Industry and Community Project
Final Report 2020

Industry Project Final Report

Education on Data Privacy

Team 10

Anchilee Scott-Kemmis
Shiqi Jiang
Chay White
Hoang Minh Le

Executive Summary

Our project inspiration stemmed from our understanding of contemporary issues in data privacy. Australia ranks 5th in the world for largest amount of data stolen per capita, with a ratio of 2:1 (ref). The response was the Australian Privacy Act in order to tackle this issue but the success was insufficient. Therefore, a data privacy education system was suggested. Unfortunately, it is uncertain whether the Australian public want and think education on data literacy is required. The project aimed to identify people's opinion and knowledge on data protection through socio-economic, cultural and demographic backgrounds and to understand the reasoning. The team created a survey, using external statistics and data as well as conducted literature reviews as an approach to this challenge. After the analysis, we found relationships between certain clusters (e.g. age, occupation etc.) We concluded that there are groups that want to learn data literacy and there are those who do not. We agreed that despite this conflict, it is necessary to educate ourselves on this matter regardless of background. With that outcome in mind, it is recommended that we create a strategy for digital education in Australia or take initiatives like publishing free courses. This project could be a stepping stone for further research on how to educate the groups of people identified.

Introduction

Data has been an important asset for both technology and society as it allows us to remove some of the burden from our daily lives. Data-driven AI is able to recognise our face from multiple angles to unlock our phone, they can also automate tasks that would take humans days to complete and data is also used for analysis, but in many other fields too like finance or medicine (Joshi, 2017). Although the benefit is clear, with great power comes great responsibility (Appelgren 2019) and so personal information needs to be carefully used as data breaches have been a worldwide issue for the last couple years. In 2020, Melbourne Polytechnic disclosed personal information of students and staff without their permission (Hendry, 2020). According to data from Privacy Rights Clearinghouse (2019), there was a drop in the number of data breach victims in The US.

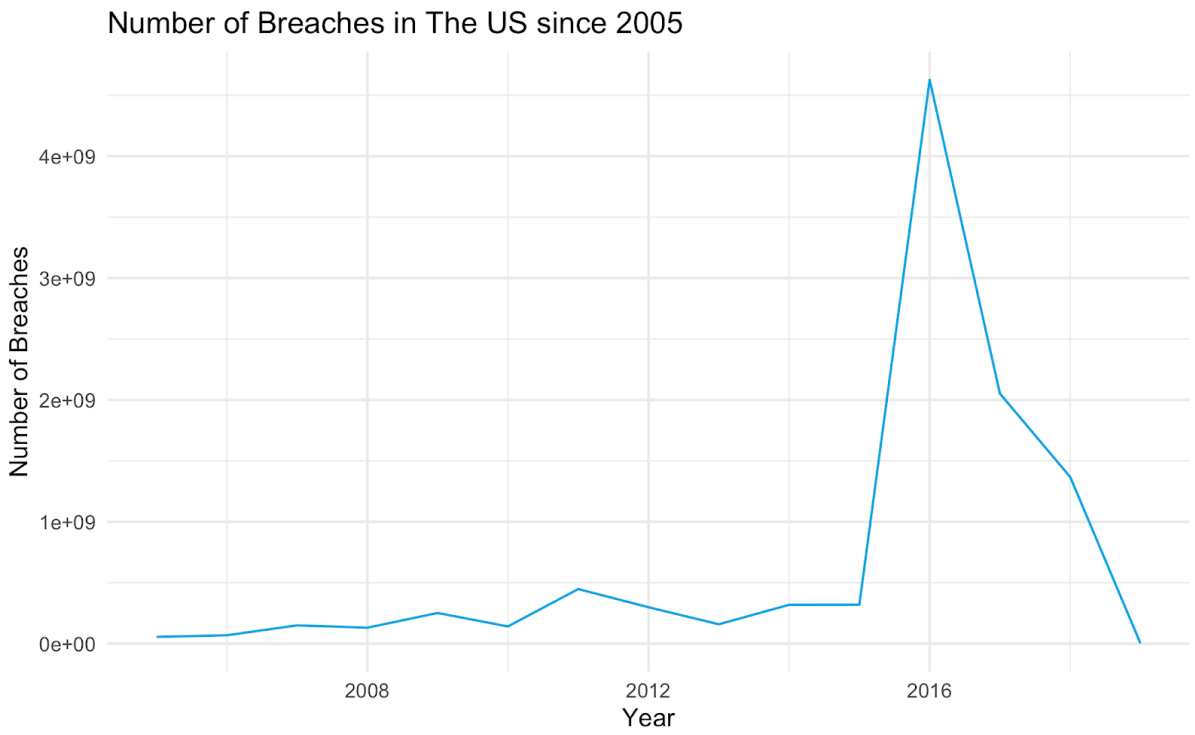


Figure 1: Number of Breaches in The US by Year, 2019

The fact that numerous people's data is stolen encourages more than 75% of the countries around the world to draft legislation around data privacy (United Nations Conference on Trade and Development, 2020). Probably the most well-known framework is the GDPR that was constructed by the EU, and what Australia partially adopted to update the Australian Privacy Act (Office of The Australian Commissioner, 2018). These legislations were designed to guide governments agencies and organisations on how to manage personal information to protect privacy (Office of the Australian Information Commissioner, 2018). This can be considered as an effective action to tackle the challenges (European Commission, 2019) but the recent examples show that further measurements are necessary.

There are many ways to improve data protection, such as frequent framework updates or publishing resources that could help avoid online harm, but the solution this report is going to elaborate is the education of data privacy and literacy. It was proven that learning about data could raise awareness of how we handle personal information online. According to Heufner (2009), employees disclosed less unauthorized personal information in health care insurance plan agencies after undertaking a 3 years training program on data privacy or based on Arain and Tarraf's work (2019), staff in health organisations, that completed training, were more likely to react correctly to spam emails than those who do not receive any training. Therefore, it would be a great step for the Australian Government to set the requirement of learning data literacy in the classroom and work places as there is no plans on this matter.

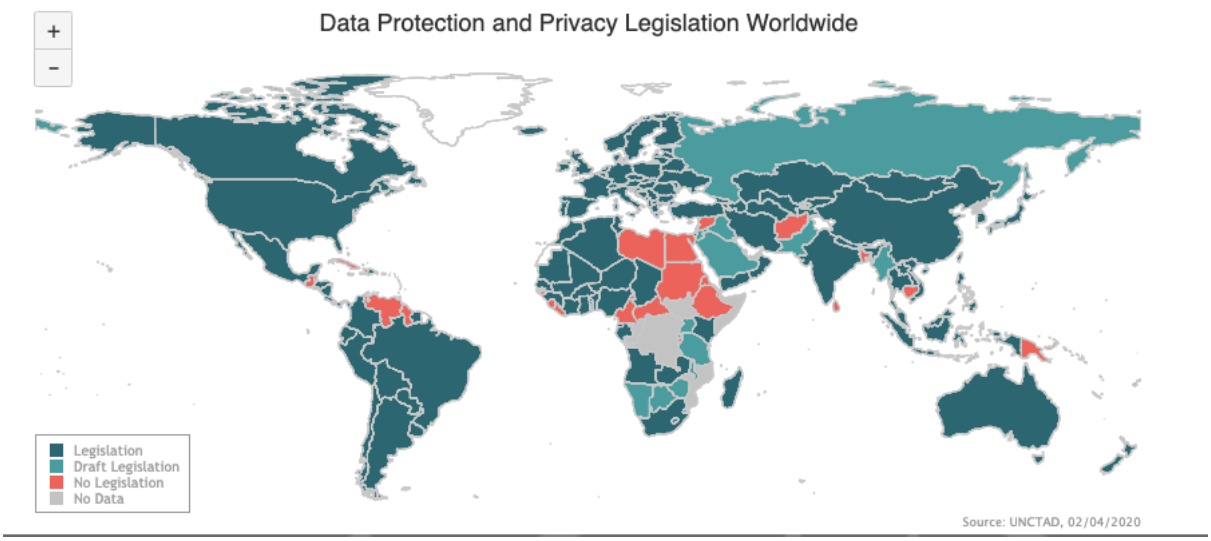


Figure 2:Data Protection and Privacy Legislation Worldwide, 2020

However, this suggestion is not as simple as it sounds. It is not confirmed whether the Australian public thinks data privacy education is needed, and we do not know exactly how informed they are on online personal information. It is possible that Australian citizens are well-aware of their data already, and the root of the problem is different in this country. We are also uncertain whether people would welcome this learning material openly, because not everyone sees the whole picture of the issue. There are possibilities that the majority of individuals do not want to be educated on data privacy.

Aim

The aim of the project was to identify clusters of people who want and do not want education on data privacy in order to assess the current view of Australian public on online harms. We would like to find clusters - such as age, cultural backgrounds and/or occupation - that could be linked to people's dislike toward data literacy and try to understand the reason behind the reluctance of this subject. The project grouped individuals based on cultural backgrounds using Hofstede's Cultural Dimensions as well as analysing them from socio-economic and demographic perspective.

To draw a bigger picture, it is also important to classify individuals who are willing to pick up the necessary knowledge to protect their personal information and affirm the need of education in Australia. The goal was to prove that education on data privacy is almost unavoidable if we want to protect our personal spheres. We also investigated how other nations handled the problem from an educational point of view to see if it was possible to implement our proposal in Australia. Finally, we also discuss how this work could be useful in developing a better data privacy framework in Australia.

Methodology

Prior to completing the presentation, each team member was responsible for a variety of different roles that were best suited to their disciplines and expertise. This was done in order to allow for the best efficiency but to also conduct the most appropriate research and data. Nevertheless, as the project continued, our roles shifted to a small degree in order to accommodate each other and to assist each other in areas that were needed. We communicated through Zoom on the daily and kept each other updated through instant messaging on Facebook.

As a collective group, the team worked homogeneously with very little to no hiccups throughout the process. We had open communication and were very open-minded to each other's ideas and knew when we needed to work towards a compromise or sway towards another member's idea instead. This strongly encouraged us to perform to the best of our abilities within the short time frame we had.

Individual Methodology

Hoang comes from a data science background, as a result of his natural pragmatic thinking and him being bilingual, he was assigned the task of searching and analysing data and conducting research in Hungarian. Hoang also volunteered to take on the task of formatting our documents. Besides, he was interested in statistical summaries and international case studies about data privacy education, and assisted Chay in gathering information. Aside from conducting literature review in English and Hungarian, Hoang visualised data from the survey using R programming language to support the presentation and report. In the rare circumstance that a team member was unable to complete a task, Hoang was responsible for assigning the tasks in order to accommodate everyone.

Chay's role was in conducting secondary research into our various demographics, he specialised and specified in the comparison of age, gender and ethnicity. Chay was assigned this role as a result of his macro-economic background. Continuing, Chay also explored correlations between the need and want for education on individual data privacy through the individual's level of education. Alongside Hoang, Chay also assisted in the analyses of the data collected. Later, Chay also assisted Anchilee in the role of proof-reading our documents in order to maintain cohesion amongst one another. Throughout the project, Chay was also able to suggest other possible areas to conduct research that would encourage a more detailed research and result; acknowledging for a deeper understanding of our demographics.

