Technische Universität Berlin

Faculty IV: Electrical Engineering and Computer Science

Quality and Usability Lab

M.Sc. Computer Science (Informatik)

SoSe 2024

The effect of online privacy literacy on online privacy valuation and online privacy protection behaviour among Pakistanis

Master thesis for M.Sc. Computer Science (Informatik) at the Technische Universität Berlin, Faculty IV - Electrical Engineering and Computer Science

Date of Submission: 13-09-2024

First Supervisor: Prof. Marian Margraf

Second Supervisor: Prof. Sebastian Möller

Written by: Suleman Samuel Gill

Matriculation number: 390129

Address: Danckelmann Strasse 46, 14059 Berlin, Germany

Email: suleman.s.gill@campus.tu-berlin.de

Affidavit

I hereby declare that the thesis submitted is my own, unaided work, completed without any unpermitted external help. Only the sources and resources listed were used.

Berlin, 13-09-2024

……

Zusammenfassung

Das Verständnis des Verhaltens der Menschen in Bezug auf die Privatsphäre und die Bewertung der Privatsphäre ist komplex. In der Literatur gibt es einen Widerspruch zwischen dem tatsächlichen Verhalten der Menschen und ihren angegebenen Präferenzen, das so genannte Datenschutzparadoxon. Die Menschen unterscheiden sich auch in ihrer Bewertung von Daten. Sie führen eine Risiko-Nutzen-Kalkulation durch, wenn sie Informationen mit anderen teilen. Das mangelnde Wissen der Menschen über den Datenschutz beeinflusst ihr mentales Risiko-Nutzen-Modell. In dieser Arbeit wurden anhand einer Online-Umfrage die Auswirkungen von Online-Datenschutzkenntnissen auf den Wert, welcher 5 verschiedenen Datentypen beigemessen wird, sowie auf das Online-Datenschutzverhalten untersucht. Es konnte ein Zusammenhang zwischen den Online-Datenschutzkenntnissen und dem Wert festgestellt werden, welcher den, hier als „personal data“ bezeichneten, Daten beigemessen wird. Diese Daten beinhalten Daten, welche die betroffene Person direkt beschreiben, wie beispielsweise ihren Namen, ihr Alter, ihr Geburtsdatum und ähnliche Informationen. Mit steigenden Online-Datenschutzkenntnissen steigt hierbei auch die Bereitschaft, für die Löschung dieser Daten von Online-Plattformen zu zahlen. Es konnte jedoch keine signifikante Korrelation zwischen Online-Datenschutzkenntnissen und Online-Datenschutzverhalten festgestellt werden. Auch zwischen den Bedenken bezüglich des Online-Datenschutzes und dem Online-Datenschutzverhalten wurde kein Zusammenhang festgestellt.

Abstract

Understanding people's privacy behaviour and privacy valuation is complex. A contradiction between the actual behaviour of the people and their stated preferences is found in the literature, and it is called the privacy paradox. People also differ in their data valuation. They do a risk-benefit calculation in their minds while exchanging information with others. People's lack of knowledge about privacy has an effect on their mental risk-benefit model. In this thesis, we examined the effect of online privacy knowledge on online privacy valuation of 5 different data types and online privacy protection behaviour among Pakistanis through an online survey. We observed that people's valuation for the data type we call "personal data", which includes data directly describing the person such as name, age, date of birth, and others, is related to their online privacy knowledge. With increasing online privacy knowledge, people are willing to pay a higher amount for the deletion of "personal data" type from online platforms. However, no significant correlation between online privacy knowledge and online privacy protection behaviour was found. There was no correlation between online privacy concerns and online privacy behaviour either.

Table of Contents

List of Figures

1 Introduction

Understanding people's privacy behaviour and privacy valuation is complex. Past studies have shown that people actually reveal more information about themselves than they say they would (Spiekermann et al., 2001). People also reveal sensitive information about themselves in exchange for small benefits, in contradiction to their stated privacy preferences (Beresford et al., 2010), leading to a privacy paradox (Norberg et al., 2007). A study done across different countries, platforms and data types shows that people in different countries vary in their data valuation (For our thesis, privacy valuation and data valuation refer to the same concept). Germans place the highest value on personal data followed by US Americans and then Latin American people. It also shows that people value different types of personal data differently, valuing financial data the highest and location data the least on average (Prince & Wallsten, 2022). It is also known that people perform some kind of risk-benefit calculation while exchanging their personal information online (Barth & de Jong, 2017). Knowledge deficiency regarding how their personal data is collected, processed, stored and shared with third parties has an impact on people's mental risk-benefit calculation (Barth & de Jong, 2017). Studies that have examined the effect of privacy knowledge on privacy protection behaviour have shown varying results (for our thesis, privacy literacy and privacy knowledge refer to the same concept). A paper published in 2013 showed that among 419 American adults, internet users with more privacy knowledge are more likely to exhibit privacy protection behaviour (Park, 2013). However, a study done on 169 students in Israel found no association between online privacy knowledge and privacy protection behaviour (Weinberger et al., 2017). Moreover, a study done in the UK in 2015 showed that, among the UK's young population (18 to 25 years old), more knowledge about online privacy regulation leads to less online privacy protection behaviour (Miltgen & Smith, 2015). A meta-analysis published in 2017 which analyzed 166

studies from 34 countries found that users who are more literate about their privacy were more likely to use privacy protective measures (Baruh et al., 2017). So, online privacy literacy is an important factor influencing online privacy protection behaviour. However, the effect of privacy literacy on privacy valuation has never been explored in the literature to the best of my knowledge and the effect of online privacy literacy on privacy protection behaviour has never been studied among people living in Pakistan. My master's thesis aims to fill this gap in literature. Privacy concern is a related construct that has been studied in relation to privacy protection behaviour. For example, the same meta-analysis published in 2017, which analyzed 166 studies from 34 countries and found that users who are more literate about their privacy were more likely to use privacy protective measures, also found that users who are more concerned about their privacy were more likely to use privacy protective measures (Baruh et al., 2017). This thesis will also look at the effect of online privacy concerns on online privacy protection behaviour among Pakistanis.

1.1 Thesis Objectives

Based on the literature gap that we have identified, this thesis will answer three research questions and test the hypothesis for each research question. The research questions and their corresponding hypotheses are as follows:

Research question 1: What is the effect of online privacy literacy on privacy valuation among Pakistanis residing in Pakistan?

There is no study which focuses specifically on the effect of online privacy knowledge on online privacy valuation to the best of our knowledge to the best of our knowledge. Therefore, we make a null hypothesis about the relationship between online privacy knowledge and online privacy behaviour among Pakistanis. So, corresponding to our first

research question, we hypothesize that online privacy knowledge has no effect on online privacy valuation among Pakistanis residing in Pakistan.

Hypothesis 1: Among Pakistanis residing in Pakistan, online privacy knowledge does not affect online privacy valuation.

Research question 2: What is the effect of online privacy literacy on online privacy protection behaviour among Pakistanis residing in Pakistan?

Some studies that have examined the effect of literacy on privacy protection behavior have shown varying results. A paper published in 2013 showed that among 419 American adults, internet users with more privacy knowledge are more likely to exhibit privacy protection behavior (Park, 2013). However, a study done on 169 students in Israel found no association between online privacy knowledge and privacy protection behaviour (Weinberger et al., 2017). Moreover, a study done in the UK in 2015 showed that, among UK's young population (18 to 25 year old), more knowledge about online privacy regulation leads to less online privacy protection behavior (Miltgen & Smith, 2015). A meta-analysis published in 2017 which analyzed 166 studies from 34 countries found that users who are more literate about their privacy were more likely to use privacy protective measures. (Baruh et al., 2017). Due to the varying results, we hypothesize that there is no association between online privacy knowledge and online privacy protection behaviour among Pakistanis residing in Pakistan, which corresponds to our second research question.

Hypothesis 2: Among Pakistanis residing in Pakistan, online privacy knowledge does not affect online privacy behaviour.

Research question 3: How does online privacy concern affect online privacy protection behaviour among Pakistanis residing in Pakistan?

A meta-analysis published in 2017 which analyzed 166 studies from 34 countries found that users who are more concerned about their privacy were more likely to use privacy protective measures (Baruh et al., 2017). Therefore, corresponding to our third research question, we hypothesize that online privacy protection behaviour will increase with increasing online privacy concerns among Pakistanis residing in Pakistan.

Hypothesis 3: Among Pakistanis residing in Pakistan, online privacy protection behavior increases with increasing online privacy concerns.

Next, we will explore past literature on privacy paradox and privacy valuation to better understand people's behaviour towards privacy and how privacy valuation is done in different ways.

2 Related literature

In this section, we will explore past literature related to our thesis. First, we will describe a phenomenon called privacy paradox in detail. Then, we will look at some of the past literature on privacy valuation.

2.1 Privacy paradox

Privacy paradox is the phenomenon where people say that they value privacy highly, yet in their behaviour, relinquish their personal data for very little in exchange or fail to use measures to protect their privacy (Beresford et al., 2010; Norberg et al., 2007; Spiekermann et al., 2001). There are different approaches to explaining the privacy paradox. We will discuss some of the approaches.

2.1.1 Rational risk-benefit calculation

Many theories explain the privacy paradox in different ways. We will see some of them. According to the Rational Choice Theory of Human Behavior, decisions are always reasonable and logical in order to gain the greatest benefit or satisfaction in line with an individual's perceived self-interest (Herbert, 1955, as cited in Barth & de Jong, 2017b). The Adaptive Cognition Theory of Social Network Participation says that user participation in online social networks can be assigned to three phases: initial use, exploratory use, and managed use. The progression from one phase to the next results from understanding the benefits and risks associated and the adaptation of activities and controls. The final phase is an equilibrium of benefits and risk awareness formed by a continuous process of risk-benefit calculation (Hu & Ma, 2010, as cited in Barth & de Jong, 2017b). The privacy calculus theory states that the perceived benefits outweigh the perceived risks, which eventually leads to the neglecting of privacy concerns that often result in the disclosure of information in exchange for social or economic benefits (Culnan & Armstrong, 1999, as cited in Barth & de Jong, 2017b). In Resource Exchange Theory, people are willing to provide personal information in exchange for other resources such as money, services, time, status and love (Donnenwerth & Foa, 1974; Foa, 1971, as cited in Barth & de Jong, 2017b). Finally, when an individual consciously ignores certain information, especially where the informative effort (cost) is considered disproportionate to the perceived potential benefits, it is called Rational Ignorance Theory (Downs, 1957, as cited in Barth & de Jong, 2017b).

2.1.2 Biased risk-benefit calculation

Contrary to a risk-benefit calculation guided by rationality, decision-making can also be influenced by different kinds of biases such as time constraints, immediate gratification, habit, etc (Barth & de Jong, 2017). Some of the biases are described below:

2.1.2.1 Heuristics

According to the Theory of Bounded Rationality, Individuals constantly try to rationally maximise benefits, but decision-making can only be rational within the limits of cognitive ability and available time (Simon, 1997, as cited in Barth & de Jong, 2017b). Then, the Filtered-Out Theory implies that individuals disclose more personal data in computer-mediated communication settings compared to face-to-face settings due to the absence of social and contextual cues leading to the disclosure of information online despite having privacy concerns (Sproull et al., 1991; Sproull & Kiesler, 1986 as cited in Barth & de Jong, 2017b). Another theory, known as the Feeling-as-Information Theory, states that individuals rely upon their feelings when making decisions about information disclosure, which are not always accurate. For example, being in a good mood lets people evaluate targets or situations as more positive than they may be (Schwarz, 2012 as cited in Barth & de Jong, 2017b).

2.1.2.2 Underestimation and overestimation of risks and benefits

According to the Optimistic Bias Theory, people tend to underestimate their own risk of privacy invasion while overestimating the chances that others experience the same. This leads them to believe that their own privacy is not at risk, which can result in increased risk exposure and a laxer precautionary stance (Irwin, 1953, as cited in Barth & de Jong, 2017b).

