12 (8.1)	12 (8.5)	8 (2.9)	13 (4.7)	2 (1.2)	3 (1.4)
Government website	20 (13.4)	14 (9.9)	11 (4.0)	10 (3.6)	6 (3.7)	6 (2.7)
Health or fitness website	21 (14.1)	18 (12.7)	8 (2.9)	17 (6.1)	3 (1.9)	3 (1.4)
Electronic health device	22 (14.8)	27 (19.0)	27 (9.9)	32 (11.5)	11 (6.8)	13 (5.9)
Health or fitness smartphone app	26 (17.4)	30 (21.1)	19 (7.0)	25 (9.0)	2 (1.2)	3 (1.4)
None of the above	90 (60.4)	81 (57.0)	211 (77.3)	187 (67.3)	131 (80.9)	171 (77.4)

**Figure 1:** Parties participants trust to access data from personal healthcare devices and apps.**Figure 2:** Participants' attitudes towards the importance of data privacy on personal healthcare devices and apps.

was that they were likely to do so, with unlikely being the next most common. There were no significant effects for gender, with men and women equally likely to use a smartphone or wearable device. Younger people were slightly more likely to use such a device. These results are detailed in Table A.1 in the Appendix.

We asked participants which parties they would trust to have access to their data from personal healthcare devices and apps. As illustrated in Figure 1, the most commonly trusted party was doctors, with hospitals and other health providers the next most common.

Compared to older people, younger people were more likely to trust close family and friends, government, health insurance companies, and drug companies with mHealth data. Men were more likely than women to trust close family and friends, the government, health insurance companies, equipment manufacturers, researchers

**Figure 3:** Participants' attitudes towards information that should be made available to companies that create health devices and apps (n (%)).**Figure 4:** Participants' frequency of reviewing privacy policies of health-related electronic devices, apps or websites (n (%)).

at universities and IT service providers. These results are detailed in Table A.2 in the Appendix.

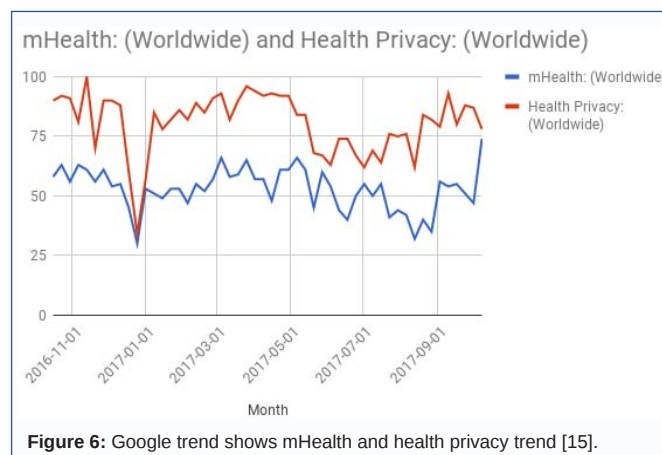
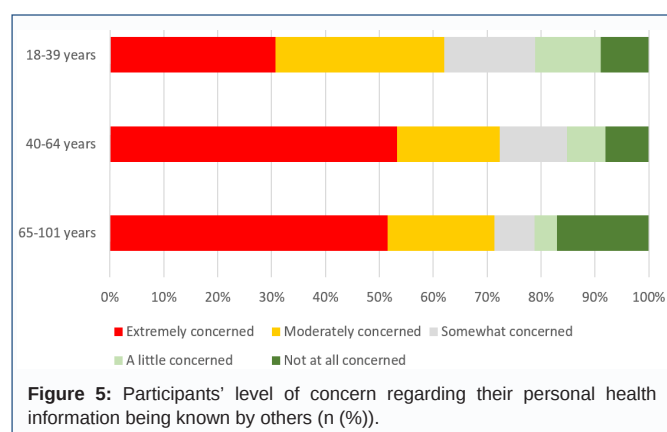
Figure 2 illustrates the importance participants place on the privacy of their mHealth data. The vast majority of participants consider their health privacy to be very important or important. Men consider their privacy slightly less important than women.

Middle-aged people consider their privacy slightly more important than other age groups. These results are detailed in Table A.3 in the Appendix.

When we asked about the information that participants believe should be made available to the companies that create mHealth systems, the majority of people believed that no personal information should be made available as illustrated in Figure 3. These results are

Table 2: Participants' issues of concern regarding their health information being made publicly available (n (%)).