Anchilee was responsible for conducting research through a sociological perspective, which is her speciality. She researched various sociological theories that she could use to assist the primary research and data collected through the survey. Anchilee compared individualistic and collectivist cultures together through Hofstede's Cultural Dimensions Theory in order to draw an understanding on if specific cultural dimensions wanted or needed more education on individual data privacy. She also examined the issue through intergenerational perspectives too. Nevertheless, Anchilee was also responsible for analysing the primary research gathered through the survey using her knowledge on qualitative

methods. On the more practical side of the project, Anchilee also took on the role of proof-reading documents that her group members have written down. Alongside Chay, they were both able to maintain cohesion. Anchilee's role through-out this project did not alter as much as anticipated.

Shiqi's role throughout this project was extensive. She had a wide variety of roles. To begin, she was responsible for the formatting of the survey that was sent out. She drafted the survey, created the questions after our group discussions and finalised it. Shiqi was also responsible for conducting research through a socio-economic perspective, researching whether there was a correlation between different socio-economic groups on the need and want for education on individual data privacy. This stemmed from her commerce background. Shiqi also conducted case study research in Mandarin, comparing countries beyond Australia's borders in order to come up with the most appropriate recommendation for possible future frameworks. Shiqi's role through-out this project also did not alter as much as initially anticipated.

Team Methodology

The methods the group applied for the project included research through the usage of a survey via google forms and was sent out to a large number of people. The survey was left open for approximately 3 and a half days, in order to allow for us enough time to conduct the survey analysis. This method demonstrated to be an interdisciplinary approach, as all group members were familiar with the formatting and how surveys should be conducted.

Another type of research the group conducted was through the usage of secondary information, including ProQuest Central, Heinonline, and Springer ebooks which allowed literature, case studies and theories research. Each of our individual disciplines had specific approaches to conducting research but nevertheless, it seemed as though we were able to go beyond our own disciplines and looked into areas of other disciplines too.

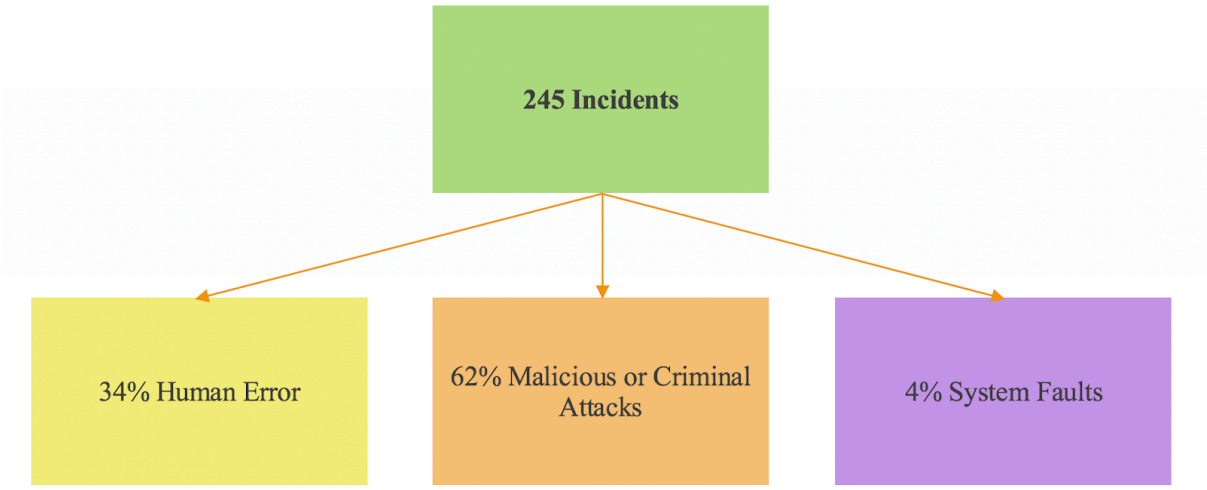


Figure 3: Number of Data Breaches Incidents in Aus. from April - June 2019, 2019

Results

Problem Landscape

The findings from the Office of the Australian Information Commissioner's (OAIC) 2019 report into data theft in Australia, revealing that there were 245 individual cases of data theft, between the 1st of April and the 30th of June, of which 34% was due to human error, 62% were due to malicious or criminal attacks and only 4% were related to system faults. Of the malicious or criminal attacks 43.81% were due to employees being targeted by Phishing scams, only 8.75% and 2.86% were due to hacking and malware respectively.

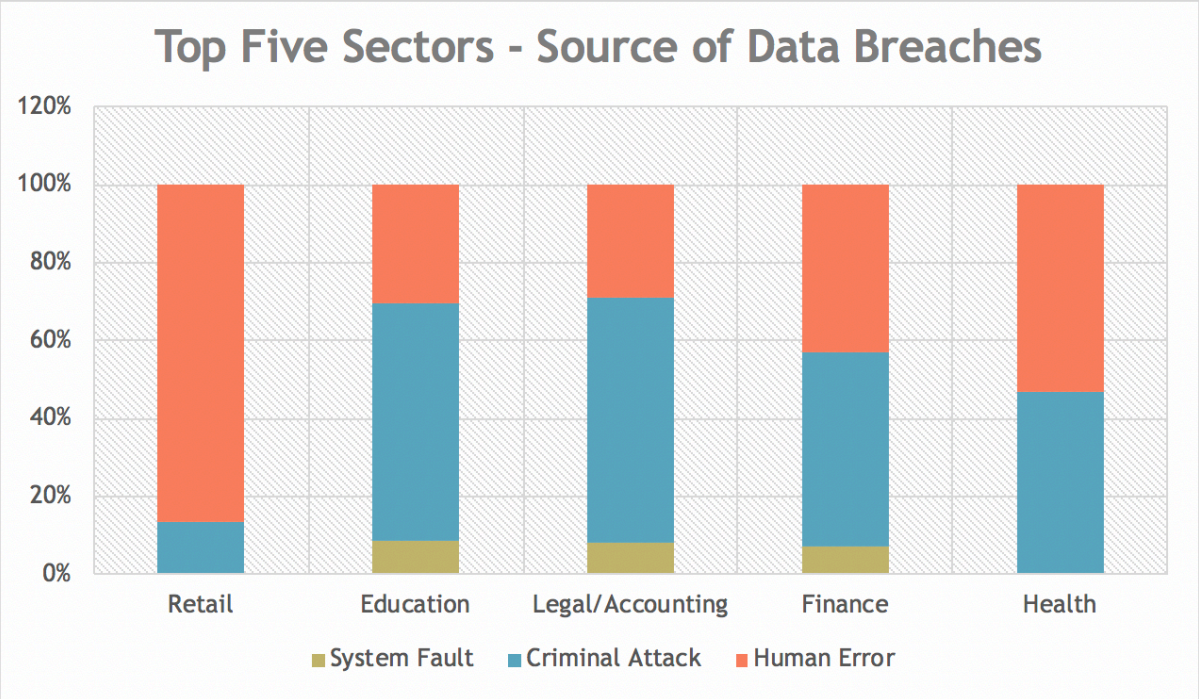


Figure 4: Distribution of Types of Data Breaches in Organisations, 2019

Demographics and Education

The five sectors with the highest incidence of data theft were identified by the OAIC as Retail, Education, Legal and Accounting, Finance and Health. We were able to identify contact information as being the most common form of data stolen, followed by financial details and identity information. Overall, Health service providers filed the most notifications of data theft in this period, at 47 notifications, 31.13% of the total. Finance was similarly affected with 42 notifications representing 27.81%. Legal and Accounting, Education and Retail had lower incidences at 15.89%, 15.23% and 9.93%. In contrast, Health recorded the lowest incidence of criminal or malicious attacks. Finance and Legal and Accounting industries recorded the highest incidence of criminal cyber-attacks, both being dominated by Phishing scams.

Industry	Average Age	Sex %	Size	Education
Finance	39 yrs	48.1%F 51.9%M	823,000	50% Bachelor Degree 24% Cert 3 or Higher 23% No Post School Education 3% Other
Health	42 yrs	79%F 21%M	801,000	48% Bachelor Degree 32% Cert 3 or Higher 16% No Post School Education
Retail	39 yrs	55%F 45%M	1,189,100	16% Bachelor Degree 26% Cert 3 or Higher 53% No Post School Education
Education	38 yrs	73.2%F 26.8%M	261,585	65% Bachelor Degree 19% Cert 3 or Higher 13% No Post School Education
Legal/Accounting	38 yrs	51.5%F 48.5%M	259, 211	63% Bachelor Degree 19% Cert 3 or Higher 16% No Post School Education

Figure 5: Demographic Distribution of Industries, 2019

The mean age of employees working in these key industries were between 38 and 42 years old, placing them in the middle-aged category of our survey. Other demographic analysis revealed that of the five industries Finance, Retail and Legal and Accounting had a nearly equitable gender spread. Health and Education were heavily female centric, with female participation rates in the 70's for both. Further analysis identified a positive trend of high levels of education attainment in these industries, suggesting a correlation with high incidences of data theft. Four of the five industries have the majority of employees holding bachelor's degrees or higher. Through our survey we identified that the majority of individuals holding a bachelor's degree or higher identified as both wanting and needing education on data privacy.

Socioeconomic Groups and Education

The study showed that Americans with lower levels of income and education express heightened concerns about their informational and physical privacy and security (Madden, 2020). Crucially, 52% of individuals in low socioeconomic households expressed they were very concerned about not knowing what personal information is being collected about them or how it is being used. This sentiment is mirrored by individuals who do not have high school degrees. It also proved that there is a positive relationship between income and education, where higher educational attainment leads to higher total incomes. ("Income | Department of Education, Skills and Employment", 2020).