2.1.2.3 Immediate gratifications

In some cases, individuals encounter self-control problems as immediate gratification prompts atypical behaviour, which may be negative over the long term (Loewenstein, 1999; O'Donoghue & Rabin, 2001, as cited in Barth & de Jong, 2017b).

2.1.2.4 Habit

Habit hinders the use of privacy tools online, which eventually leads to a disconnect between privacy concerns and behaviours (Quinn, 2016 as cited in Barth & de Jong, 2017b).

2.1.3 Little to no risk assessment

There are situations in which a person is just focused on reaching a goal and the benefits a person will get, regardless of any other consideration. In these cases, no risk-benefit assessment takes place in the person's mind. We will look at some of these situations (Barth & de Jong, 2017).

2.1.3.1 The value of the outcome overshadows the risk assessment

In social networks, people share private information because doing so is a must for becoming a part of a group, despite being aware of the potential dangers of sharing private information (Lutz & Strathoff, 2014; Tönnies, 2012, as cited in Barth & de Jong, 2017b). In such situations, the desire to belong to a social network overrides the fear of potential data misuse (Lutz & Strathoff, 2014; Tönnies, 2012, as cited in Barth & de Jong, 2017b).

2.1.3.2 The lack of knowledge

People cannot evaluate risks or act optimally in a situation due to this lack of knowledge about the importance of their personal data and the potential danger of disclosing it, which leads to inaccurate estimation of potential dangers (Acquisti & Grossklags, 2005; Harsanyi, 1967, as cited in Barth & de Jong, 2017b).

2.2 Privacy paradox challenged

Usually, people side with one of the two arguments when it comes to privacy paradox (Solove, 2020). On one side is the so-called behaviour valuation argument, which says that behaviour is the best metric to evaluate how people actually value privacy (Samuelson, 1938; Solove, 2020). People on the behaviour valuation argument side call for less privacy regulation because people's behaviour reveals that people give a low value to privacy and easily give it away in exchange for some benefits (Solove, 2020). On the other side is the so-

called behaviour distortion argument, which states that people's behaviour is not an accurate metric of preferences because behaviour is distorted by biases and heuristics, manipulation and skewing, and other factors (Solove, 2020). In contrast to both of these sides, Professor Daniel Solove says that the privacy paradox does not exist and is the result of a misinterpretation (Solove, 2020). He argues that the behaviour involved in privacy paradox studies involves people making decisions about risk in specific contexts, whereas people's privacy concerns or privacy valuations are more general (Solove, 2020). So, it is illogical to generalise from people's decisions in specific situations about how people value their privacy broadly (Solove, 2020). Furthermore, he says that people fail to make rational risk-benefit assessments about their privacy because it is a complex process and almost impossible to do optimally (Solove, 2020). The behaviour in the privacy paradox studies does not lead to a conclusion for less regulation (Solove, 2020). On the other hand, minimising behavioural distortion will not cure people's failure to protect their own privacy (Solove, 2020). So, regulations should focus on the way information is processed, stored, and transferred rather than giving more control to the people (Solove, 2020).

2.3 Privacy Valuation

There are two possible approaches to performing online privacy valuation: Market valuations of data or individual perceptions of the value of data. (OECD, 2013). There is no single perfect measure of data valuation (OECD, 2013). All the methods mentioned before have some advantages and disadvantages (OECD, 2013). We will explore both approaches.

2.3.1 Market-based data valuation

Market-based data valuation refers to the values of data records that can be assessed from the markets. This includes measures such as market capitalisation/revenues/net income per data

record, market price of data, cost of data breach and data prices in illegal markets (OECD, 2013). All the information given in the market-based data valuation is taken from the OECD (2013) paper.

2.3.1.1 Financial result per data record

According to OECD (2013), Financial result (market capitalisation, revenue, profits etc) per data record is calculated by dividing the company's market capitalisation, revenue, or profit by the total number of data records used by the company. This method only works for companies that either draw most or all of their revenue from data or firms that separate their earnings from data and other sources. Market capitalisation per data record is not a good measure of data valuation because the market capitalisation of a company might fluctuate with the confidence of the people in the company, which might not be related to the value of the data. Profits per data record is not a good measure of data valuation because profits are calculated after deducting the costs, which may change and may not be tied to the data. Revenues per data record is considered a more robust measure of data valuation than market capitalisation and profits since it shows the average revenue brought in by each data record, and it is less prone to market shocks. Financial result per data record is relatively easy to identify, and it reflects the actual economic value generated through data. However, this can be inaccurate since there are many other factors influencing revenues or net income. Furthermore, it is difficult to determine exactly which portion of revenue or net income is directly tied to the data. For example, as cited in OECD (2013), a data broker called Experian had a market capitalisation of around 19 USD per record in 2011, compared to Facebook's market capitalisation of about 60 USD per record in 2011, which gets most of its income through targeted advertising based on data. In the OECD (2013), it is shown that not only did the market capitalisation of both Experian and Facebook change significantly over time, but it also follows the US Dow Jones Industrial average from 2007 to 2011, which proves that

market capitalisation is volatile and is subject to market shocks and sentiment. Revenues per data record is a better gauge for the data valuation because it is directly linked to the money others pay you to access the data. In addition, revenues per data record are shown to be more stable and less prone to market conditions over time (OECD, 2013).

2.3.1.2 The market price of data

According to OECD (2013), the market price of data is the price offered by data brokers per data entry. Companies known as data brokers engage in data selling. While it is relatively easy to find out the value of data since the prices are available from the data brokers, and it does reflect the actual market value of a specific data because the data is sold in a competitive market, It neglects the context in which data is sold which has a significant influence on the demand and the price of data. A phone number alone may have a lower value than a phone number in combination with the income level or set of particular interests. Furthermore, the quality of data sold by data brokers cannot be verified beforehand. The cost of this risk likely also distorts the true value of the data being sold. In addition, the market price also includes the costs incurred by the data broker, such as the search and labour costs. Some estimates of the prices of data will be described next. As cited in OECD (2013), in the US, an address entry was being sold for 0.50 USD, data of birth for 2 USD, a social security number for 8 USD, a driver's license number for 3 USD, and a military record was being sold for 35 USD in the market in 2011. A combination of date of birth, address, social security number, credit and military record was being sold for 55 USD (OECD, 2013).

2.3.1.3 Cost of data breach

OECD (2013) describes the cost of a data breach as the economic cost of a data breach, both for firms and individuals, per data entry. While it reflects the real market value of the data by

estimating the cost of damages caused by the data breach, it does not account for the cost of reputational damage done to the firm as a result of the data breach (OECD, 2013).

2.3.1.4 Data price in the illegal market

According to OECD (2013), the data price in the illegal market is the estimation of data prices, per data entry, in the illegal markets. These markets exist as online forums and exchange information about malware, cyber-attacks, and people's personal information, as observed by security firms such as Panda Security. From these illegal markets, the valuation of personal data can be estimated. For example, as cited in OECD (2013), the price of credit card information ranged from 1 USD to 30 USD depending on factors such as the frequency of e-commerce and e-banking, and the demographics of a data subject. While this approach does show the market value of a specific piece of data, it is difficult to measure, and it is likely to underestimate the value of the data since the criminals have to balance the risk of being detected and caught by authorities (OECD, 2013).

2.3.2 Individual's perceptions of the value of data

According to OECD (2013), measures based on an individual's valuation of data include surveys and economic experiments. Surveys and economic experiments are forms of the valuation of data based on the individual's perspective, where individuals report the valuation of their data themselves. They capture the pure economic value of data for an individual, and the results can be used to make comparisons across different countries and data types, as is done in the literature, for example, by Prince & Wallsten (2022). However, the value of data here is hypothetical and context-dependent, as people can assign different values to their data in different contexts, as discussed in the literature, for example, by Solove (2020). When performing economic experiments and doing surveys, two measures are usually used in the literature to assess the individual's valuation of data: their Willingness To Pay (WTP) and

their Willingness TO Accept (WTA); for example, the WTA and the WTP are assessed by (Winegar & Sunstein, 2019). Next, we will look at some of the studies done to assess the WTA and WTP of people for different types of data.

2.3.2.1 Defining the WTP and the WTA

The WTP and the WTA are defined differently by different studies as they see fit for their purpose, like Schmitt et al. (2021) describes the WTP as the amount people are willing to pay for the protection of data from getting disclosed, while Winegar & Sunstein (2019) describes the WTP as the amount people are willing to pay for the deletion of their data which is stored by companies. Furthermore, some studies refer to the WTP and WTA amounts as monthly recurring amounts, like the study by Winegar & Sunstein (2019), others refer to the WTP and WTA amounts as one-time, non-recurring payments, as in the study by Bauer et al. (2012) and Tang & Wang (2021). Some studies, like Tang & Wang (2021), use additional words like maximum and minimum when describing the WTP and the WTA amounts. All these differences in the WTA and WTP descriptions are important since the WTA and the WTP amounts are subject to framing and contextual effects (Acquisti et al., 2013). Despite these differences, the common thing is that the WTP is the amount that a person pays to prevent others from accessing their data and the WTA is the amount that a person receives to allow access to their data (Acquisti et al., 2013; Bauer et al., 2012; Schmitt et al., 2021; Tang & Wang, 2021; Winegar & Sunstein, 2019).

2.3.2.2 Some previous literature on the WTP and the WTA

Here we will look at some of the studies done to assess the WTA and the WTP of people for different types of data. This is not an exhaustive list of studies involving the WTA and WTP.

A paper published in 2019, which surveyed 2416 Americans, found that, on average, they were willing to pay 5 USD per month for maintaining their data privacy but would demand

80 USD per month to allow access to their personal data. This study also showed that Americans value their health data more than the demographic data (Winegar & Sunstein, 2019)

A paper published in 2018 that asked 500 Koreans about compensation in the event of information leakage found that consumers value information based on the severity of damage it can cause if leaked. So, they value basic personal information such as age, gender, telephone number, social security number and financial information such as purchase list and payment details more than their browsing history or social media posts. It also shows that consumers tend to value location information more than other types of personal information. Furthermore, consumers assess the cost and benefit of privacy protection differently based on their past experiences and personal preferences, with consumers who place importance on privacy and who have experienced an information leak before valuing their medical information significantly higher (Lim et al., 2018).

A paper published in 2021, which investigated 710 Chinese WeChat app users about their privacy valuation, showed that Chinese people value their financial information (payment and bank card details) the most and their social media posts (WeChat moment posts) the least. The value of location information was less than financial information but more than social media posts. Furthermore, more people were willing to accept money in exchange for their information than those who were willing to pay money to protect their information (Tang & Wang, 2021).

In a paper published in 2021, Jeffrey Prince and Scott Wallsten assess the WTA for different data types in different countries, namely the US, Germany and four Latin American countries (Argentina, Brazil, Columbia, and Mexico). After adjusting for currency differences, they found that out of the six countries surveyed, Germans value the privacy of their data the

highest, followed by the Latin American countries, with the US Americans valuing the privacy of their data the least on average. Among the Latin American countries, Columbians value their data privacy the most, followed by Mexicans and Brazilians, with Argentinians valuing their data privacy the least. In addition, the study also finds that people value their financial information the most across countries, while location information was valued the least out of all the data types surveyed. Browsing history data was valued less than financial information but more than location data (Prince & Wallsten, 2022)

A study published in 2021 which compared the WTP amounts between Pakistan and Germany for different data types found that Pakistanis were willing to pay significantly more for the protection of their financial data than the Germans. It also found that Pakistanis value their financial data significantly more than their location or medical data. Moreover, Germans were less concerned about their online privacy than Pakistanis as they felt protected by laws like the GDPR. Germans were also willing to pay less on average, 30 euros per month, than Pakistanis, who were willing to pay 40 euros per month on average for the protection of their data (Schmitt et al., 2021).