	18-39 years (N=291)		40-64 years (N=551)		65-101 years (N=383)	
	Men (N=149)	Women (N=142)	Men (N=273)	Women (N=278)	Men (N=162)	Women (N=221)
Physical harm (bullying, assault)	30 (20.1)	33 (23.2)	45 (16.5)	69 (24.8)	26 (16.0)	51 (23.1)
Losing my job	44 (29.5)	32 (22.5)	57 (20.9)	66 (23.7)	16 (9.9)	31 (14.0)
Losing other income or financial entitlements	45 (30.2)	25 (17.6)	67 (24.5)	77 (27.7)	31 (19.1)	60 (27.1)
Changes to the cost of health insurance	64 (43.0)	46 (32.4)	129 (47.3)	108 (38.8)	65 (40.1)	80 (36.2)
Loss of social connections (friends, colleagues, etc)	35 (23.5)	18 (12.7)	47 (17.2)	55 (19.8)	27 (16.7)	47 (21.3)
Impact on my mental health	46 (30.9)	45 (31.7)	68 (24.9)	111 (39.9)	33 (20.4)	72 (32.6)
Waste of my time	55 (36.9)	37 (26.1)	102 (37.4)	123 (44.2)	61 (37.7)	85 (38.5)
Embarrassment	48 (32.2)	44 (31.0)	87 (31.9)	107 (38.5)	46 (28.4)	68 (30.8)
None of the above	45 (30.2)	48 (33.8)	84 (30.8)	74 (26.6)	60 (37.0)	76 (34.4)



also detailed in Table A.4 in the Appendix.

Figure 4 presents how often participants review the privacy policies of mHealth systems. Of the participants who use these platforms, the most common response was that they never reviewed the privacy policy, followed by rarely. Younger and middle-aged people reported reviewing privacy policies more frequently. These results are detailed in Table A.5 in the Appendix.

The level of concern participants have in relation to others knowing their personal health information is illustrated in Figure 5. The majority of participants across age groups were extremely or moderately concerned. Men were slightly less concerned, while middle-aged people were slightly more concerned. These results are detailed in Table A.6 in the Appendix.

Table 2 shows the issues that participants would be concerned about if their health information was made available to the public. The most common issue reported was that it would change the cost of health insurance. Younger people were secondarily concerned with associated embarrassment and wasted time. Middle and older aged people were also concerned about wasted time. Men were less likely than women to be concerned about physical harm or mental health. Men were more likely than women to be concerned about changes to health insurance costs. Younger and middle-aged people were more likely to be concerned about losing their job than older people.

Discussion

The survey results show that about one-third of the respondents record and/or share their health information in journals, websites or apps. Younger people, between 18 and 39 years of age, are likely to

be using websites and electronic health devices or smartphone apps.

It is expected the number of users of mHealth systems will see high growth [12-15] with mHealth application usage growing from 149.3 billion downloads in 2016 to 352.9 billion by 2020 [12], and the revenue more than doubling from 24.39 billion in 2017 to 58.8 billion in 2020 [15]. However, there is also data [15, 16] indicating users are aware of health privacy issues. Google Trend data in Figure 6 shows normalised global queries on Google about mHealth and health privacy. The patterns are closely aligned, indicating people have an interest in privacy (Figure 5).

This survey and other data [1] have shown that while a large part of the population use or have an interest in using mHealth systems, the majority of them believe that no personal information should be made available to companies that create these devices and apps. The entities least trusted by the survey respondents are telecommunication and mobile phone companies, IT service providers, equipment manufacturers, application developers and drug companies. However, the technical architecture of most personal health devices is such that these entities can potentially gain access to users' data. For example [9]:

- Most smartphone health applications report data back to servers which the application developers control, allowing direct, unfettered access to users' data.
- The above also applies for dedicated health equipment such as FitBit and Garmin devices. The equipment manufacturers control the servers which those devices communicate with.

• Unless strong security mechanisms are in place, it is possible that telecommunication providers, mobile phone companies and other IT service providers can also access users' data. As network operators, telecommunication providers and mobile phone companies can theoretically inspect all data traversing the network. Security mechanisms, such as HTTPS, can make the data inaccessible to network operators in this case. However, while HTTPS is in widespread use for smartphones and websites, small, portable medical devices may forego the security mechanisms to save on processing and battery life, exposing private data to the network operators. Similarly, without adequate security mechanisms, IT service providers may access have access to private data in the case that cloud computing is used by application developers.

The validity of this distrust is further justified from a technical perspective by [8] who used a controlled environment to evaluate and identify privacy leaks of wide range of mHealth systems.