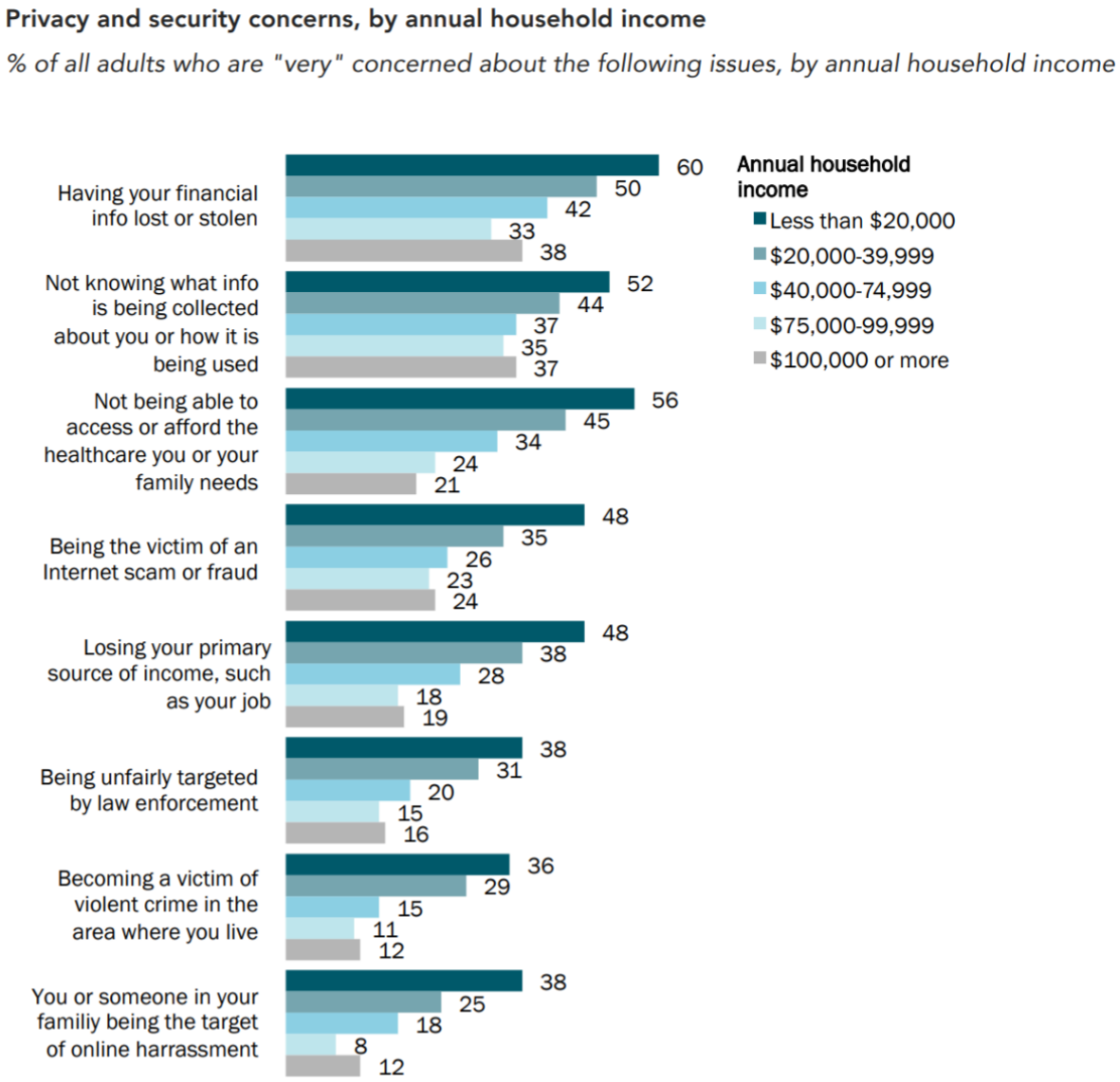


Figure 6: Privacy and Security Concerns by Annual Household Income (Madden, 2020)

Research into the different socioeconomic groups in the data collected from the survey, found that the majority of both low-income and high-income individuals want and need education on data privacy in Australia. However, there are higher prevalence's of

individuals from the high-income group that find their education on data privacy protection lacking. The survey found that most people have “very little” or “no” understanding of law and regulations on data privacy protection, wider reading suggests it is hard for them to understand the privacy laws (Brooke et al., 2020). Overall, our primary research observes that although it is more crucial for people in low-income to receive relevant education to avoid being victims in data breaches, the high-income group have positive attitudes towards education on data privacy.

Our survey also collected the data of different occupations including students, audio engineers, managers etc. The survey was designed to group those occupations into data focused, non-data focused and other. The findings revealed that most students, tutors and other occupational groups that were not data focused are more likely to need and want education. The data relevant occupations group however are less likely to want education on data privacy.

Individualism, Collectivism and Education

We compared Australia to six other nations, Thailand, China, the United States, The United Kingdom, Canada and Hungary. The data provided through Hofstede’s cultural analysis demonstrated that Australia ranked to be one of the highest individualistic countries, alongside the United States and United Kingdom (Hofstede, 2007). Nevertheless, the individualistic countries which include Canada and Hungary, ranged from 80-90, which are significantly different from collectivist countries like Thailand and China, which scored 20 on the scale (Hofstede, 2007).

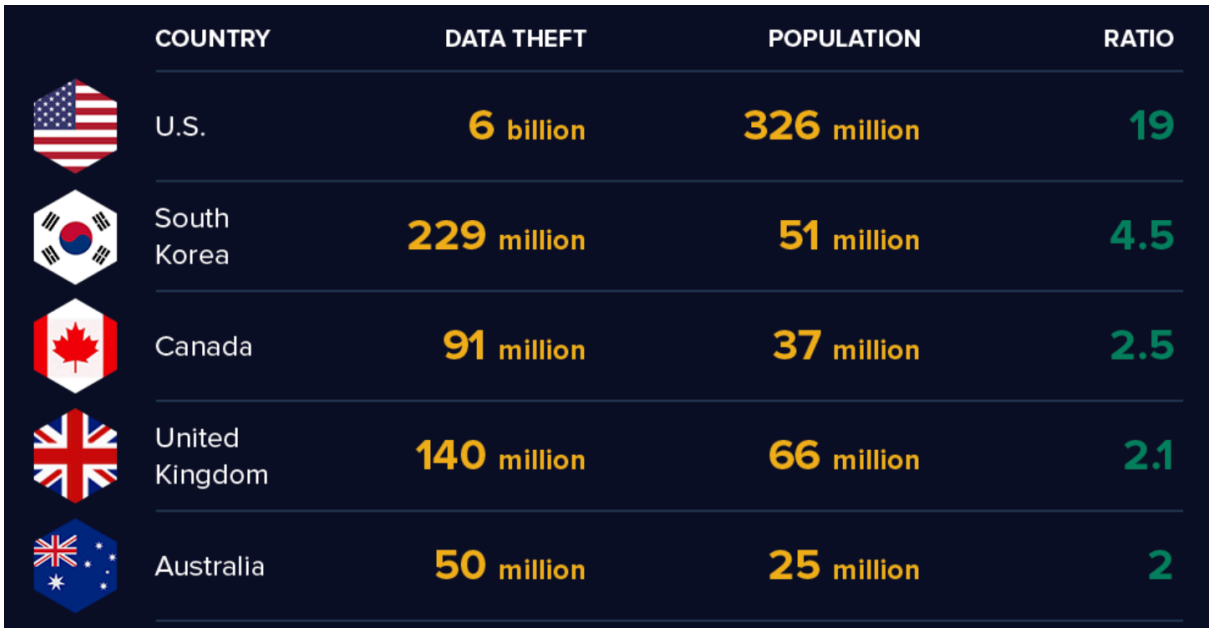


Figure 7: Countries with Most Data Breaches, 2020

Figure 7 demonstrates that according to Sobers (2020) Australia ranks fifth in the world for highest data breaches per capita alongside the United States, South Korea, Canada and the United Kingdom. Furthermore, the results of the survey indicate that over 50% believe they need education on data privacy and over 50% of individuals also want to receive education on data privacy. Nonetheless, 25-28.7% of individuals believe that they may need education on data privacy, as seen in figures 22 and 24.

Literature review - International Case Studies and Education

Literature reviews covered three areas of the topic: reviews in Hungarian, international case studies and Australian papers. Most academic papers in Hungarian discuss technological attitudes of teaching staff and how IT gadgets are used in the classroom. Tomasovszky (2014) researched how information technology is used in primary schools. Békési (2010) researched the mindset of educators when it comes to technology. A Hungarian study on the harmful facets of the internet (Soltész, 2017) was also utilised to understand the consequences of disclosed personal information. The Hungarian government's framework for digital education strategy (Hungarian Government, 2016) was also analysed to see how another country tackles this challenge.

In terms of international case studies, we found instances of how other nations raised awareness on data privacy. Countries like Norway (Norwegian Directorate of Education and Training, 2007) or Scotland (Scottish Association for Mental Health, 2017) published resources that helped citizens learn about preventing online damages. There are also attempts at teaching data analytics in the classroom for teachers (Rodriguez-Triana, 2016) and students (Hoogland, Schildkamp, Kleij, Heitink, Kippers, Veldkamp, Dijkstra, 2016).

When it comes to Australian resources, a report was identified about the Australian public's attitude toward online privacy (Office of Australian Commissioner 2017). It details the current knowledge and opinion of Australians on issues related to data protection. The survey suggested that the general public is well-aware of online harm and took some precautions. The report details the opinion of citizens about organisations (such as health and finance companies being the most trustworthy entities) when it came to data privacy and displayed their current online behaviour. We also found a paper on impacts of data breaches in healthcare within Australia that (Williams, Hossack 2013).

Analysis

Demographics and Education

The five sectors with the highest incidences of data theft were identified by the OAIC as Retail, Education, Legal and Accounting, Finance and Health. Breaking down these industries into demographic makeups, the mean age of employees working in these key industries were between 38 and 42 years old, placing them in the middle-aged category of our survey. The close grouping of age data points identifies this cluster and places them in the industries with the highest incidences, suggesting the strong correlation between this age group and human error relating to data breaches. Interestingly, a cross examination of our survey and the data found through literature review reveals that individuals in this age bracket were most likely to not want education on data privacy. Furthermore, middle aged individuals are also reluctant to be educated, reminding them of the over-structured education they experienced from their younger years, finding it difficult at their age or only willing to study if it will further their career (Olkinuora 2008). It is also known that data literacy involves information technology one way or the other. A study from Singh (2014) showed that older generations are selective about what technology they would use which could be a crucial problem. This finding is also supported by Herold (2011) who observed the relationship between employees lack of training and personal data breaches within companies. There is a possibility that the age groups unwillingness to learn about data privacy and the tactics needed to avoid breaches has resulted in the high levels of human error uncovered in our report.

The trend of high levels of education attainment in the mentioned industries also correlates with the trend of individuals who have achieved a bachelor's degree identifying the need for education on data privacy. A contradiction was identified, the majority of respondents in that category also identified to want education, however it was observed that the majority of the respondents of younger demographics wanted education, thus was discounted and not identified as a challenge to the findings outlined in the paragraph above.

Another interesting finding is that younger generations are open to learn data literacy based on the survey and think it is a necessary knowledge, a positive sign for the future data protection. Even in the classrooms, Hoogland (2016) argued that data driven decision making can lead to increased student learning which could suggest a need for teaching data to them, too. Studies also showed that elderly people completely exclude education in general due to their abilities of adaptation (Olkinuora 2008).

Socioeconomic Groups and Education

Income

In an early article, it was proposed that the novel surveillance typically is used firstly on the less affluent (Gilman, M., 2012). People of lower-income statutes are the ones with the most to lose from having their privacy compromised (Mannan, 2020). They are the ones who have to expose more personal information in order to receive welfare while lacking knowledge on data privacy (Madden, 2020). Also, conducting drug tests, monitoring closed-circuit television, and psychometric tests are often conditions of employment for low-income workers (Byrne, 2020). Under this condition, they are often targeted by advertisers for tobacco and fast food, damaging their families' health and wellbeing for generations (Byrne, 2020).

Table 2. Privacy Strategies Among Social Media Users by Income

The percentage who responded "yes" to the question: "While using the Internet, have you ever done any of the following things?"

	All social media users	Less than $20K	$20K or more
	(a)	(b)	(c)
Used privacy settings to limit who can see what you post online	76%	65%	79%[b]
Avoided communicating online when you had sensitive information to share	60%	52%	63%[b]
Set your browser to turn off cookies or notify you before you receive a cookie	56%	47%	58%[b]

Figure 8: Privacy Strategies Among Social Media Users by Income (Madden, Gilman, Levy & Marwick, 2017)

Although Beck (2016) claims that information of low- and middle- income level countries are needed to contribute to better health service and infrastructure (Beck et al., 2016), health organisations have amongst the highest recorded quantity of data theft.

There are also arguments that internet users with lower levels of income and education are less likely to use certain privacy-enhancing tools and strategies (Madden, 2020). From research, 65% of low-income individuals say they have used privacy settings to limit who may view what they post online, this is compared to 79% of those in wealthier households (Madden, Gilman, Levy & Marwick, 2017). Majority of them also use Android phones (Mannan, 2020), and based on Aaron (2013) studies, Android phones have put less effort into data protection when compared to Apple, having a higher chance of data being intercepted by third parties.