There have been studies which looked at the valuation of people's data as a whole without distinguishing different types of data. For example, a study published in 2012 featured an experiment in which 1045 European Facebook users were asked about their willingness to pay to keep their Facebook profile from getting deleted. The study showed that while people's valuation of their Facebook profile varied between 0 to 150 Euros, on average, people valued their Facebook profile at 9.40 Euros. A significant proportion of the participants, about 48%, were not willing to pay anything to keep their Facebook profile, and the majority of the respondents with non-zero WTP used Facebook for diary-keeping (Bauer et al., 2012)

Furthermore, a study published in 2015 asked 203 individuals to give access to their Facebook profile in exchange for varying sums of money while they were engaged in complex everyday activities using anonymous avatars in a virtual world. It found that the proportion of people who were willing to grant access to their Facebook profile increases with the amount of money offered, with 70% of participants willing to give access to their Facebook profile for 1.01 USD with the mean of 0.72 USD and the median of 0.61 USD (Steinfeld, 2015).

Studies have also been done in the context of smartphone apps. For example, a study published in 2013 surveyed 1726 Americans in which participants were asked to choose an App out of 6 options, one original App on the market and 5 alternatives, all having the same functionality but varying levels of price, advertising and user permissions. It found that US smartphone App users are willing to make a single payment of 2.28 USD to keep their online browser history private, 4.05 USD to conceal their list of contacts, 1.19 USD to hide their location from firms, USD 1.75 to protect their phone's identification number, and 3.58 USD to keep the contents of their text messages from being shared. Consumers are also willing to pay 2.12 USD to remove advertisements while using the app (Savage & Waldman, 2013)

Some field experiments to evaluate the valuation of people's data have been conducted in the past as well. A study published in 2010 performed an experiment with 225 students from the Technical University of Berlin. In the first part of the experiment, students were asked to choose to shop from two fictitious competing Compact Disk (CD) selling stores, one of which offered a discount of 1 euro for revealing more sensitive personal information than the other. It was found that about 93% of the buyers chose to buy from a store that offered a one-euro discount in exchange for relatively more sensitive personal information, such as date of birth and monthly income. It shows that students are willing to disclose their date of birth and

monthly income for 1 euro. In the second part of the experiment, where one of the stores asked the participants to provide more sensitive personal information without offering a discount, students were found to buy equally likely from both stores. This shows students are not concerned about privacy issues despite their stated dissatisfaction over data collection and privacy protection (Beresford et al., 2010)

Auctions have also been conducted to evaluate the value of data. For example, a study published in 2013 used a reverse second-price auction with 168 residents in Spain to assess their WTA for both online and offline data. They found that people value offline data like age and address more than their online browsing history, at 25 Euros and 7 Euros, respectively. They also showed that users prefer to get money or improved services in exchange for their data rather than getting targeted advertisements (Carrascal et al., 2013).

In the next section, we will describe different methods used in the previous literature for measuring privacy knowledge, privacy protection behaviour, privacy concerns, and privacy valuation. Then, we will describe and explain the survey design for this thesis.

3 Methodology

Here, we will describe different methods used in the previous literature for measuring privacy knowledge, privacy protection behaviour, privacy concerns, and privacy valuation. Then, we will describe and explain the survey design for this thesis.

3.1 Overview of the methods

In the overview, we will explore and describe different methods used in the previous literature for measuring privacy knowledge, privacy protection behaviour, privacy concerns, and privacy valuation.

3.1.1 Methods for measuring privacy knowledge

Here, we describe some of the methods for measuring the privacy knowledge of people in the existing literature. In this thesis, we take the terms privacy knowledge and privacy literacy to mean the same. This is not an exhaustive list of methods for measuring privacy knowledge.

3.1.1.1 The method used by O'Brien & Torres (2012)

This method was used by O'Brien & Torres (2012). It consists of 6 true-or-false questions. The total score ranges from 0 to 6. While it is concise, it is not suitable for our study because it is specific to Facebook (O'Brien & Torres, 2012, as cited in Rakhmanov, 2021).

3.1.1.2 The method used by Park (2013)

Park (2013) used this method. It consists of a total of 19 questions. The questions are divided into three sections: Surveillance practices (which has 8 questions), policy understanding (which has 7 questions) and technical dimension (which has 4 questions). Surveillance practices and policy understanding sections have yes or no questions and they are combined to evaluate the total privacy literacy score out of 15. The technical dimension section is used to assess privacy protection behaviour on a 6-point frequency scale, where 1 is never, and 6 is always. While this is a relatively comprehensive survey as a whole, it does not cover privacy literacy adequately, as knowledge about technical terms or jargon is not evaluated. Furthermore, questions in the policy understanding section are not specific to a region or country, which would make it difficult to assess the knowledge of the participants about the specific policies of the government where they live (Park, 2013, as cited in Rakhmanov, 2021).

3.1.1.3 The method used by Park & Mo Jang (2014)

This method was used by Park & Mo Jang (2014) for measuring privacy knowledge. It consists of 7 true-or-false questions with the I-don't-know option. A point is given for the

correct answer; no point is awarded otherwise. While being concise, it is meant specifically for the privacy knowledge assessment in the context of smartphone apps and is, therefore, not suitable for this study (Park & Mo Jang, 2014, as cited in Rakhmanov, 2021).

3.1.1.4 The method used by Zeissig et al. (2017)

This method was used by Zeissig et al. (2017)It consists of 15 questions, evaluated on a 5-point Likert scale. It has four dimensions: Experience, privacy concern, awareness, and privacy self-efficacy. It is a relatively comprehensive method with subjective questions as well, but it is missing questions about data protection laws and institutional practices (Zeissig et al., 2017, as cited in Rakhmanov, 2021).

3.1.1.5 The OPLIS scale

The OPLIS survey was designed in 2015 after extensive literature research coving about 350 relevant pieces of literature. It consists of 4 different parts, measuring different dimensions of the online privacy knowledge and giving an overall score as well. The four dimensions are knowledge about Institutional practices, knowledge about technical aspects of data protection, knowledge about data protection law, and knowledge about data protection strategies. OPLIS stands for Online Privacy Literacy Scale, with a minimum possible score of 0 and a maximum of 20. While this survey is comprehensive, covering different dimensions of privacy literacy, it might be lengthy for some people, and it has specific questions about the EU and German laws, which limits its suitability to people living in Germany, but these questions can be replaced or adapted to suit people living elsewhere (Trepte et al., 2015, as cited in Rakhmanov, 2021).

3.1.2 Methods for measuring privacy protection behaviour

Here, we describe some of the methods for measuring the privacy protection behaviour of people in the existing literature. In this thesis, we take the terms privacy behaviour and privacy protection behaviour to mean the same. This is not an exhaustive list of methods for measuring privacy protection behaviour.

3.1.2.1 The method used by Park (2013)

This method is used by Park (2013), consists of 12 total questions evaluated on a 6-point frequency scale, where 1 signifies never and 6 signifies very often. It has two dimensions, namely, social dimension and technical dimension. While this is a comprehensive method, it is based on relatively older literature from the 2000s (Park, 2013).

3.1.2.2 The method used by used by Miltgen & Smith (2015)

Like the previous method, this method used by Miltgen & Smith (2015) also consists of 12 total questions, which are evaluated on a 4-point frequency scale instead, where 1 signifies never and 4 signifies always. It has 3 dimensions, which are: technical protection, general caution, and withholding. While its dimensions are comprehensive, the questions are too generic as they do not mention specific techniques, actions or tools for privacy protection, which hampers its ability to assess privacy protection behaviour. For example, one of the questions asks about the tools and strategies to limit unwanted emails without mentioning specific tools and strategies. Similarly, another question mentions not giving personal details without specifying what personal details are (Miltgen & Smith, 2015).

3.1.2.3 The method used by Büchi et al. (2017)

This method was used by Büchi et al. (2017). It consists of 4 total questions, assessed on a 4-point frequency scale where 1 signifies never and 4 signifies frequently. While this is concise method, like the previous method, the questions are not precise enough. For example, one of

the questions asks about modifying privacy settings without mentioning the specific settings, which renders this method too vague to properly assess privacy behaviour (Büchi et al., 2017).

3.1.2.4 The method used by Bernadas & Soriano (2018)

This method was used by Bernadas & Soriano (2018). It consists of 5 total yes-or-no questions. While it is concise, the behaviour assessment is not precise enough as questions are evaluated on a binary scale instead of a frequency scale used in previous methods. Furthermore, like some methods mentioned before, questions in this method are generic, for example, one of the questions asks about reviewing privacy settings without mentioning the specific settings (Bernadas & Soriano, 2018).

3.1.2.5 The method used by Boerman et al. (2021)

This method was used by Boerman et al. (2021). It has a total of ten questions, assessed on a 5-point frequency scale where 1 denotes never, and 5 denotes very often with the do-not-know option which is usually counted as a missing response. So, the higher the score, the more the privacy protection behaviour of a participant. Unlike some previous methods, it does not use generic language. It is focused on statements about a range of specific online strategies to protect privacy online. Furthermore, it is adapted from previous papers and used in a very recent paper published in 2021, which makes it one of the most up-to-date scales for measuring online privacy protection behaviour (Boerman et al., 2021).

3.1.3 Methods for measuring privacy concerns

Here, we describe some of the methods for measuring the privacy concerns of people in the existing literature. This is not an exhaustive list of methods for measuring privacy concerns.

3.1.3.1 The Concern For Information Privacy (CFIP) scale

The CFIP scale was published in a paper in 1996 (Smith et al., 1996). It has 4 dimensions: collection, unauthorized secondary use, improper access, and errors. It focuses on individuals' concerns about organizational privacy practices and responsibilities. As it is an older scale, it may have become outdated for online users in today's world since the internet has evolved a lot since 1996. In addition, it does not test a person's concern about the risks associated with person's online activities (Smith et al., 1996, as cited in Groß, 2020).

3.1.3.2 The Internet Privacy Concerns (IPC) scale

The IPC scale was published in 2004 (Dinev & Hart, 2004). It has two dimensions namely, Abuse (which is concern about misuse of online information) and finding (which is concern about being observed and specific information about an individual being revealed without individual consent or knowledge). It also contains questions about the security of online transactions. While it is a newer scale than CFIP, it is still a relatively old scale (Dinev & Hart, 2004, as cited in Groß, 2020).

3.1.3.3 The Internet Users' Information Privacy Concern (IUIPC-10) scale

The original scale Internet users' information privacy concern (IUIPC), also known as IUIPC-10, was published in 2004 (Malhotra et al., 2004). It was derived from the earlier 15-item CFIP scale which we have described before. As the name suggests, in IUIPC, questions were directed towards internet users. IUIPC has three dimensions: control, awareness and collection. Malhotra et al. deemed collection of data as the starting point of privacy concerns in users. The control dimension was included on the conviction that users only think of procedures as fair when they have control over the procedures. The authors of IUIPC also considered being informed about the data collection important and hence included the awareness dimension. Control and awareness dimensions each have 3 items, and the

collection dimension has 4 items, making it a 10-item scale. Each item is evaluated on a 7-point Likert scale (Malhotra et al., 2004, as cited in Groß, 2020).

3.1.3.4 The IUIPC-8 scale

In 2020, Thomas Groß came up with the statically improved IUIPC-8 scale, which has better construct validity and reliability. IUIPC-8 is the same as IUIPC-10, but with 8 items instead of 10, with one less item each in control and awareness dimensions (Groß, 2020).

3.1.4 Methods for measuring privacy valuation

Here, we describe some of the methods for measuring the privacy valuation of people in the existing literature. In this thesis, we take the terms privacy valuation and valuation of data to mean the same. This is not an exhaustive list of methods for measuring privacy knowledge.