The privacy of users' data may be compromised in several ways:

- Deliberate release by the company. For example, a company selling the data to other parties for marketing or insurance purposes.
- Accidental release by the company. For example, using no or poor implementations of security mechanisms, allowing other parties with unfettered access to the data.
- Release due to malicious third parties. For example, security attacks on products, websites or databases, leading to publication or sale of the data.

The survey results have shown that the majority of participants across all age groups were extremely or moderately concerned that their private health information may be made public. The main concern of a disclosure is an increased cost of health insurance, however other concerns (e.g. embarrassment, waste of time, impact on mental health) were also prominent. This suggests users are aware of both the financial and health costs of privacy intrusions. Correlating the perceived impacts of privacy intrusions with actual impacts may give insight into necessary education on health data privacy.

Just because companies can access users' data, doesn't mean they do. Most applications have associated privacy policies outlining what the developer may do with the data. A key finding of our investigation is that most users of mHealth systems do not review or read privacy policies. This aligns with conclusions from other studies with respect to privacy policies [6], but is still a significant finding as it is specific for mHealth data. The ignorance of privacy policies observed also suggests that the policies are of little help in raising awareness about the issues or protecting users' electronic health information. Other problems with privacy policies is that they are not necessarily binding agreements [2, 4, 6, 7], and it is difficult for a user to know if the privacy policy has been implemented effectively.

In summary, this survey highlights the mismatch between user's behaviour with mobile health applications (i.e. they are often used, and it is expected the usage to grow) and their expectations of privacy.

Conclusion

Use of personal mobile Health (mHealth) devices and applications is rising, and further uptake has the potential to improve mental and physical health outcomes. However, the sensitive nature of the data used in mHealth means, without adequate privacy protections, users may be severely impacted if intrusions occur. This paper conducted a

national survey to obtain public opinion on a range of topics held by a random sample of Australian residents. Our analysis on collected data reveals usage preferences and privacy perspectives of users of mHealth systems. For example, most of the people expressed their confidence towards the mHealth system provided by a healthcare provider. Furthermore, most of the users expressed that privacy of data is very important to them but they are confused with current privacy provisions as current measures to protect users' privacy is complex and not user friendly. We believe this national survey will help mHealth systems developers, law makers and health providers to better understand users' requirements.

Acknowledgements

This research is undertaken as part of our CQ University Population Research Grant Scheme (PRGS).

NSS-2016 received approval by the Human Ethics Research Review Panel at CQ University before administration to the general public. Project: H14/09-203, NATIONAL SOCIAL SURVEY 2016.

References

1. Dong W, Xingting Z, Jianbo L. Consumers' perceived attitudes to wearable devices in health monitoring in China: A survey study. *Comput Methods Programs Biomed.* 2017; 140: 131-137.
2. BinDhim NF, Trevena L. Health-related smartphone apps: regulations, safety, privacy and quality. *BMJ Innovations.* 2015; 1(2): 43-45.
3. Le T, Thompson H, Demiris G. An examination of electronic health information privacy in older adults. *Stud Health Technol Inform.* 2013; 192: 709-713.
4. McCarthy M. Federal privacy rules offer scant protection for users of health apps and wearable devices. *BMJ.* 2016; 354: i4115.
5. Ratnayake H. Privacy risk assessment in relation to health and wellbeing apps: Towards harmonizing the European laws, industry interests and the privacy expectations of the users. University of Oslo. 2015.
6. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc.* 2015; 22(e1): e28-e33.
7. Blenner SR, Köllmer M, Rouse AJ, Daneshvar N, Williams C, Andrews LB. Privacy policies of android diabetes apps and sharing of health information. *JAMA.* 2016; 315(10): 1051-1052.
8. Mense A, Urbauer P, Sauermann S, Wahl H. Simulation environment for testing security and privacy of mobile health apps. 2016.
9. Safavi S, Shukur Z. Conceptual Privacy Framework for Health Information on Wearable Device. *PLOS One.* 2014; 9(12): e114306.
10. O'Donnell HC, et al. Healthcare Consumers' Attitudes Towards Physician and Personal Use of Health Information Exchange. *J Gen Intern Med.* 2011; 26(9): 1019 -1026.
11. Australian Privacy Principles (APPs). The Privacy Act, Health information and medical research' Australian Privacy Foundation. 2017.
12. Statista. Mobile App Usage - Statistics & Facts. 2017.
13. Ventola CL. Mobile Devices and Apps for Health Care Professionals. *Uses and Benefits.* P T. 2014; 39(5): 356-364.
14. Price Waterhouse Coopers (PWC). Emerging mHealth: Paths for growth. 2017.
15. Google Trends. 2017.
16. Statista. mHealth (mobile health) industry market size projection from 2012 to 2020 (in billion U.S. dollars). 2017.