Occupation

First, We also looked at people with technological backgrounds. When asked about their level of knowledge about data privacy on a 1 to 10 scale, people with no tech background averaged a score of 5.2 while their counterparts were 6.3. It is unquestionable that non-tech individuals should raise their knowledge level but people with technology histories ought to have a higher confidence especially when personal information is useful to a variety of stakeholders (Kalkbrenner, A.,2018) in order to increase the market power. Thus, suggesting they must work with personal information ethically and apply their knowledge in practice.

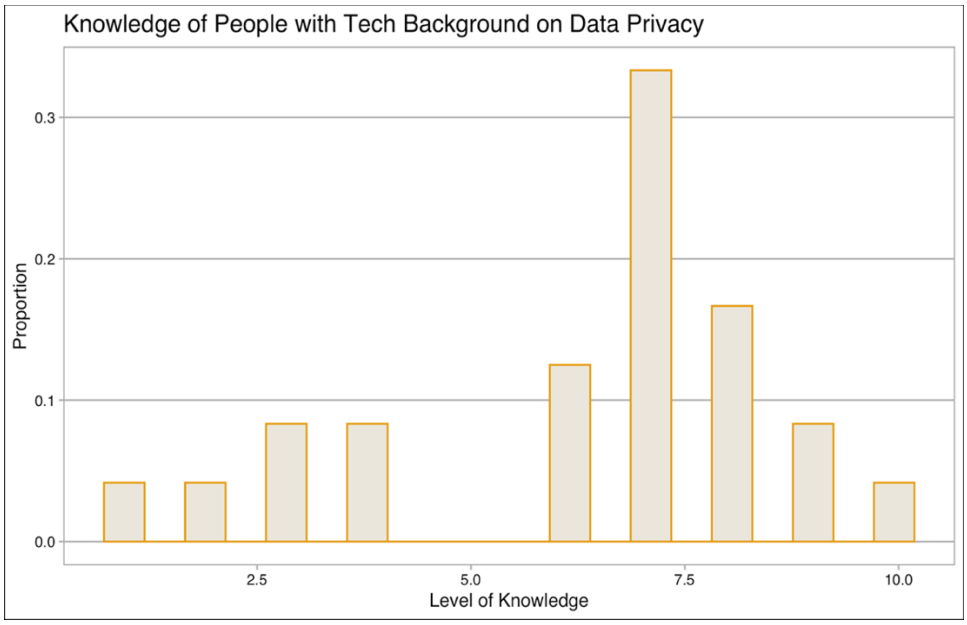


Figure 9: Knowledge of People with Tech Backgroundd on Data Privacy

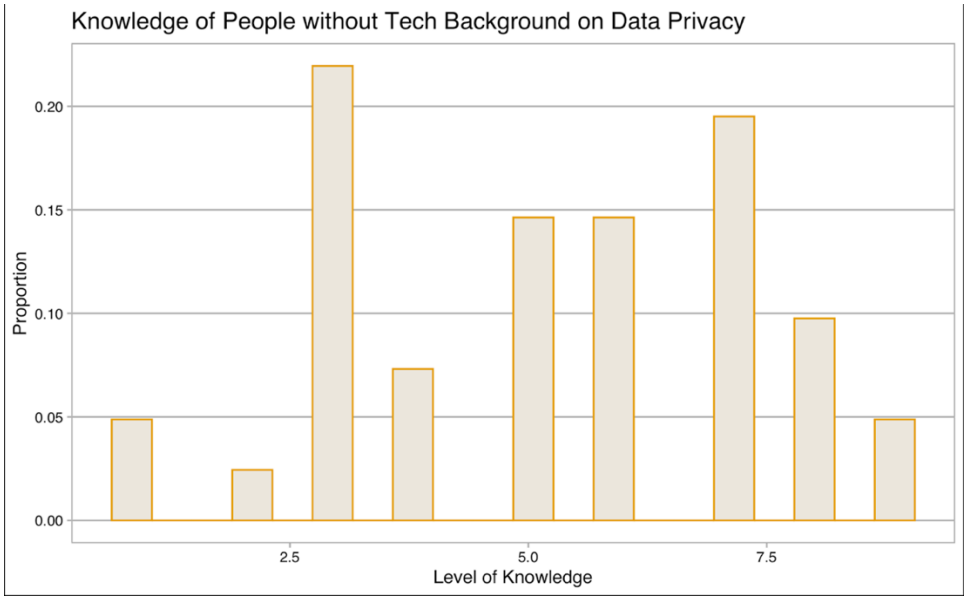


Figure 10: Knowledge of People without Tech Background on Data Privacy

An occupation we also considered were teachers, who are essential part of educating students on data privacy, but when it comes to IT being involved in teaching, they are afraid students may be distracted by work, playing games and being exposed to online harm like bullying or sexism (Bekesi, 2010). We also need to point out that training teachers on this subject would require them to go out of their comfort zone which could be something they reject to do. That could be a problem as they are pillars in the education system. Tutors who completed the survey all wanted education on data privacy, but they are also in the Gen Z generation.

Another interesting group of people who are somewhat negligent on learning data privacy are the healthcare practitioners, according to William and Hossack (2013) "commonly health practitioners are heard to say 'it will never happen to us' or 'what would anyone want with our practice data?". Knowing that health organisations have one of the highest numbers of data breaches, the attitude of healthcare practitioners need to be investigated.

Individualism, Collectivism and Education

After conducting and combining more research, we found that individualistic societies have higher incidences of data theft in comparison to collectivist societies as Sobers' data exhibited. In agreement with Han, Shavitt (1994), a clear correlation to why possible as individualistic countries have higher data breaches is due to the fundamental understanding that individualistic cultures emphasise on freedom and pleasure (Han, Shavitt, 1994).

However, Hungary is also an individualistic country which is the 17th on the list of EU countries when measuring data breaches and data stolen in 2019 (DLA Piper, 2019). The reason for the great outcome could be the fact that they constructed the Hungarian Digital Education strategy in 2016 which detailed a plan to educate people with different backgrounds on data literacy. This framework targets people who are in school as well as out of school and describe plans on teaching digital literacy in the long term. The framework goes deep into the mission and future vision of the strategy with short assessment of finance behind the work.

Unlike Hungary, Australia has one of the highest number of data breaches per capita, not just because they are an individualistic country but because of them being misinformed. According to the statistics and survey from the Office of Australian Commissioner (2017), Australians think health and finance organisations as well as government agencies are the most trustworthy entities, yet these industries have the record of most data breaches in the country (OAIC, 2019). On top of that, based on the same survey many people do not read privacy policies, shred documents or refuse to provide personal information, despite 61% of them checking website security which is a concerning pattern.This research suggests that human errors are mostly likely the cause of data breaches (OAIC, 2019) which correlates with the groups' unwillingness to learn about data privacy and the tactics needed to avoid breaches. This propounds that it has resulted in the high levels of human error uncovered in our report.

Literature review - International Case Studies and Education

As we elaborated on the question of who wants and needs training on data privacy, we also looked at how different nations implemented this subject into their educational system. One of the most interesting actions was taken by the Hungarian government who created the Hungarian Digital Education Strategy in 2016. This framework targets people who are in school as well as out of school and describe plans on teaching digital literacy in the long term. The framework goes deep into the mission and future vision of the strategy with short assessment of finance behind the work.

Investigation on teaching methods could be conducted in order to discover study outlines and deepen the understanding of data privacy education due to having different groups of individuals with different ways of comprehending data privacy. Naturally, there are some studies on data analytics in the classroom (Rodriguez-Triana, 2016), but it is important to see how teaching data privacy can be conducted. Learning can be done outside of the classroom could be an option too. The Norwegian Directorate of Education and Training (2007) published resources for teenagers to raise awareness of their personal information or Scottish Association for Mental Health released training and guides against online bullying (Scottish Association for Mental Health, 2017).

These resources are necessary but need to be complemented with more research. Although strengthening personal privacy protection awareness can help avoid data breaches from the root (Lingyu Liu,2018), there is no way for people to receive the convenience without sacrificing privacy (Zhou, 2020). Brooke (2020) claims “data-driven products and services are often marketed with the potential to save users time and money or even lead to better health and well-being”. 71% of people said that they were willing to give up privacy to get access to what technology can offer (Sherman, 2020). Therefore, it is required to understand the balance of sharing data and receiving comfort.

With these instances, it is shown that having some form of learning must be achieved, and the Australian government should implement similar efforts into data privacy programs. Although we have data strategies (Department of Industry, Innovation and Science, 2020), unfortunately it does not go into details about educational plans. Therefore, having clear visions and resources available is essential as well. The possibility of building fundamental knowledge for society is very high.

Limitation

In our report we identified several limitations that we have attempted to overcome.

Issues with sample

We identified issues with sample and selection and the existence of sample bias. The survey was largely sent to individuals we know so there is a large proportion of younger individuals in the survey as we had limited time to access the appropriate scope of participants which means the sample is not truly random. Furthermore, we believe that there

was insufficient sample size for strong statistical measurement. We received 80 participants, which allowed us to identify an adequate number of significant relationships from the data. A larger sample size would have made these relationships even clearer. Another limitation was the lack of previous research studies on the topic.

Issues during research

During the research phase it was identified that there were few or no prior research papers that drew links between demographic, socioeconomic groups, individualist/collectivist cultures and their incidence of data theft or interest in education on data privacy. In the same way the limitation of the research on the socio-economic perspective is that most data is based on America and other nations not Australia because of a lack of local research. However, there are similarities of socio-economic globally because of cultural similarities between some of the countries and Australia, we concluded that it also has high reference value in the area of Australia. Moreover, limited access to some key raw data presented us with some issues, we sought access to data from data privacy education firms, however due to their data privacy codes we were not given access. Additionally, the time constraints of this unit meant condensed research and analysis periods. A short three-week period including a plan, two presentations and a report has created a situation in which research and analysis were completed but felt rushed.

Conflicts arising from cultural bias and other personal issues

We identified a bias in our group as we all largely come from the same socioeconomic background. We had similar bias's towards how we perceived low and high socioeconomic individuals would respond to data, we attempted to overcome through an anonymous survey thereby eliminating bias.

Conclusion

We were able to analyse sufficient data that answers have been presented in response to the questions outlined in the aim. At the outset, we undertook secondary research which confirmed our assumption that education has the potential to reduce the incidence of data theft in Australia. We Identified individualist nations like Australia as those that have the highest levels of data theft, showing that there is a need for education in this country. The aim was to identify problem clusters, the investigation recognised that the highly educated, the middle aged group, teachers, health practitioners and those who have high levels of contact with data represent groups of individuals who experience high incidences of data theft and will not seek education on the topic without encouragement. Another aim was to draw conclusions as to why people may not want education on data privacy. The investigation into this was not complete, further study is required to gather sufficient data to be able to make an informed determination. As we identified Australia's need, we aimed to identify countries who had implemented data privacy education successfully. The case studies

identified Hungary, France and Norway as being implementers of data privacy education who enjoy relatively low levels of data privacy breaches when compared to other individualist nations.

Recommendation

We recommend further research to be undertaken into why some groups of individuals feel as though they do not need education on data privacy to better identify their cultural attitude towards the problem sphere. Further research should be carried out into the most appropriate forms of education for those problem clusters. It is our hypothesis that groups of individuals will respond to forms of education differently, suggesting that the most effective and efficient form of education must be identified for each group. It may then be possible to target those problem clusters and perform primary research into the effects of education on high incidence groups, confirming using our own data the validity of our assumption. Beyond this the research may be utilised to draft an Australian digital education strategy, similar to that operating in Hungary with the hope of researching those beyond the problem groups.