3.1.4.1 Surveys

Surveys involve asking questions to the participants about the WTP of the participants like it is done by Schmitt et al. (2021), WTA of the participants like it is done by Prince & Wallsten (2022) or both the WTP and WTA like it is done by Winegar & Sunstein (2019). The questions can vary in the contexts in which they are formulated, like Schmitt et al. (2021) ask for privacy valuation in a different context as compared to Winegar & Sunstein (2019). The survey questions can be closed-ended, like it is done by Schmitt et al. (2021), or open-ended like it is done by Winegar & Sunstein (2019). However, with open-ended questions, people might exaggerate their data valuation, as observed by Winegar & Sunstein (2019).

3.1.4.2 Field experiments

Field experiments attempt to find out people's privacy valuation by performing in real-life situations, as done by Beresford et al. (2010) and Acquisti et al. (2013). Field experiments give us a chance to observe the actual actions of people in real-life situations in regard to

their privacy valuations, as shown by Beresford et al. (2010) and Acquisti et al. (2013) rather than exaggerated data valuation as shown in response to the Winegar & Sunstein (2019) survey questionnaire. Unlike the surveys, though, additional resources, including financial resources, are needed to conduct the field experiments, as shown by Beresford et al. (2010) and Acquisti et al. (2013).

3.2 Survey Design

Here, we will describe our survey design in the order in which it was shown to the online survey participants. The online survey was conducted using google forms. It had a total of 8 sections. Next, we will describe each section in detail.

3.2.1 Section 1: Information about the survey

The first section of the survey gives a brief introduction to the survey, stating who is conducting the survey and for which purpose, along with its target audience. Furthermore, it also gives the instructions about filling out the survey and the estimated time it would take to complete the survey. It is emphasized that people answer all the questions based on their existing knowledge without the use of any online or offline resource and there are no right and wrong answers to get the responses which reflect the actual state of mind of the individuals. Then, under the heading of "Data protection information", the text gives the participants information about how their data will be stored and used and that the data will be deleted after the completion of the master thesis. It also tells the respondents information about how they can request the deletion of their data using their personal unique code and give feedback about the survey. Lastly, it asks each participant to consent to participate in the survey. The participant can choose whether to do the survey or not without any consequences.

The survey only proceeds to the next page if the participant has explicitly agreed to take part in the survey.

3.2.2 Section 2: Personal unique code

As mentioned in the last paragraph, the second section asks people to construct a unique code based on the given set of instructions, which will not only help to get responses from real and unique persons, but a participant can also use it to request deletion after submitting a response. The instructions which are given to the participants are as follows:

1. The first letter of your mother's first name:
2. The first letter of your father's first name:
3. The first letter of your place of birth:
4. The last digit of your year of birth:
5. The last digit of your birthday:

These instructions must be followed in the same order as given to construct the personal unique code.

3.2.3 Section 3: Questions about online privacy knowledge

The third section presents questions about privacy knowledge. To assess the privacy knowledge of the participants, we chose to use the OPLIS scale because it is comprehensive, covering four different and relevant dimensions of privacy knowledge, including questions specific to the EU and German laws, which can be adapted to any region in the world as per requirement (Masur et al., 2017, as cited in Rakhmanov, 2021) So, the OPLIS scale will be used in this study for measuring the online privacy knowledge of the participants, with all

five of the questions in the "Knowledge about data protection law" (Masur et al., 2017, p. 5) section of the scale replaced with the five questions related to the data protection laws in Pakistan. The order of all the questions in the modified OPLIS scale used in our study was randomized to mitigate the ordering effects (Acquisti et al., 2013; Winegar & Sunstein, 2019). The order of the answer options was also randomized for the same reason except for the True, False, and Don't-know answer options. The order of the True, False, and Don't-know answer options was not randomized to prevent participants' confusion while answering the question on their screens. The five replacement questions about data protection law in Pakistan are taken from a paper published in 2021 (Aleem et al., 2021). We tried to make the replacement questions and the answer choices as close as possible to the original questions and answer choices to minimize distortion in the OPLIS scale. Furthermore, it should be noted that neither the English translation of the OPLIS scale used in our study has been checked for its validity and reliability (Masur et al., 2017) nor the effect of the replacement questions on the validity and the reliability of the OPLIS scale was calculated because it is beyond the scope of the master's thesis. The complete OPLIS Scale with the replacement questions used to measure privacy knowledge in this study is given in the appendix. The replacement of the questions is described in detail below:

The first question, "Forwarding anonymous user data for the purpose of market research is legal in the European Union." (Masur et al., 2017, p. 5) with the answer options: True, False, and, Don't know (Masur et al., 2017, p. 5), was replaced with "Unauthorized access, copying and transmission of any data with dishonest intention is illegal in Pakistan". The answer options stayed the same.

The second question, "The EU-Directive on data protection..." (Masur et al., 2017, p. 5) with the four answer options, "A. ... has to be implemented into national data protection acts by

every member state." (Masur et al., 2017, p. 5), "B. ... does not exist yet." (Masur et al., 2017, p. 5), "C. …functions as a transnational EU-data protection act." (Masur et al., 2017, p. 5), and "D. ... solely serves as a non-committal guideline for the data protection acts of the member states." (Masur et al., 2017, p. 5) was replaced with "Pakistan Electronic Crimes Act (PECA)..." with the answer options formed to resemble the original answer options, "A. ...was passed in 2016.", "B. ...does not exist.", "C. ...is being drafted by the Pakistani parliament.", and "D. ...solely serves as a non-committal guideline for the data protection in Pakistan." Note that the order of the answer options in this question was randomised.

The third question, "In Germany, the same standard GTC applies for all SNS. Any deviations have to be indicated." (Masur et al., 2017, p. 5) with the three answer options: True, False, and, Don't know (Masur et al., 2017, p. 5) was replaced with "Pakistani law enforcement agencies may ask residents to transfer their private data without the requirement of court warrant." With the same answer options.

The fourth question, "According to German law, users of online applications that collect and process personal data have the right to inspect which information about them is stored." (Masur et al., 2017, p. 5) with the answer options: True, False, and, Don't-know (Masur et al., 2017, p. 5) was replaced with "Internet service providers (ISPs) in Pakistan are obligated to retain specific traffic data for at least one year and share it with the investigative agencies upon request." with the same answer options.

The fifth and last question in the "Knowledge about data protection law" (Masur et al., 2017, p. 5) section of the OPLIS scale, "Informational self-determination is…" (Masur et al., 2017, p. 5) with the answer options, "A. ... a fundamental right of German citizens." (Masur et al., 2017, p. 5), "B. ... a philosophical term." (Masur et al., 2017, p. 5), "C. … the central claim of data processors." (Masur et al., 2017, p. 5), and "D. ... the central task of the German Federal

Data Protection Commissioner.” (Masur et al., 2017, p. 5) was replaced with “The "Dignity of man" is...” with the answer options, “...a fundamental right of the Pakistani citizens.”, “...a philosophical term.”, “... the central claim of data processors.”, and “...the central task of the National Commission for Personal Data Protection.”. The order of the answer options for this question was randomized.

The privacy knowledge questions are placed early in the survey because this is the lengthiest section in the survey with a total of 20 questions. A participant who is mentally fresh is more likely to answer the questions truthfully and more likely to complete the survey without losing interest.

3.2.4 Section 4: Questions about privacy protection behaviour

This section of the survey is about privacy protection behaviour. We use the method from a paper published in 2021 (Boerman et al., 2021) for the assessment of people’s online privacy protection behaviour in our survey. It has a total of ten questions, assessed on a 5-point frequency scale where 1 denotes never, and 5 denotes very often with the do-not-know option which is usually counted as a missing response. So, the higher the score, the more the privacy protection behaviour of a participant. Unlike some previous methods, it does not use generic language. It is focused on statements about a range of specific online strategies to protect privacy online. Furthermore, it is adapted from previous papers and used in a very recent paper published in 2021, which makes it one of the most up-to-date scales for measuring online privacy protection behaviour (Boerman et al., 2021). For these reasons, we decided to use this scale without any changes for measuring privacy protection behaviour in our study. The complete scale for measuring privacy protection in this study is given in the appendix. While the order of the questions in this section was also randomized to minimize the ordering effect (Acquisti et al., 2013; Winegar & Sunstein, 2019), the layout of the answer options was

kept the same to avoid confusion among participants. The section about protection behaviour questions was placed on the 4th number, after privacy knowledge questions, because it has the second highest number of questions which is 10.

3.2.5 Section 5: Questions about privacy concerns

The fifth section contains questions about online privacy concerns. For this study, we will use the IUIPC-8 (Groß, 2020), as it is, to gauge the privacy concerns of the respondents. We chose the IUIPC-8 scale because it includes 3 important dimensions of privacy concerns: control, awareness, and collection and its validity and reliability have been proven relatively recently in 2020, making it one of the most up-to-date privacy concern scales (Groß, 2020). The complete scale used for measuring privacy concerns in this study is given in the appendix. While the order of the questions in this section was also randomised to minimize the ordering effect (Acquisti et al., 2013; Winegar & Sunstein, 2019), the layout of the answer options was kept the same to avoid confusion among participants. Online privacy concerns section is placed 5th in the survey because it is the third lengthiest section with a total of 8 questions.

3.2.6 Section 6: Questions about the WTA

The sixth section of the survey contains questions about the respondents' willingness to accept money in exchange for their data, also referred to as the WTA questions. For our study, we describe the WTA amount as the monthly amount in Pakistani Rupees for which a person would allow the companies to access their data. This description of the WTA amount is based on the paper published in 2019 (Winegar & Sunstein, 2019). The questions in this section are about 5 data types. These 5 data types are taken from a paper which examined the differences in privacy valuation between Germans and Pakistanis (Schmitt et al., 2021), making these

data types relevant in the Pakistani context. The five data types are: financial data, location data, medical records, “personal data” (we will refer to this either as “personal data” or “personal data type” to distinguish it from the general use of the term), and web activity data.The question design was taken from the paper published in 2019 (Winegar & Sunstein, 2019) with some modifications to accommodate the five different data types and our target audience (Pakistanis). The sample WTA question for the “personal data type” is as follows:

It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access your “personal data” (e.g. your name, age, date of birth and personal registration number)?

The term "online platforms" was used to avoid the effect of people’s personal perceptions of a specific company on the privacy valuation. The currency (Pakistan Rupees) and the recurring nature of the transaction (per month) are specified to clarify the scenario. The specific data type is also explained by giving the participant examples of what is considered personal data, improving the clarity of the question even more. This is done so that every participant is on the same page while doing the WTA questions.

The answer options are also based on the same paper from where we adopted the data types, that is, (Schmitt et al., 2021). The answer options from this paper were chosen because this is only paper, we found which has privacy valuation answer options specifically tailored towards Pakistanis. The authors of the paper, based the amounts of the answer options on the prices of everyday things in Pakistan (Schmitt et al., 2021). However, since the paper was published in 2021, we adjusted the amounts in the answer options to year 2023 using Pakistan’s year-over-year percentage change in the Consumer Price Index (CPI) data provided by the International Monetary Fund (IMF) (* *, n.d.). Overlap between the

answer options was also removed to have a clear distinction between the value categories. Answer options were formed in the following way:

The category of “nothing, online platforms can access my personal data for free.” is created to accommodate the zero WTA amount as it is also done in the literature (Schmitt et al., 2021). We added explicit text to clarify this value category to the participant.

The value category of “1 - 235 Rupees per month.” is created based on the 0-150 Rupee category in the paper (Schmitt et al., 2021). We came up with the upper limit of 235 for our value category by adjusting the 150 amount in the following way:

The amount of 150 was first adjusted for the year 2022 using the inflation rate of 19.87% as provided by the IMF (* *, n.d.). So, 150 now becomes 179.805 in 2022. Now, the amount of 179.805 is further adjusted using the IMF inflation rate of 30.77% (* *, n.d.). So, the amount of 179.805 now becomes 235.131 which is rounded to the nearest Rupee to be 235 Rupees per month. Similarly, the “236 - 470 Rupees per month.” category is made based on the 150-300 value category in the paper (Schmitt et al., 2021) after adjusting for inflation to reflect the amounts in today’s Pakistan as accurately as possible. The “471 - 705 Rupees per month.” category is created based on the 300-450 value category in the paper (Schmitt et al., 2021) after adjusting for inflation. Finally, the “706 and more Rupees per month.” category is created based on the 450 and more value category in the paper (Schmitt et al., 2021), after adjusting for inflation.