Appendix

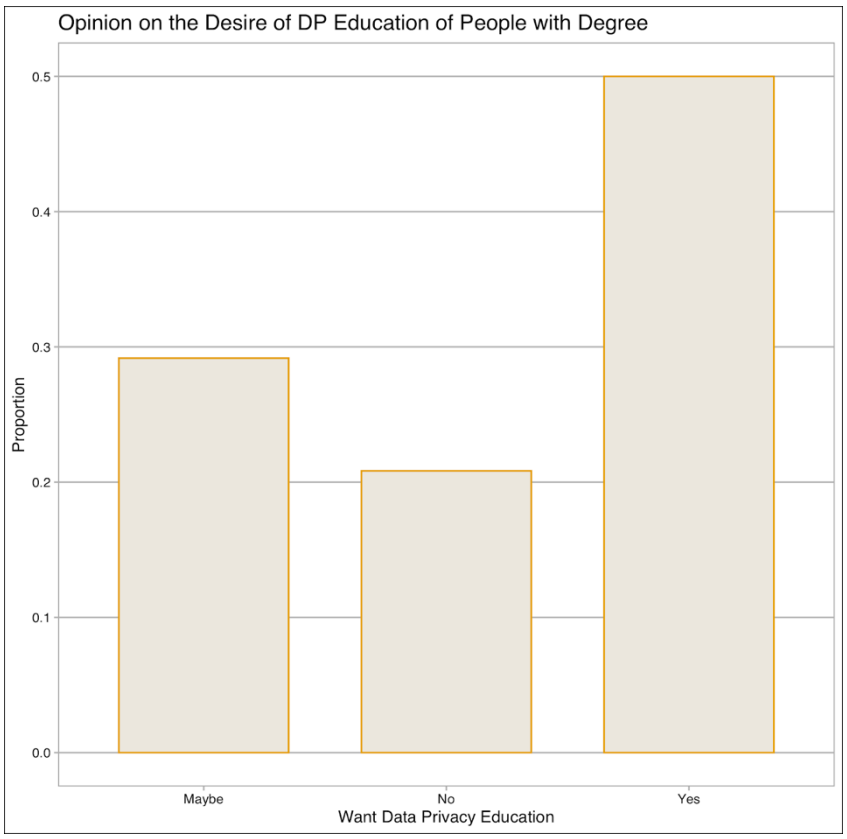


Figure 11: Opinion on the Desire of Data Privacy Education of People with Degree

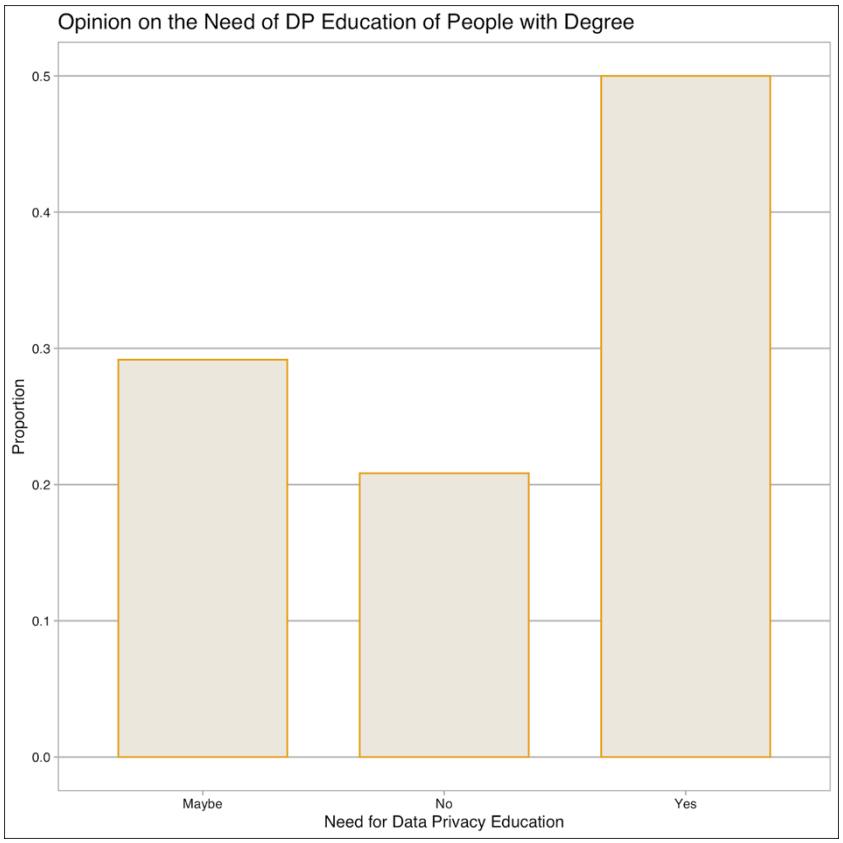


Figure 12: Opinion on the Need of Data Privacy Education of People with Degree

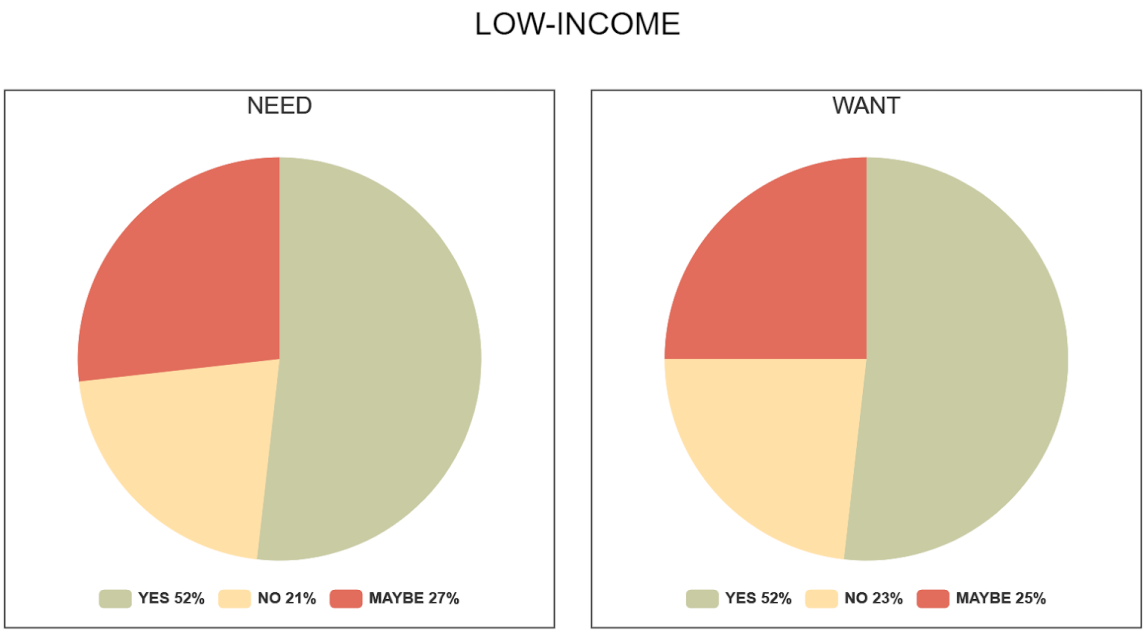


Figure 13:the Necessity and Willing for Low-income Group to Get the Education on Data Privacy

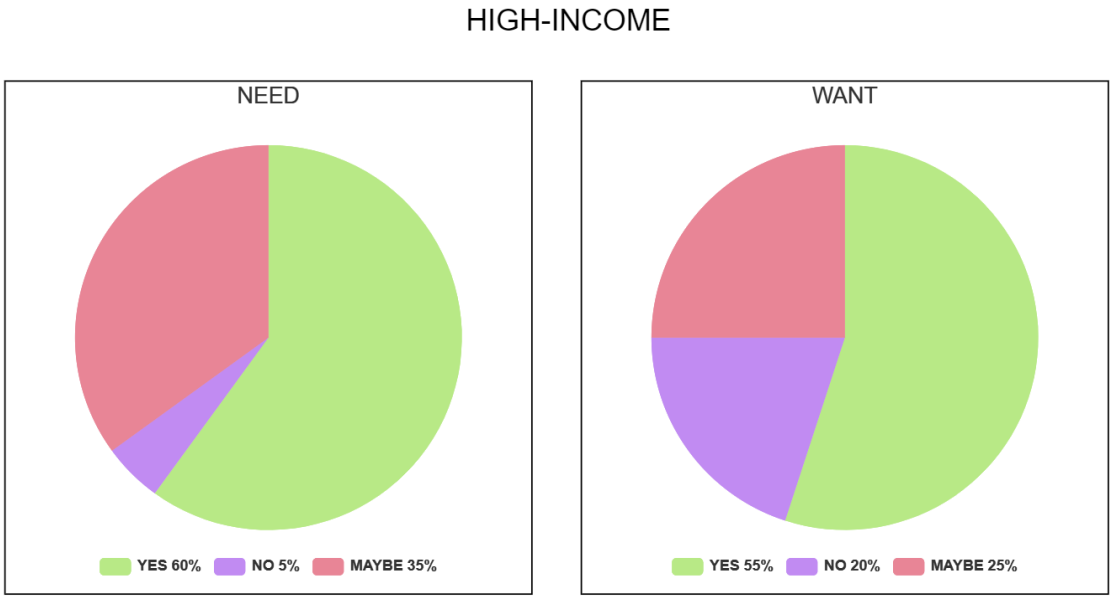


Figure 14: The Necessity and Willing for High-income Group to Get the Education on Data Privacy

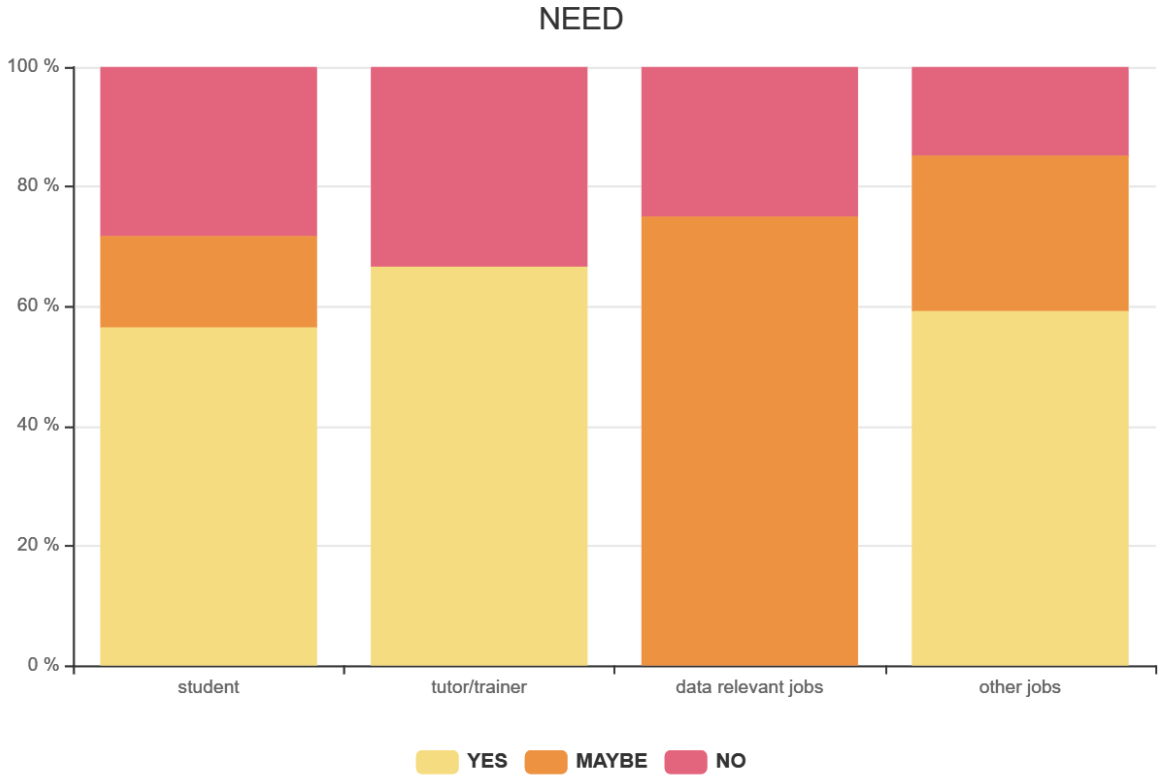


Figure 15: The Necessity of Education on Data Privacy in Different Occupations

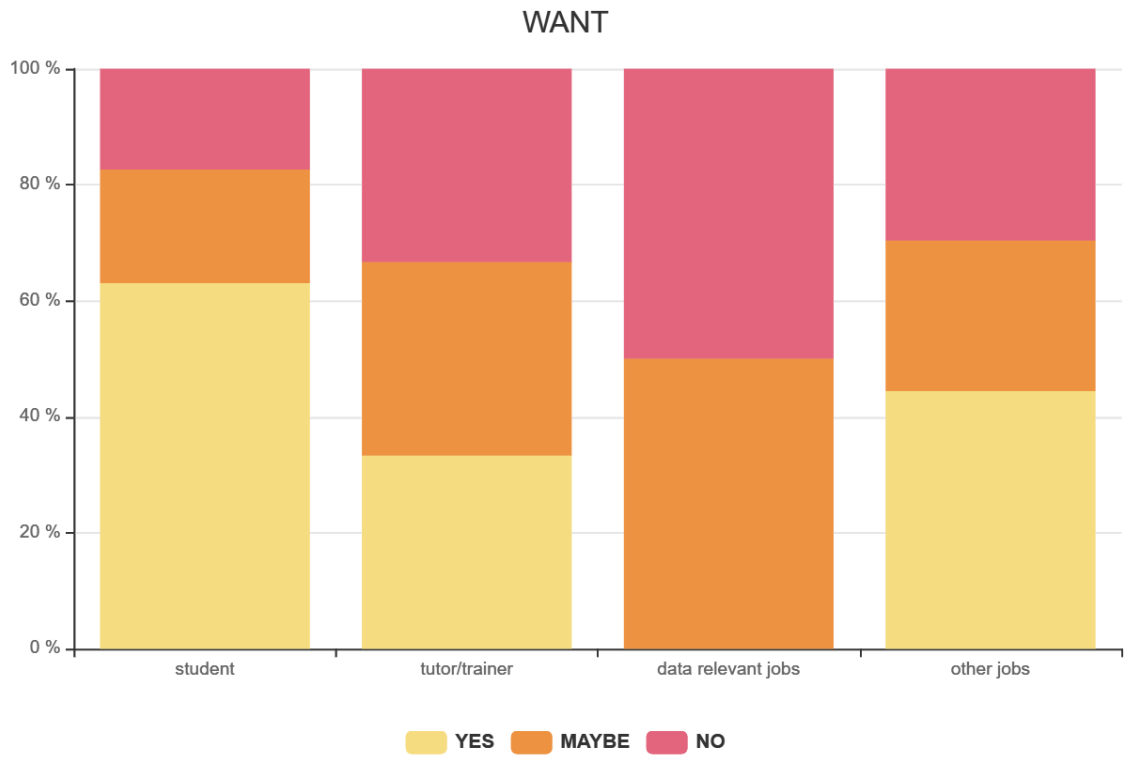


Figure 16: The Willingness to Education on Data Privacy in Different Occupations

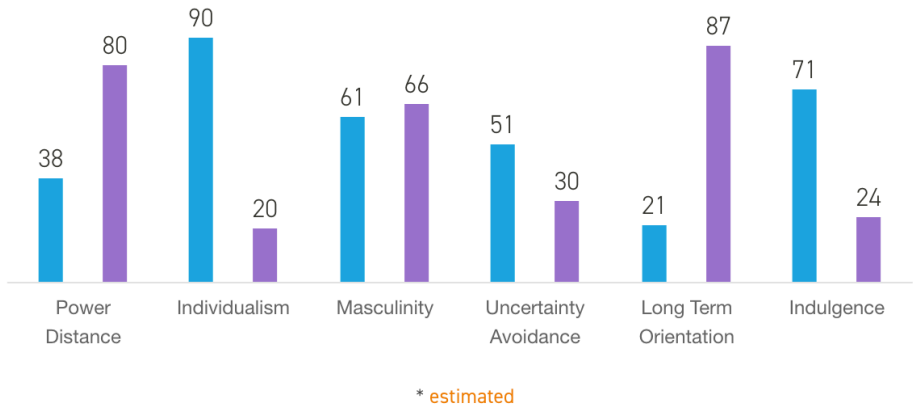


Figure 17: Australia and China Comparison (Hofstede, 2007)

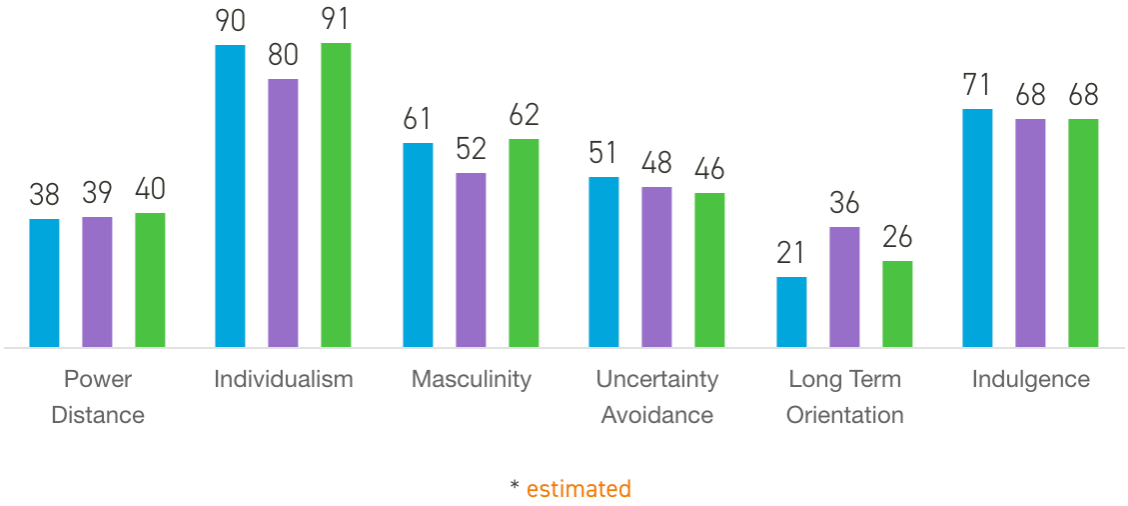


Figure 18: Australia, The US and Canada Comparison (Hofstede 2007)

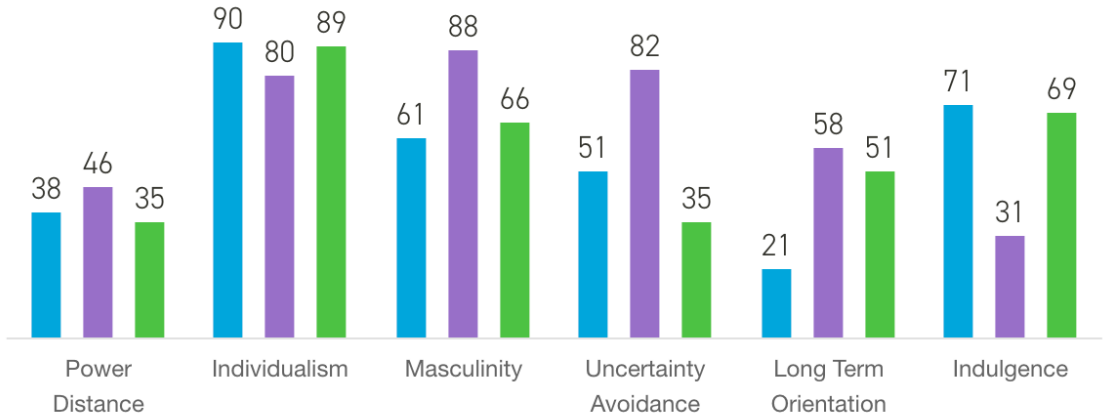


Figure 19: Australia, Hungary, UK Comparison (Hofstede 2007)