In addition, we added the answer option, “nothing, I do not want to trade my personal data in exchange for money.” to our WTA questions to accommodate those who do not want to exchange their data for money.

The complete WTA questions together with the answer options are given in appendix. The WTA questions are placed in the sixth section because there are only 5 WTA questions. While the order of the WTA questions is randomized, the order of the answer options is kept the same to avoid causing confusion among the participants. The answer options are presented in the same order as given in the appendix.

3.2.7 Section 7: Questions about the WTP

The second last section of the survey is about the willingness to pay questions for the deletion of data, also referred to as WTP questions. For our study, we describe the WTP amount as the monthly amount in Pakistani Rupees a person would pay to the companies to delete that person's data from the companies' records. This description of the WTP amount is based on the paper published in 2019 (Winegar & Sunstein, 2019). The WTP questions are very similar to the WTA questions. This is done to maintain consistency and to minimize the influence of anything other than the obvious difference between willingness to accept and willingness to pay for the respondents. The WTP questions in this section are about the same 5 data types as the WTA questions: financial data, location data, medical records, personal data, and web activity data. The general structure of the questions is also taken from the same paper (Winegar & Sunstein, 2019), from where we adopted the WTA questions, with some modifications to account for the five different data types and Pakistani participants. The sample WTP question for the "personal data type" is as follows:

It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. What would you be willing to pay per month (in Pakistan Rupees) to delete all of your "personal data" (e.g. your name, age, date of birth and personal registration number) from all parties that hold it?

The term, online platforms, was used to avoid the effect of people's personal perception of a specific company on the privacy valuation. The currency (Pakistan Rupees) and the recurring nature of the transaction (per month) are specified to clarify the scenario. The specific data type is also explained by giving the participant examples of what is considered personal data improving the clarity of the question even more. This is done so that every participant is on the same page while doing the WTP questions.

The answer options to the WTP questions are similar to the answer options to the WTA questions in the previous section. The answer options with the amounts 1 - 235 Rupees per month, 236 - 470 Rupees per month and 471 - 705 Rupees per month are kept the same to ensure consistency and enable comparison between the WTP and WTP. The two answer options which differ from the WTA answer options are as follows:

The "nothing, I can't afford to pay" answer option is for people who would be willing to pay to delete their data but cannot afford to, and the "nothing, I do not want to delete my personal data held by online platforms " option is for those who do not want to delete their data held by online platforms.

The complete WTP questions together with the answer options are given in appendix. While the order of the WTP questions is randomised, the order of the answer options is kept the same to avoid causing confusion among the participants. The answer options are presented in the same order as given in the appendix. The WTP questions are placed in the seventh section because there are only 5 WTP questions, like the 5 WTA questions. There was no particular reason to put the WTA questions before the WTP questions.

3.2.8 Section 8: Demographic questions

The final section of our online survey contains 5 demographic questions. The 5 questions were presented in a random order. The questions asked about the participants' gender, age range, monthly income, nationality, and whether or not an individual resides in Pakistan. The gender question had 4 options: male, female, Other and prefer not to say. These answer options are selected based on the fact that Pakistan officially only recognizes three genders, male, female and a gender-neutral "X", as reported in the news article (Ullah, 2017). The "prefer not to say" option is included to give the participant a choice to opt out. The age range question has eight options, which were adopted from the paper assessing the value of data among the Chinese people (Tang & Wang, 2021). The eight options were "Below 18", "18-25", "26-30", "31-40", "41-50", "50-60", "61 and above", and "Prefer not to say". Again, the "prefer not to say" option was added to allow the participants to opt out of the question if they wish to do so. The question on the monthly personal income also has eight answer options. These answer options were constructed based on the income tax brackets in Pakistan as published by Pakistan's Federal Board of Revenue in 2023 and mentioned in an online news article (Staff, 2023). The eight answer options are, "None", "Up to 50,000 Rupees per month.", "50,001 - 100,000 Rupees per month.", "100,001 - 200,000 Rupees per month.", "200,001 - 300,000 Rupees per month.", "300,001 - 500,000 Rupees per month.", "500,001 Rupees and above per month.", and "Prefer not to say". Again the "Prefer not to say" option is provided to allow the participant to be able to opt out. The nationality question has three answer options, "Pakistani", "Multiple (Pakistani and other)", and "Other (non-Pakistani)". The extended list of nationalities is not given as an option because, for our study, we are only interested in knowing if a person is a Pakistani national or not. The "prefer not to say" opt-out option is also not given because the question about nationality will be used to filter non-Pakistani nationals because we are specifically targeting Pakistani nationals for our study.

The final question about whether a participant is residing in Pakistan or not has only two answer options, “Yes” and “No”, with no opt-out option because this question is also used as a filter since we are specifically looking for Pakistani citizens who are residing in Pakistan currently. Pakistanis living abroad might differ in their online privacy knowledge, online privacy behaviour and online privacy valuation from those who are residing in Pakistan. All 5 demographic questions are given in the appendix. The demographic questions are placed in the section because demographic questions are mentally easier to do.

4 Results

Here, we will describe the results of our online survey and what we found out after analysing the answers to our online survey.

4.1 Descriptive statistics

First, we will look at the descriptive statistics about the demographics of our survey participants and then, we will report the descriptive statistics about the participants’ privacy valuation.

4.1.1 Demographical descriptive statistics

The online survey was opened and distributed to friends and family in Pakistan on 16th of May 2024 and the survey was closed on the 6th of June 2024. During this period, a total of 39 people participated in the survey. Two of the responses were later removed for filling out junk data. So, we were left with 37 responses. Our analysis and results are based on these 37 unique responses. Out of the 37 respondents, 19 were male, 15 were female and 3 indicated that they prefer not to specify their gender.

Furthermore, the largest age group in our sample, 15 participants, was between the ages of 18 to 25. Nine participants were between the ages of 26 to 30. Six were between the ages to 31 to 40. Only one participant was in the age range of 41 to 50. Three were between 51 to 60 years old and, only one person indicated to 61 and above. Three people did not disclose their age.

Income statistics revealed that 6 of the participants had no personal monthly income. Ten people had an income of up to 50000 Rupees per month, six had an income in the 50001 to 100000 Rupees per month range. Six had an income in the 100001 to 200000 Rupees per month range and, only one person earned between 200001 to 300000 Rupees per month. Eight participants chose not to reveal their monthly income. The demographics are shown in Table 4-1.

Table 4-1 Demographic profile of respondents

Demographic characteristic	**Category**	**Number of participants**
Sex	Male	19
	Female	15
	Other	0
	Prefer not to say	3
Age range	Below 18	0
	18 - 25	15

	26 - 30	9
	31 – 40	6
	41 - 50	1
	51 - 60	3
	61 and above	1
	Prefer not to say	2
Personal Monthly income (in PKR)	None	6
	Up to 50,000	10
	50,001 - 100,000	6
	100,001 – 200,000	6
	200,001 – 300,000	0
	300,001 – 500,000	1
	500,001 and above	0
	Prefer not to say	8

4.1.2 Descriptive statistics about privacy valuation

Now, we will examine the descriptive statistics for the participants' responses to the WTA and WTP questions.

4.1.2.1 Descriptive statistics about willingness to pay responses

Here, we will look at the descriptive statistics for the participants' responses to the WTP for all 5 different data types.

Out of 37 participants, only 19 were willing to pay money to online platforms in exchange for the deletion of their financial data. Out of these 19, six indicated that they could not afford to pay. Six were willing to pay between 471 and 705 Rupees per month for the deletion of their financial data. Another 5 were willing to pay between 1 and 235 Rupees per month, while the remaining two participants said that they could not pay between Rupees 236 to 470 per month. This is shown in Table 4-2.

Table 4-2 Descriptive statistics about WTP for financial data

Descriptive statistics about WTP for financial data	
Amount	**Number of participants**
Nothing, I do not want to delete my personal data held by online platforms.	18
Nothing, I can't afford to pay.	6
1 - 235 Rupees per month.	5
236 - 470 Rupees per month.	2
471 - 705 Rupees per month.	6
706 and more Rupees per month	0

Out of 37 participants, only 19 were willing to pay money to online platforms in exchange for the deletion of their location data. Seven indicated that they could not afford to pay. Six were willing to pay between 471 and 705 Rupees per month for the deletion of their location data. Another 4 were willing to pay between 1 and 235 Rupees per month, while the remaining two participants said that they could pay between Rupees 236 and 470 per month. This is shown in Table 4-3.

Table 4-3 Descriptive statistics about WTP for location data

Descriptive statistics about WTP for location data	
Amount	**Number of participants**
Nothing, I do not want to delete my personal data held by online platforms.	18
Nothing, I can't afford to pay.	7
1 - 235 Rupees per month.	4
236 - 470 Rupees per month.	2
471 - 705 Rupees per month.	6
706 and more Rupees per month	0

Out of 37 participants, only 20 were willing to pay money to online platforms in exchange for the deletion of their medical data. Out of these 20, eleven indicated that they could not afford to pay. Six were willing to pay between 471 and 705 Rupees per month for the deletion of their medical data, while the remaining 3 were willing to pay between 1 and 235 Rupees per month. This is shown in Table 4-4.

Table 4-4 Descriptive statistics about WTP for medical data

Descriptive statistics about WTP for medical data	
Amount	**Number of participants**
Nothing, I do not want to delete my personal data held by online platforms.	17
Nothing, I can't afford to pay.	11
1 - 235 Rupees per month.	3
236 - 470 Rupees per month.	0
471 - 705 Rupees per month.	6
706 and more Rupees per month	0

Out of 37 participants, only 22 were willing to pay money to online platforms in exchange for the deletion of their "personal data". Out of these 22, ten indicated that they could not afford to pay. Seven were willing to pay between 471 and 705 Rupees per month for the deletion of their personal data. Another 4 were willing to pay between 1 and 235 Rupees per month, while the remaining one participant said that they could pay between Rupees 236 to 470 per month. This is shown in Table 4-5.

Out of 37 participants, only 19 were willing to pay money to online platforms in exchange for the deletion of their web activity data. Out of these 19, nine indicated that they can not afford to pay. Four were willing to pay between 471 and 705 Rupees per month for the deletion of their web activity data. Another five were willing to pay between 1 and 235 Rupees per month, while the remaining one participant said that they could pay between Rupees 236 to 470 per month. This is shown in Table 4-6.

Table 4-5 Descriptive statistics about WTP for "personal data"

Descriptive statistics about WTP for "personal data"	
Amount	**Number of participants**
Nothing, I do not want to delete my personal data held by online platforms.	15
Nothing, I can't afford to pay.	10
1 - 235 Rupees per month.	4
236 - 470 Rupees per month.	1
471 - 705 Rupees per month.	7
706 and more Rupees per month	0

Table 4-6 Descriptive statistics about WTP for web activity data

Descriptive statistics about WTP for web activity data	
Amount	**Number of participants**
Nothing, I do not want to delete my personal data held by online platforms.	18
Nothing, I can't afford to pay.	9
1 - 235 Rupees per month.	5
236 - 470 Rupees per month.	1
471 - 705 Rupees per month.	4
706 and more Rupees per month	0

4.1.2.2 Descriptive statistics about willingness to accept responses

Here, we will look at the descriptive statistics for the participants' responses to the WTA for all 5 different data types.

Out of 37 participants, only 14 were willing to accept money in exchange for their financial data. Out of these 14, eight were willing to give online platforms access to their financial data for free. Three required between 471 and 705 Rupees per month in exchange for their financial data, two people required 706 Rupees per month or more, while only one participant asked between Rupees 1 to 235 per month for selling financial data. This is shown in Table 4-7.

Table 4-7 Descriptive statistics about WTA for financial data

Descriptive statistics about WTA for financial data	
Amount	**Number of participants**
Nothing, I do not want to trade my personal data in exchange for money.	23
Nothing, online platforms can access my personal data for free.	8
1 - 235 Rupees per month.	1
236 - 470 Rupees per month.	0
471 - 705 Rupees per month.	3
706 and more Rupees per month	2

Out of 37 participants, only 15 were willing to accept money in exchange for their location data. Out of these 15, six were willing to give online platforms access to their location data for free. Six required 706 Rupees per month or more. Two required between 471 and 705

Rupees per month in exchange for their location data, while only one participant asked between Rupees 1 to 235 per month for selling location data. This is shown in Table 4-8.

Table 4-8 Descriptive statistics about WTA for location data

Descriptive statistics about WTA for location data	
Amount	**Number of participants**
Nothing, I do not want to trade my personal data in exchange for money.	22
Nothing, online platforms can access my personal data for free.	6
1 - 235 Rupees per month.	1
236 - 470 Rupees per month.	0
471 - 705 Rupees per month.	2
706 and more Rupees per month	6

Out of 37 participants, only 16 were willing to accept money in exchange for their medical data. Out of these 16, seven people were willing to give online platforms access to their medical data for free. Eight required 706 Rupees per month or more, and only one participant asked between Rupees 471 to 705 per month for selling medical data. This is shown in Table 4-9.

Table 4-9 Descriptive statistics about WTA for medical data

Descriptive statistics about WTA for medical data	
Amount	**Number of participants**
Nothing, I do not want to trade my personal data in exchange for money.	21
Nothing, online platforms can access my personal data for free.	7
1 - 235 Rupees per month.	0
236 - 470 Rupees per month.	0
471 - 705 Rupees per month.	1
706 and more Rupees per month	8

Out of 37 participants, only 17 were willing to accept money in exchange for their personal data. Out of these 17, six were willing to give online platforms access to their personal data for free. Six required 706 Rupees per month or more. Two required between 471 and 705 Rupees per month in exchange for their personal data. Another 2 respondents required between 1 and 235 Rupees per month, while only one participant asked between Rupees 236 to 470 per month for selling personal data. This is shown in Table 4-10.

Table 4-10 Descriptive statistics about WTA for "personal data"

Descriptive statistics about WTA for "personal data"	
Amount	**Number of participants**
Nothing, I do not want to trade my personal data in exchange for money.	20
Nothing, online platforms can access my personal data for free.	6
1 - 235 Rupees per month.	2
236 - 470 Rupees per month.	1
471 - 705 Rupees per month.	2
706 and more Rupees per month	6

Out of 37 participants, only 18 were willing to accept money in exchange for their web activity data. Out of these 18, seven were willing to give online platforms access to their web activity data for free. Eight required 706 Rupees per month or more. One required between 471 and 705 Rupees per month in exchange for their web activity data. Another one required between 1 and 235 Rupees per month, while the remaining one participant asked between Rupees 236 to 470 per month for selling web activity data. This is shown in Table 4-11.

Table 4-11 Descriptive statistics about WTA for web activity data

Descriptive statistics about WTA for web activity data	
Amount	**Number of participants**
Nothing, I do not want to trade my personal data in exchange for money.	19
Nothing, online platforms can access my personal data for free.	7
1 - 235 Rupees per month.	1
236 - 470 Rupees per month.	1
471 - 705 Rupees per month.	1
706 and more Rupees per month	8

4.2 Comparison between WTA and WTP

To make a comparison between the WTA and the WTP, first we removed the participants' answers that indicated that they did not want to engage in the trade of money and their data. We did this by removing the "nothing, I do not want to trade my financial data in exchange for money." responses for the WTA question. We repeated this for WTA questions for all the 4 remaining data types: location data, medical data, personal data and web activity data. Then we removed the "nothing, I do not want to delete my financial held by online platforms."

responses for the WTP question. We repeated this for WTP questions for all the 4 remaining data types: location data, medical data, personal data and web activity data.

After this, we were left with a total of 80 responses for WTA and 99 responses for the WTP across all data types. Next, to compare the WTA and WTP, we decided to determine the median value for both WTA and WTP since we are statistically not permitted to do arithmetic operations on ordinal data to draw meaningful conclusions (Bhandari, 2020). Even the median is only permitted in cases where the median can be determined without having to do any arithmetic operation on the ordinal data itself (Bhandari, 2020).

To determine the median value for the WTA, first all the ordinal values are arranged in the ascending order. For the WTA with 80 total responses, the median would be the average of the 40^{th} and the 41^{st} values. Since the 40^{th} and the 41^{st} values are both the same, the median can be found without having to perform any arithmetic operation and hence, would be statistically valid and meaningful. The median value for WTA is “236 – 470 Rupees per month”.

To determine the median value for the WTP, first all the ordinal values are arranged in the ascending order. For the WTP with 99 total responses, the median would be the 50^{th} value. Since the median is the 50^{th} value in an ordered data set, the median is found without having to perform any arithmetic operation and hence would be statistically valid and meaningful. The median value for WTP is “1 – 235 Rupees per month”.

We can see that the overall WTA amount is higher than the WTP amount.

4.3 Comparison between valuations of different data types

To compare the valuations of different data types, we would compare the WTP for the five data types we surveyed. WTP is a better measure of comparison of data types because people are willing to engage more when asked to pay for the deletion of data as shown by 19 more responses for the WTP questions than the WTA questions. It also shows that people prefer to pay for the deletion of data over accepting money for selling their data. This is specifically important because people are more willing to pay than accept money despite Pakistan being a developing country with a GDP per capita of 1,407 US Dollars (*World Bank Open Data*, n.d.) and an HDI of 0.540, which is below the global average HDI (Nations, n.d.). So, WTP is a better representation of people's valuation of their data.

Now, to compare the WTP for different data types, we need to calculate the average value for the WTP of each data type. Since we have collected responses for WTP as ordinal data, we can not use the mean as a measure of central tendency because it involves performing arithmetical operations on ordinal data which can not yield meaningful results statistically as discussed before (Bhandari, 2020). Similarly, for calculating the median for the WTP of each data type, we had to perform arithmetic operations which makes the median an unsuitable measure in our context. The frequency for the WTP of each of the 5 different data types comes out to be the same, 0, making it unusable for the purpose of comparison as well.

Since, we could not use any of the three conventional measures of central tendency in our case, we decided to use an unconventional measure to estimate the WTP of each data type to make a meaningful comparison. We decided to use the percentage of the number of people who indicated that they were willing to pay a non-zero amount to online platforms to delete their data of a specific type, out of the total number of people who were willing to pay for that specific data type. We use this percentage as a proxy to estimate the WTP for each data

type because, in our opinion, the more people willing to pay a non-zero for the specific data type, the more that data type is valued in the eyes of respondents, given the economic conditions of average people in a developing country like Pakistan, as described before (Nations, n.d.; *World Bank Open Data*, n.d.).

Using the above measure, financial data is valued the highest with 68.42% of the people who were willing to pay a non-zero amount out of the total respondents who were willing to pay for the financial data. Location data was valued the second highest, with 63.16% of respondents willing to pay a non-zero amount. Next is the "personal data", for which 54.55% were willing to pay a non-zero amount. For the web activity data, 52.63% were willing to pay a non-zero amount, making it the second lowest-valued data type. Finally, the lowest-valued data type among Pakistanis is the medical data with only 45% of the participants willing to pay a non-zero amount for it.

4.4 Relationship between privacy literacy and privacy valuation

To determine the relation between privacy literacy and privacy valuation (our first research question, we would look at the relationship between privacy literacy and WTP and WTA for different data types one by one as we surveyed the participants for their WTP and WTA for each data type separately.

4.4.1 Privacy literacy and willingness to accept (WTA)

In this section, we will look at the relationship between privacy literacy and willing to accept for each of the five data types individually. For privacy literacy, the sum of the correct answers given by each participant will be used as their privacy literacy score. All the analyses referring to privacy literacy will use this score.

4.4.1.1 Privacy literacy and the willingness to accept for financial data

First, we removed the participants' responses "nothing, I do not want to trade my financial data in exchange for money." for the Willingness To Accept for Financial data (WTA-F) as those participants were not willing to exchange their financial data for money. After that, we were left with 14 data points out of 37. So, we did all the processing on 14 remaining data points.

Next, we assign five answer options to WTA-F question a numerical value from 0 to 4 in the following way:

- The "nothing, online platforms can access my financial data for free." option was assigned a value of 0.
- The "1 - 235 Rupees per month." option was assigned a value of 1.
- The "236 - 470 Rupees per month." option was assigned a value of 2.
- The "471 - 705 Rupees per month." option was assigned a value of 3.
- The "706 and more Rupees per month" option was assigned a value of 4.

WTA-F variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTA-F variables.

To determine the relationship between privacy literacy and WTA-F, we need to see whether the privacy literacy and the WTA-F variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.696. WTA-F is shown to be not normally distributed as its value of significance is less than 0.001.

This is shown in Figure 4-1. Since WTA-F is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.156	14	.200*	.958	14	.696
WTA for Financial Data Ordinal	.349	14	<,001	.720	14	<,001

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-1: Normality test for privacy literacy and WTA for financial data

Now, in order to check if privacy literacy and WTA-F have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.407 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTA-F. Moreover, deviation from linearity has a significance value of 0.570 which shows that there is no non-linear relationship between the two variables either. This is shown in Figure 4-2.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTA for Financial Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	18.357	7	2.622	.851	.587
		Linearity	2.448	1	2.448	.794	.407
		Deviation from Linearity	15.909	6	2.651	.860	.570
	Within Groups		18.500	6	3.083		
	Total		36.857	13			

Figure 4-2: Linearity test for privacy literacy and WTA for financial data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTA-F by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTA-F either as shown in Figure 4-3.

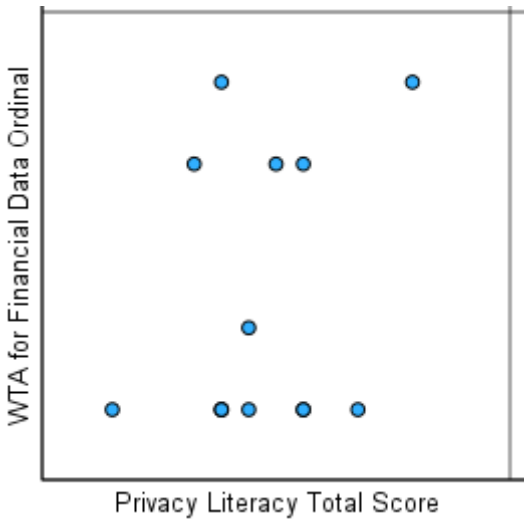

Figure 4-3: Scatter plot between privacy literacy and WTA for financial data

We find that there is a small positive statistically non-significant correlation between privacy literacy and WTA-F as shown by Spearman's rank correlation coefficient of 0.141 and Kendall's tau correlation coefficient of 0.130. This is shown in the Figure 4-4. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTA-F among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTA for Financial Data Ordinal	Correlation Coefficient	.130
		Sig. (2-tailed)	.573
		N	14
Spearman's rho	WTA for Financial Data Ordinal	Correlation Coefficient	.141
		Sig. (2-tailed)	.631
		N	14

Figure 4-4: Correlation between privacy literacy and the WTA for financial data

4.4.1.2 Privacy literacy and the willingness to accept for location data

First, we removed the participants' responses "nothing, I do not want to trade my location data in exchange for money." for the Willingness To Accept for Location data (WTA-L) as those participants were not willing to exchange their location data for money. After that, we were left with 15 data points out of 37. So, we did all the processing on 15 remaining data points.

Next, we assign five answer options to WTA-L question a numerical value from 0 to 4 in the following way:

- The “nothing, online platforms can access my location data for free.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTA-L variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTA-L variables.