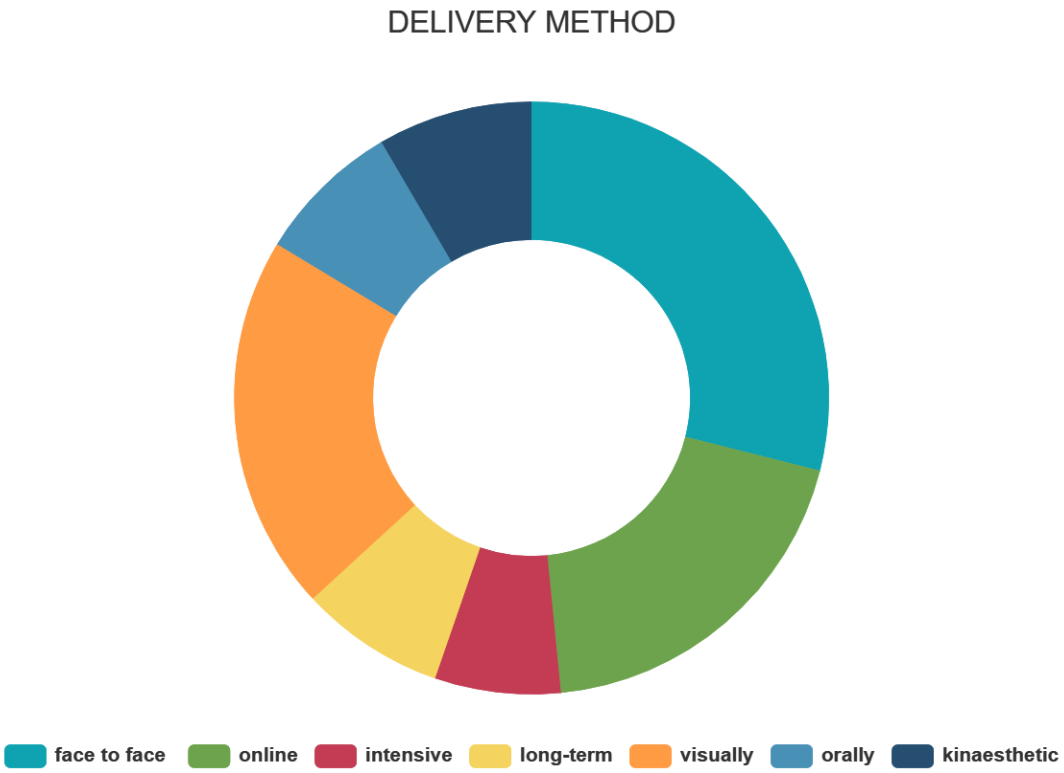


Figure 20: The Effectiveness of Different Study Methods

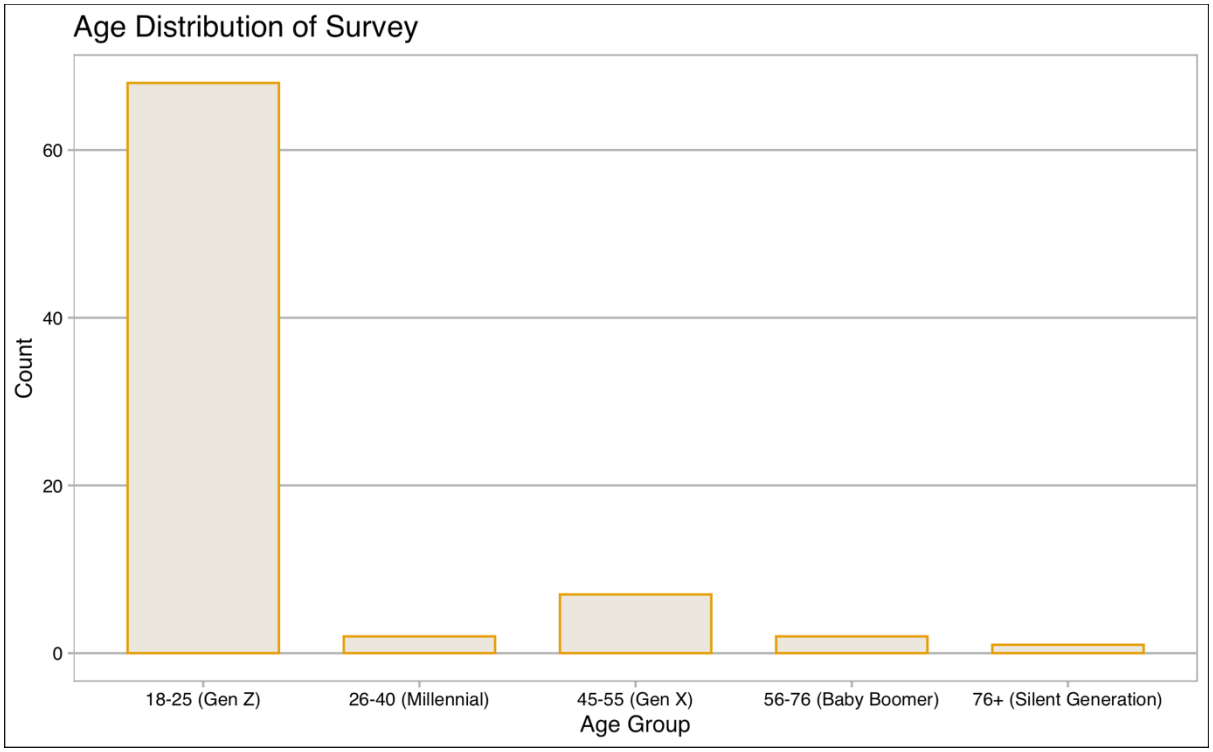


Figure 21: Age Distribution of Survey

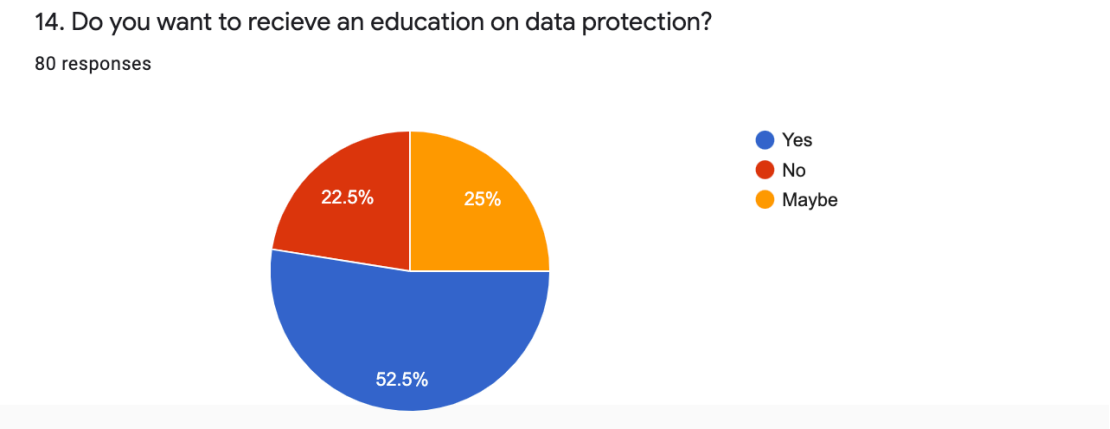


Figure 22: Wanting to Receive Education from Survey

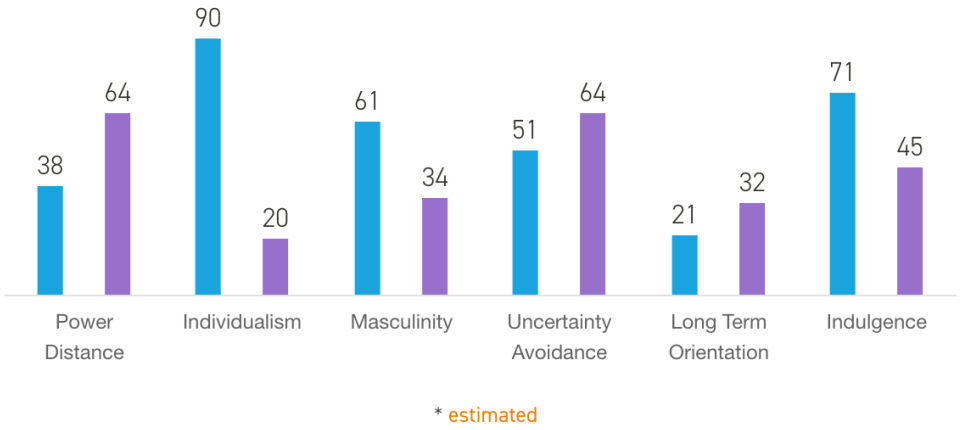


Figure 23: Australia and Thailand Comparison (Hofstede 2007)

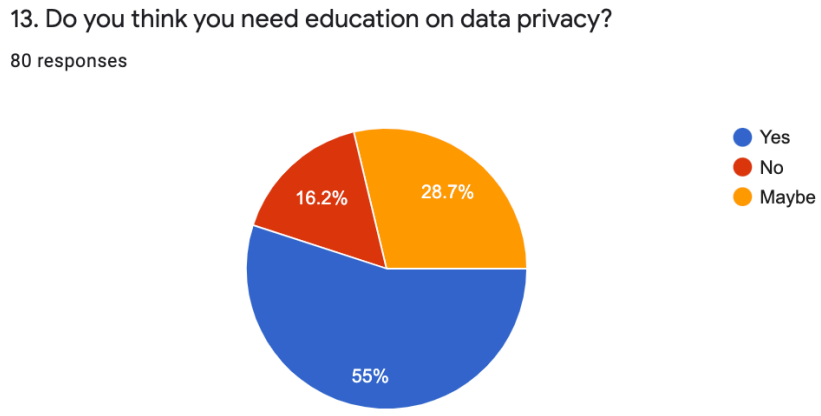
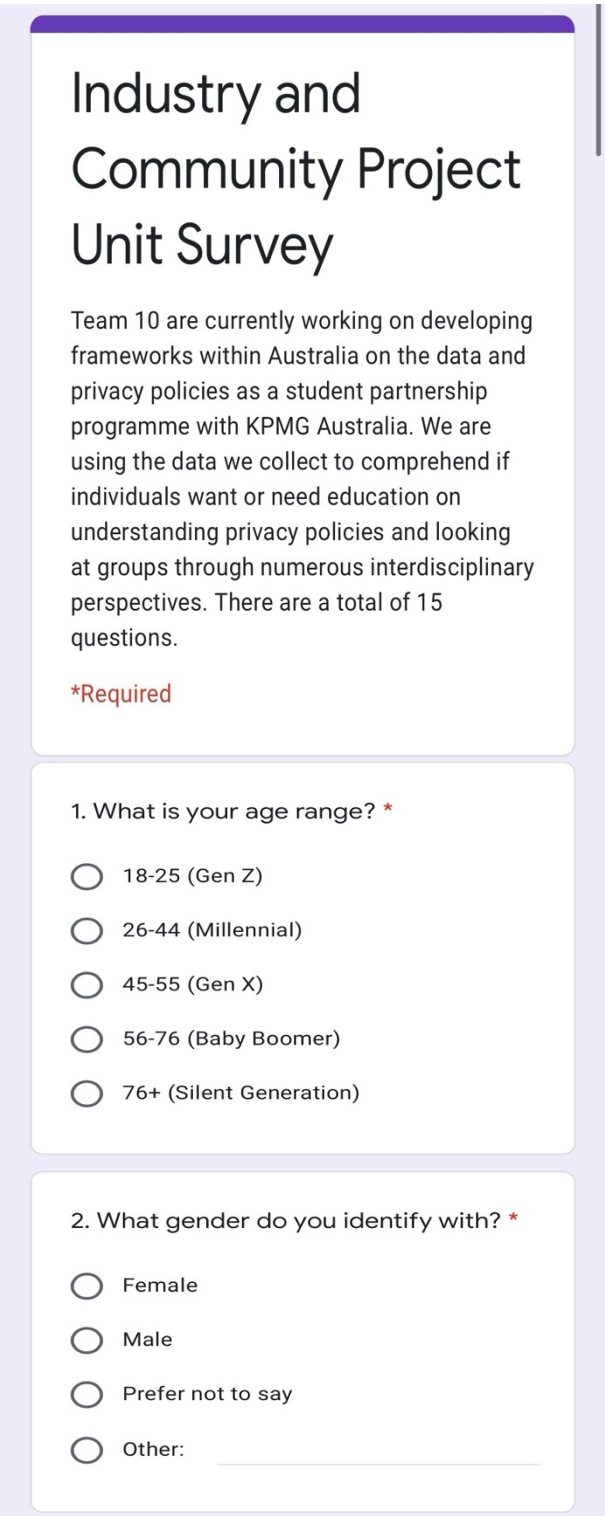


Figure 24: Opinion on the Need of Education from Survey

Survey



Industry and Community Project Unit Survey

Team 10 are currently working on developing frameworks within Australia on the data and privacy policies as a student partnership programme with KPMG Australia. We are using the data we collect to comprehend if individuals want or need education on understanding privacy policies and looking at groups through numerous interdisciplinary perspectives. There are a total of 15 questions.