To determine the relationship between privacy literacy and WTA-L, we need to see whether the privacy literacy and the WTA-L variables are normally distributed or not. To check for the normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.169. WTA-L is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-5. Since WTA-L is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.228	15	.034	.916	15	.169
WTA for Location Data Ordinal	.261	15	.007	.734	15	<,001

a. Lilliefors Significance Correction

Figure 4-5: Normality tests for privacy literacy and the WTA for location data

In order to check if privacy literacy and WTA-L have a monotonic relationship, first, we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.699 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTA-L. Moreover, deviation from linearity has a significance value of 0.423 which shows that there is no non-linear relationship between the two variables either. This is shown in Figure 4-6.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTA for Location Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	25.600	7	3.657	1.011	.495
		Linearity	.589	1	.589	.163	.699
		Deviation from Linearity	25.011	6	4.169	1.152	.423
	Within Groups		25.333	7	3.619		
	Total		50.933	14			

Figure 4-6: Linearity test for privacy literacy and WTA for location data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTA-L by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTA-L either as shown in Figure 4-7.

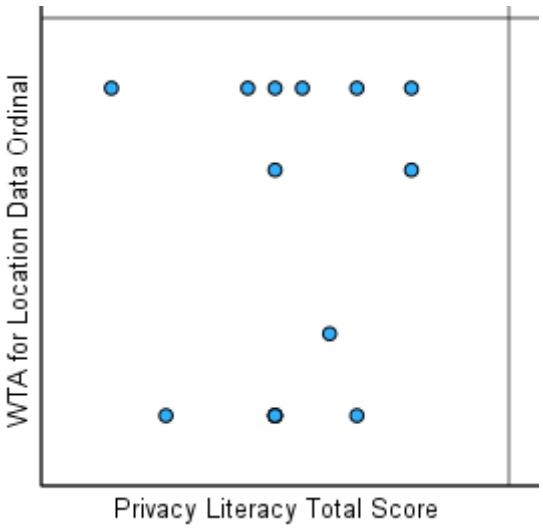

Figure 4-7: Scatter plot for privacy literacy and the WTA for location data

We find that there is a small positive statistically non-significant correlation between privacy literacy and WTA-L as shown by Spearman's rank correlation coefficient of 0.123 and Kendall's tau correlation coefficient of 0.112. This is shown in Figure 4-8. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTA-L among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTA for Location Data Ordinal	Correlation Coefficient	.112
		Sig. (2-tailed)	.618
		N	15
Spearman's rho	WTA for Location Data Ordinal	Correlation Coefficient	.123
		Sig. (2-tailed)	.663
		N	15

Figure 4-8: Correlation between privacy literacy and the WTA for the location data

4.4.1.3 Privacy literacy and the willingness to accept for medical data

First, we removed the participants' responses "nothing, I do not want to trade my medical records in exchange for money." for the Willingness To Accept for Medical data (WTA-M) as those participants were not willing to exchange their medical data for money. After that, we were left with 16 data points out of 37. So, we did all the processing on 16 remaining data points.

Next, we assign five answer options to WTA-M question a numerical value from 0 to 4 in the following way:

- The “nothing, online platforms can access my medical records for free.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTA-M variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTA-M variables.

To determine the relationship between privacy literacy and WTA-M, we need to see whether the privacy literacy and the WTA-M variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.816. WTA-M is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-9. Since WTA-M is not normally distributed, we decided to perform non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.139	16	.200*	.969	16	.816
WTA for medical records Ordinal	.317	16	<,001	.669	16	<,001

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-9: Normality tests for privacy literacy and the WTA for medical data

In order to check if privacy literacy and WTA-M have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.894, which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTA-M. Moreover, deviation from linearity has a significance value of 0.735 which shows that there is no non-linear relationship between the two variables either. This is shown in Figure 4-10.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTA for medical records Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	32.438	10	3.244	.579	.784
		Linearity	.109	1	.109	.019	.894
		Deviation from Linearity	32.328	9	3.592	.641	.735
	Within Groups		28.000	5	5.600		
	Total		60.438	15			

Figure 4-10: Linearity test for privacy literacy and the WTA for medical data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTA-M by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTA-M either as shown in Figure 4-11.

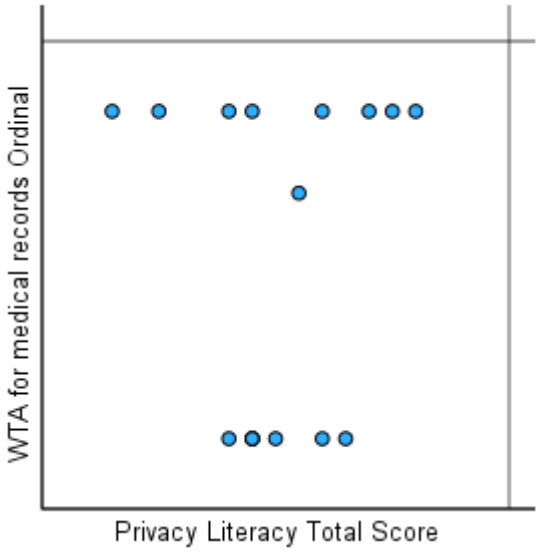

Figure 4-11: Scatter plot for privacy literacy and the WTA for medical data

We find that there is a small positive statistically non-significant correlation between privacy literacy and WTA-M as shown by Spearman's rank correlation coefficient of 0.062 and Kendall's tau correlation coefficient of 0.067. This is shown in Figure 4-12. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTA-M among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTA for medical records Ordinal	Correlation Coefficient	.067
		Sig. (2-tailed)	.757
		N	16
Spearman's rho	WTA for medical records Ordinal	Correlation Coefficient	.062
		Sig. (2-tailed)	.818
		N	16

Figure 4-12: Correlation between privacy literacy and the WTA for medical data

4.4.1.4 Privacy literacy and the willingness to accept for "personal data"

First, we removed the participants' responses "nothing, I do not want to trade my personal data in exchange for money." for the Willingness To Accept for Personal data (WTA-P) as those participants were not willing to exchange their personal data for money. After that, we were left with 17 data points out of 37. So, we did all the processing on 17 remaining data points.

Next, we assign five answer options to WTA-P question a numerical value from 0 to 4 in the following way:

- The “nothing, online platforms can access my personal data for free.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTA-P variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTA-P variables.

To determine the relationship between privacy literacy and WTA-P, we need to see whether the privacy literacy and the WTA-P variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.312. WTA-P is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-13. Since WTA-P is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.143	17	.200*	.939	17	.312
WTA for Personal Data Ordinal	.219	17	.029	.782	17	.001

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-13: Normality tests for privacy literacy and the WTA for "personal data"

In order to check if privacy literacy and WTA-P have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.241, which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTA-P. Moreover, deviation from linearity has a significance value of 0.856 which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-14.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTA for Personal Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	16.083	7	2.298	.576	.760
		Linearity	6.289	1	6.289	1.576	.241
		Deviation from Linearity	9.795	6	1.632	.409	.856
	Within Groups		35.917	9	3.991		
	Total		52.000	16			

Figure 4-14: Linearity test for privacy literacy and the WTA for "personal data"

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTA-P by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTA-P either as shown in Figure 4-15.

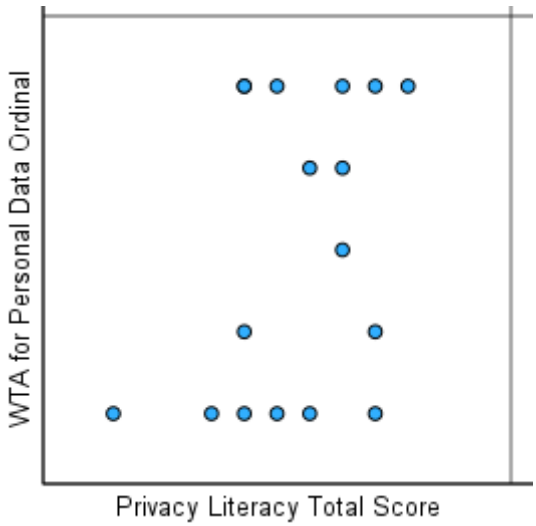

Figure 4-15: Scatter plot for privacy literacy and the WTA for "personal data"

We find that there is a small positive statistically non-significant correlation between privacy literacy and WTA-P as shown by Spearman's rank correlation coefficient of 0.308 and Kendall's tau correlation coefficient of 0.240. This is shown in the Figure 4-16. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTA-P among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTA for Personal Data Ordinal	Correlation Coefficient	.240
		Sig. (2-tailed)	.235
		N	17
Spearman's rho	WTA for Personal Data Ordinal	Correlation Coefficient	.308
		Sig. (2-tailed)	.229
		N	17

Figure 4-16: Correlation between privacy literacy and the WTA for "personal data"

4.4.1.5 Privacy literacy and the willingness to accept for web activity data

First, we removed the participants' responses "nothing, I do not want to trade my web activity data in exchange for money." for the Willingness To Accept for Web activity data (WTA-W) as those participants were not willing to exchange their web activity data for money. After that, we were left with 18 data points out of 37. So, we did all the processing on 18 remaining data points.

Next, we assign five answer options to WTA-W question a numerical value from 0 to 4 in the following way:

- The “nothing, online platforms can access my web activity data for free.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTA-W variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTA-W variables.

To determine the relationship between privacy literacy and WTA-W, we need to see whether the privacy literacy and the WTA-W variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.216. WTA-W is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-17. Since WTA-W is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.189	18	.087	.933	18	.216
WTA for Web Activity Data Ordinal	.284	18	<,001	.727	18	<,001

a. Lilliefors Significance Correction

Figure 4-17: Normality tests for privacy literacy and the WTA for web activity data

In order to check if privacy literacy and WTA-W have a monotonic relationship, first, we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.494 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTA-W. Moreover, deviation from linearity has a significance value of 0.073 which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-18.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTA for Web Activity Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	46.444	9	5.160	2.692	.089
		Linearity	.986	1	.986	.515	.494
		Deviation from Linearity	45.458	8	5.682	2.965	.073
	Within Groups		15.333	8	1.917		
	Total		61.778	17			

Figure 4-18: Linearity test for privacy literacy and the WTA for web activity data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTA-W by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTA-W either as shown in Figure 4_19.

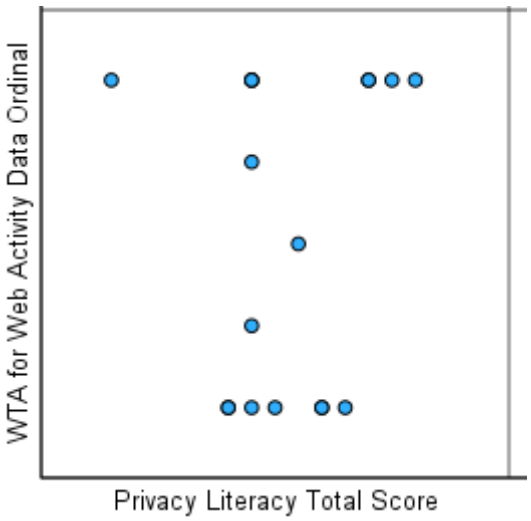

Figure 4-19: Scatter plot for privacy literacy and the WTA for web activity data

There is a small positive statistically non-significant correlation between privacy literacy and WTA-W, as shown by Spearman's rank correlation coefficient of 0.200 and Kendall's tau correlation coefficient of 0.152. This is shown in the figure... This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTA-W among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTA for Web Activity Data Ordinal	Correlation Coefficient	.152
		Sig. (2-tailed)	.448
		N	18
Spearman's rho	WTA for Web Activity Data Ordinal	Correlation Coefficient	.200
		Sig. (2-tailed)	.427
		N	18

Figure 4-20: Correlation between privacy literacy and the WTA for web activity data

4.4.2 Privacy literacy and Willingness to Pay (WTP)

In this section, we will look at the relationship between privacy literacy and willing to pay to delete each of the five data types individually.