*Required

1. What is your age range? *

- ◯ 18-25 (Gen Z)
- ◯ 26-44 (Millennial)
- ◯ 45-55 (Gen X)
- ◯ 56-76 (Baby Boomer)
- ◯ 76+ (Silent Generation)

2. What gender do you identify with? *

- ◯ Female
- ◯ Male
- ◯ Prefer not to say
- ◯ Other:

3. In which country did you reside for most of your life? *

Your answer

4. What is your ethnic background? *

Your answer

5. What level of education have you completed? *

- Middle School
- High School
- Undergraduate
- Masters
- PhD
- Other:

6. Do you have a technological background? *

- Yes
- No
- Maybe

7. What is your current occupation? *

Your answer

8. How much do you earn p/a? (AUD) *

- ○ $0 – $18,200
- ○ $18,201 – $37,000
- ○ $37,001 – $90,000
- ○ $90,001 – $180,000
- ○ $180,001 and over
- ○ I would rather not say
- ○ Financially dependent on family

9. Do you read what you consent to prior to registering for any platforms? *

- ○ yes
- ○ no

10. Are you aware of what happens with your personal information after you have shared them with data collectors? *

- ◯ Yes
- ◯ No
- ◯ Maybe

11. Are you willing to give up your personal data in order to receive free social media services? *

- ◯ Yes
- ◯ No
- ◯ Maybe

12. From 1 to 10, how informed are you on data privacy? 1 being not aware and 10 being fully aware *

1 2 3 4 5 6 7 8 9 10

not aware at all ◯◯◯◯◯◯◯◯◯◯ fully aware

13. Do you think you need education on data privacy? *

- ◯ Yes
- ◯ No
- ◯ Maybe

14. Do you want to recieve an education on data protection? *

- ○ Yes
- ○ No
- ○ Maybe

15. How do you learn most effectively (you can choose more than one) *

- ☐ Online
- ☐ Face to face
- ☐ Intensive
- ☐ Long-term study
- ☐ Visually
- ☐ Orally
- ☐ Kinaesthetic (Physically Performing)

References

Aaron, S. (2013). *Request for investigation and complaint for injunctive relief*. Retrieved 20 July 2020, from https://perma.cc/W9AT-YUFD

Appelgren, C. (2019). *'with great power comes great responsibility'*. Retrieved from https://www.independent.com.mt/articles/2019-04-09/blogs-opinions/With-great-power-comes-great-responsibility-6736206375

Arain, A. M., Tarraf, R., Ahmad A. (2019). *Assessing staff awareness and effectiveness of educational training on iT security and privacy in a large healthcare organization*. Journal of Multidisciplinary Healthcare 2019.12, 73–81

Beck, E., Gill, W., & De Lay, P. (2016). *Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data*. *Global Health Action*, *9*(1), 32089. https://doi.org/10.3402/gha.v9.32089

Bekesi, A., 2010. *Az IKT eszközök az oktatásban*. Retrieved from https://dea.lib.unideb.hu/dea/bitstream/handle/2437/105068/Szakdolgozat_Bekesi_Attila_titkositott.pdf;jsessionid=F51527F841CC311BC3592A2C65548A9E?sequence=1

Brooke, A., lee, r., Anderson, m., Perrin, a., Kumar, m., & Turna, e. (2020*). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Retrieved 14 July 2020, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Byrne, c. (2020). *Trading privacy for survival is another tax on the poor. Retrieved 19 July 2020, from* https://www.fastcompany.com/90317495/another-tax-on-the-poor-surrendering-privacy-for-survival

Cottrel (2016*). Champions of Children's Privacy*. Retrieved 16 July 2020 from https://americanlibrariesmagazine.org/2016/05/02/childrens-privacy-libraries/

Data Protection and Privacy Legislation Worldwide [image], 2020. Retrieved 16 July 2020 from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection- Laws.aspx

Department of Industry, Innovation and Science, 2020. *Data Strategy 2018-2020*. Canberra, Australia, Author.

DLA Piper, 2019. *DLA Piper GDPR Data Breach Survey: February 2019*. Retrieved 16 July 2020 from https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/

Edwards, K. (2015). *Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users.* Retrieved 17 July 2020 from https://core.ac.uk/download/pdf/51097987.pdf

European Commission, 2019. *General Data Protection Regulation shows result, but works need to continue.* Retrieved 18 July 2020 from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449

Fawcett, T. & Provost, F. (2013). *Data Science for Business,* from O'Reilly Media, Inc. Joshi P. (2017). *Artificial Intelligence with Python*, from Packt Publishing.

Financial Services. (2020). Retrieved 8 July 2020, from https://nationalindustryinsights.aisc.net.au/industries/financial-services

Geert Hofstede Cultural Dimensions (2007). Retrieved from **http://taylortraining.com/clients/mcc/Hofstede_Cultural_Dimension_Explained(external).pdf**

Gilman, M. (2012). *The class differential in privacy law*. *Brooklyn Law Review*, *77*(4).

Government, A. (2020). *Protecting your CDR data*. Retrieved 9 July 2020, from https://www.oaic.gov.au/consumer-data-right/protecting-your-cdr-data/

Han, S., Shavitt, S. (1994). Persuasion and Culture: *Advertising Appeals in Individualistic and Collectivist Societies*. *Journal of Experimental Social Psychology,* 30, pp. 326-350.

Health Informatics: Digital Health Service Delivery – The Future is Now! p 155. Retrieved 16 July 2020 from https://www.iospress.nl/book/health-informatics-digital-health-service-delivery-the-future-is-now/#:~:text=The%20theme%20of%20HIC%202013,the%20field%20of%20health%20informatics.&text=This%20book%20will%20be%20of,future%20provision%20of%20healthcare%20services.

Hendry, J., 2020. *Melbourne TAFE data breach exposes 55k student, staff files*. Retrieved 16 July 2020 from https://www.itnews.com.au/news/melbourne-tafe-data-breach-exposes-55k-student-staff-files-539180?eid=3&edate=20200311&utm_source=20200311_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

Heufner (2009). *Privacy Staff Training and Employee Privacy Disclosures*. Retrieved 16 July 2020 from https://search.proquest.com/openview/4a0535ec0d949f267dbd1f8d392ac01f/1?pq-origsite=gscholar&cbl=18750&diss=y

Hofstede Insights: *Country Comparison. (2020).* Retrieved 16 July 2020 from **https://www.hofstede-insights.com/country-comparison/**

Hoogland, Schildkamp, Kleij, Heitink, Kippers, Veldkamp, Dijkstra (2016). *Prerequisites for data-based decision making in the classroom: Research evidence and practical illustrations*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0742051X16301408

Hungarian Government, 2016. *Magyarország Digitális Oktatási Stratégiája*. Budapest, Hungary, Author.

Income | Department of Education, Skills and Employment. (2020). Retrieved 14 July 2020, from https://www.education.gov.au/income

Kalkbrenner, A. (2018). *Climate Change, Big Data Revolution and Data Privacy Rights*. Journal of Environmental Law and Practice, 32(1), 1–17. Retrieved 16 July 2020 from http://search.proquest.com/docview/2117080912/

Kitchin, NIRSA, Maynooth University (2016).*Getting smarter about smart cities: Improving data privacy and data security*. Retrieved 16 July from https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security

Lingyu Liu. (2018*). Research on Risk Control and Guarantee System of Personal Data Security.* Shanxi University.

Madden, M. (2020). *Privacy, Security and Digital Inequality* Retrieved 14 July 2020, from https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for poor Americans*. Retrieved 20 July 2020, from https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview

Mannan, h. (2020). *Data Privacy Is a Human Right*. Retrieved 14 July 2020, from https://modus.medium.com/data-privacy-is-a-human-right-cf36e1b45859

Norwegian Directorate of Education and Training (2007). *You Decide Campaign.* Retrieved 16 July 2020 from https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/YouDecide.pdf

Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019. (2019). Retrieved 8 July 2020, from https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/

Number of Breaches in The US by Year [images], 2019. Data retrieved 18 July from https://privacyrights.org/data-breaches

OECD. (2000). *Globalisation, Migration and Development,* retrieved 19 July 2020 from https://doi-org.ezproxy1.library.usyd.edu.au/10.1787/9789264180413-en.

Office of Australian Commissioner (2017). *Australian Community Attitudes to Privacy Survey*. Retrieved 20 July 2020 from

https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report/

Office of The Australian Commissioner, 2018. *Australian entities and the EU General Data Protection Regulation (GDPR)*. Retrieved 15 July 2020 from https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/#:~:text=Key%20messages,apply%20from%2025%20May%202018.&text=The%20GDPR%20and%20the%20Australian,by%20design%20approach%20to%20compliance

Olkinuora, Rinne, Makinen, Jarvinen, Jauhiainen (2008). *Promises and risks of the learning society: the meanings of lifelong learning for three Finnish generations*. Studies in the Education of Adults, 40:1, 40-61, DOI: 10.1080/02660830.2008.11661555

Privacy Rights Clearinghouse, 2019. *Data Breaches*. Retrieved 19 July 2020 from https://privacyrights.org/data-breaches

Reidenberg, J., & Schaub, F. (2018). Achieving big data privacy in education. *Theory And Research In Education*, *16*(3), 263-279. doi: 10.1177/1477878518805308

Rodriguez-Triana, Martinez-Mones, Villagra-Sobrino (2016). *Learning Analytics in Small-Scale Teacher-Led Innovations Ethical and Data Privacy Issues.* Retrieved 20 July 2020 from https://epress.lib.uts.edu.au/journals/index.php/JLA/article/view/4581

Stahl, M. (2016). Erhaltungstherapie bei metastasiertem Pankreaskarzinom. *Karger Kompass Onkologie*, *3*(2), 80-81. doi: 10.1159/000449191

Sherman, e. (2020). Yahoo is now a part of Verizon Media. Retrieved 14 July 2020, fromhttps://finance.yahoo.com/news/people-concerned-privacy-theory-not-143308057.html

Singh, V. (2014). “We are not phobic but selective”: the older generation’s attitude towards using technology in workplace communications. *Development And Learning In Organizations: An International Journal*, *28*(4), 18-20. doi: 10.1108/dlo-10-2013-0082

Sobers, R. (2020). The World in Data Breaches. Retrieved 9 July 2020, from https://www.varonis.com/blog/the-world-in-data-breaches/

Soltész., B., 2017. *Az internet veszélyai a fiatalkorúakra*. Retrieved 20 July 2020 from http://midra.uni-miskolc.hu/document/25672/20958.pdf

The Right to Privacy in Thailand. (2015). Retrieved 20 July 2020 from https://privacyinternational.org/sites/default/files/2017-12/privacy_thailand.pdf

Tomasovszky, E., 2014. *Az információs és kommunikácós technikák alkalmazása az általános iskolai oktatásban*. Retrieved 21 July 2020 from http://www.tomacolor.hu/szakdolgozat.pdf

United Nations Conference on Trade and Development, 2020. *Data Protection and Privacy Legislation Worldwide*. Retrieved 20 July 2020 from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Welcome to the Labour Market Information Portal. (2020). Retrieved 7 July 2020, from https://lmip.gov.au/default.aspx?LMIP/GainInsights/IndustryInformation/HealthCareandSocialAssistance#:~:text=Over%20the%20past%20five%20years,are%20around%20%241%2C000%20per%20week.

Williams, P., & Hossack, E. (2020). It will never happen to us: The likelihood and impact of privacy breaches on health data in Australia. Retrieved 16 July 2020, from https://ro.ecu.edu.au/ecuworks2013/313/

Yao-Huai (2005). *Privacy and data privacy issues in contemporary China*. Retrieved 15 July 2020 from https://link.springer.com/article/10.1007/s10676-005-0456-y

Zhou, C. (2020). Why do Chinese people seem to be more willing to give up privacy for security than Australians? Retrieved 14 July 2020, from https://www.abc.net.au/chinese/2018-04-14/china-privacy/9645522

SID: 480133780, 490189739, 480555409, 470527823