4.4.2.1 Privacy literacy and the willingness to pay for financial data

First, we removed the participants' responses "nothing, I do not want to delete my financial data held by online platforms." for the Willingness To Pay for Financial data (WTP-F) as those participants were not willing to pay online platforms to delete their financial data. After

that, we were left with 19 data points out of 37. So, we did all the processing on 19 remaining data points.

Next, we assign five answer options to WTP-F question a numerical value from 0 to 4 in the following way:

- The “nothing, I can't afford to pay.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTP-F variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTP-F variables.

Test for the normal distribution of the privacy literacy and WTP-F variables

To determine the relationship between privacy literacy and WTP-F, we need to see whether the privacy literacy and the WTP-F variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.513. WTP-F is shown to be not normally distributed as its value of significance is 0.002. This is shown in Figure 4-21. Since WTP-F is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.145	19	.200*	.957	19	.513
WTP for Financial Data Ordinal	.210	19	.026	.813	19	.002

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-21: Normality tests for privacy literacy and the WTP for financial data

In order to check if privacy literacy and WTP-F have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.620 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTP-F. Moreover, deviation from linearity has a significance value of 0.699 which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-22.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTP for Financial Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	11.132	9	1.237	.636	.745
		Linearity	.514	1	.514	.264	.620
		Deviation from Linearity	10.618	8	1.327	.683	.699
	Within Groups		17.500	9	1.944		
	Total		28.632	18			

Figure 4-22: Linearity test for privacy literacy and the WTP for financial data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTP-F by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTP-F either as shown in Figure 4-23.

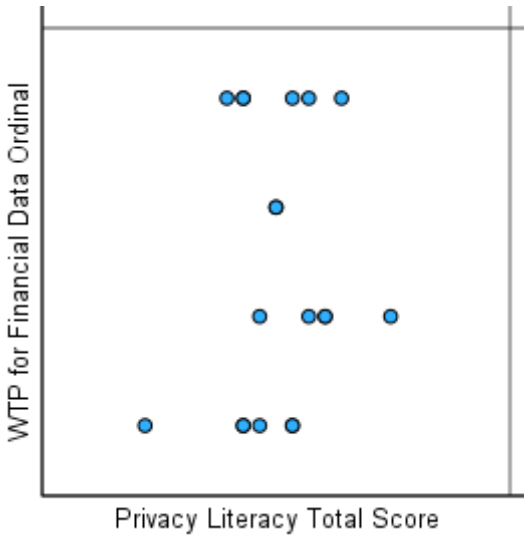

Figure 4-23: Scatter plot for privacy literacy and the WTP for financial data

We find that there is a small positive statistically non-significant correlation between privacy literacy and WTP-F as shown by Spearman's rank correlation coefficient of 0.119 and Kendall's tau correlation coefficient of 0.098. This is shown in Figure 4-24. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTP-F among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTP for Financial Data Ordinal	Correlation Coefficient	.098
		Sig. (2-tailed)	.604
		N	19
Spearman's rho	WTP for Financial Data Ordinal	Correlation Coefficient	.119
		Sig. (2-tailed)	.628
		N	19

Figure 4-24: Correlation between privacy literacy and the WTP for financial data

4.4.2.2 Privacy literacy and the willingness to pay for location data

First, we removed the participants' responses "nothing, I do not want to delete my financial data held by online platforms." for the Willingness To Pay for Location data (WTP-L) as those participants were not willing to pay online platforms to delete their location data. After that, we were left with 19 data points out of 37. So, we did all the processing on 19 remaining data points.

Next, we assign five answer options to WTP-L question a numerical value from 0 to 4 in the following way:

- The “nothing, I can't afford to pay.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTP-L variable as a result became an ordinal variable with values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTP-L variables.

To determine the relationship between privacy literacy and WTP-L, we need to see whether the privacy literacy and the WTP-L variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.505. WTP-L is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-25. Since WTP-L is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.178	19	.114	.956	19	.505
WTP for Location Data Ordinal	.222	19	.014	.795	19	<,001

a. Lilliefors Significance Correction

Figure 4-25: Normality tests for privacy literacy and the WTP for location data

In order to check if privacy literacy and WTP-L have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.809, which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTP-L. Moreover, deviation from linearity has a significance value of 0.529, which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-26.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTP for Location Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	13.921	9	1.547	.844	.598
		Linearity	.114	1	.114	.062	.809
		Deviation from Linearity	13.807	8	1.726	.941	.529
	Within Groups		16.500	9	1.833		
	Total		30.421	18			

Figure 4-26: Linearity test for privacy literacy and the WTP for location data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTP-L by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTP-L either as shown in Figure 4-27.

Figure 4-27: Scatter plot for privacy literacy and the WTP for location data

There is a small negative to zero statistically non-significant correlation between privacy literacy and WTP-L as shown by Spearman's rank correlation coefficient of -0.013 and Kendall's tau correlation coefficient of 0.000. This is shown in Figure 4-28. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTP-L among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTP for Location Data Ordinal	Correlation Coefficient	.000
		Sig. (2-tailed)	1.000
		N	19
Spearman's rho	WTP for Location Data Ordinal	Correlation Coefficient	-.013
		Sig. (2-tailed)	.956
		N	19

Figure 4-28: Correlation between privacy literacy and the WTP for location data

4.4.2.3 Privacy literacy and the willingness to pay for medical data

First, we removed the participants' responses "nothing, I do not want to delete my medical data held by online platforms." for the Willingness To Pay for Medical data (WTP-M) as those participants were not willing to pay online platforms to delete their financial data. After that, we were left with 20 data points out of 37. So, we did all the processing on 20 remaining data points.

Next, we assign five answer options to WTP-M question a numerical value from 0 to 4 in the following way:

- The “nothing, I can't afford to pay.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTP-M variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTP-M variables.

To determine the relationship between privacy literacy and WTP-M, we need to see whether the privacy literacy and the WTP-M variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.611. WTP-M is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-29. Since WTP-M is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.118	20	.200*	.963	20	.611
WTP for Medical Records Ordinal	.331	20	<,001	.687	20	<,001

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-29: Normality tests for privacy literacy and the WTP for medical data

In order to check if privacy literacy and WTP-M have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.210 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTP-M. Moreover, deviation from linearity has a significance value of 0.257, which shows that there is no non-linear relationship between the two variables either. This is shown in Figure 4-30.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTP for Medical Records Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	20.450	9	2.272	1.567	.247
		Linearity	2.598	1	2.598	1.791	.210
		Deviation from Linearity	17.852	8	2.232	1.539	.257
	Within Groups		14.500	10	1.450		
	Total		34.950	19			

Figure 4-30: Linearity test for privacy literacy and the WTP for medical data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTP-M by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTP-M as shown in Figure 4-31.

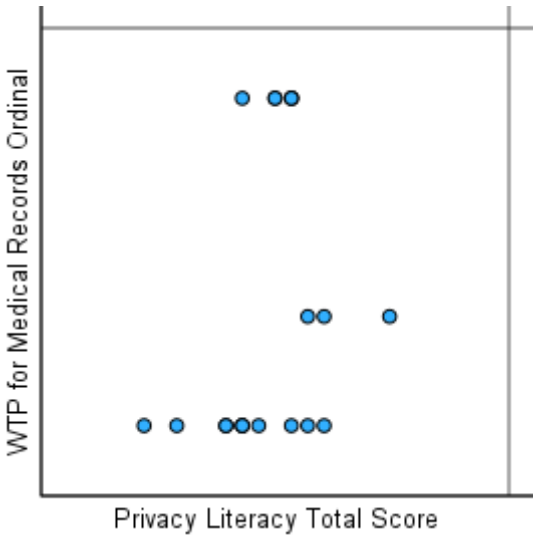

Figure 4-31: Scatter plot for privacy literacy and the WTP for medical data

There is a small positive statistically non-significant correlation between privacy literacy and WTP-M, as shown by Spearman's rank correlation coefficient of 0.375 and Kendall's tau correlation coefficient of 0.273. This is shown in Figure 4-32. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTP-M among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTP for Medical Records Ordinal	Correlation Coefficient	.273
		Sig. (2-tailed)	.151
		N	20
Spearman's rho	WTP for Medical Records Ordinal	Correlation Coefficient	.375
		Sig. (2-tailed)	.103
		N	20

Figure 4-32: Correlation between privacy literacy and the WTP for medical data

4.4.2.4 Privacy literacy and the willingness to pay for "personal data"

First, we removed the participants' responses "nothing, I do not want to delete my "personal data" held by online platforms." for the Willingness To Pay for Personal data (WTP-P) as those participants were not willing to pay online platforms to delete their personal data. After that, we were left with 22 data points out of 37. So, we did all the processing on 22 remaining data points.

Next, we assign five answer options to WTP-P question a numerical value from 0 to 4 in the following way:

- The “nothing, I can't afford to pay.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTP-P variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTP-P variables.

To determine the relationship between privacy literacy and WTP-P, we need to see whether the privacy literacy and the WTP-P variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.264. WTP-P is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-33. Since WTP-P is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.157	22	.169	.946	22	.264
WTP for Personal Data Ordinal	.274	22	<,001	.744	22	<,001

a. Lilliefors Significance Correction

Figure 4-33: Normality tests for privacy literacy and the WTP for "personal data"

In order to check if privacy literacy and WTP-P have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.082, which is statistically not significant (but still very close to being statistically significant). Hence, there might be a linear relationship between privacy literacy and WTP-P. Moreover, deviation from linearity has a significance value of 0.980, which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-34.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTP for Personal Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	11.697	9	1.300	.596	.778
		Linearity	7.868	1	7.868	3.608	.082
		Deviation from Linearity	3.828	8	.479	.219	.980
	Within Groups		26.167	12	2.181		
	Total		37.864	21			

Figure 4-34: Linearity test for privacy literacy and the WTP for "personal data"

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTP-P by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTP-P either as shown in Figure 4-35.

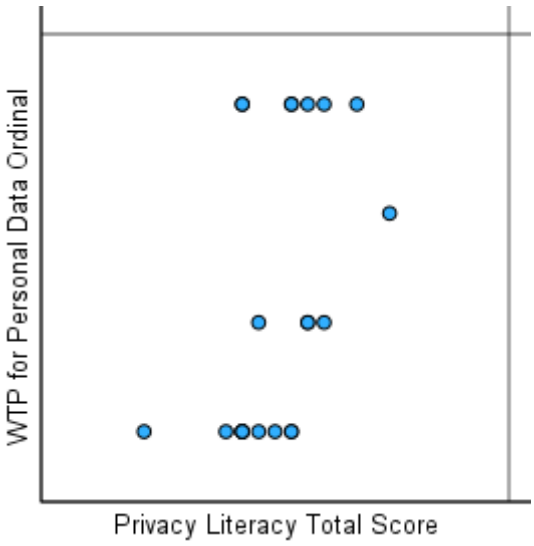

Figure 4-35: Scatter plot for privacy literacy and the WTP for "personal data"

There is a moderate positive statistically significant correlation between privacy literacy and WTP-P as shown by Spearman's rank correlation coefficient of 0.518 and Kendall's tau correlation coefficient of 0.426. This is shown in Figure 4-36. This coincides with our previous finding that there might be a linear monotonic relationship between privacy literacy and WTP-P. So, we conclude that WTP-P increases with increasing online privacy literacy among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTP for Personal Data Ordinal	Correlation Coefficient	.426*
		Sig. (2-tailed)	.017
		N	22
Spearman's rho	WTP for Personal Data Ordinal	Correlation Coefficient	.518*
		Sig. (2-tailed)	.014
		N	22

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 4-36: Correlation between privacy literacy and the WTP for "personal data"

4.4.2.5 Privacy literacy and the willingness to pay for web activity data

First, we removed the participants' responses "nothing, I do not want to delete my web activity data held by online platforms." for the Willingness To Pay for Web activity data (WTP-W) as those participants were not willing to pay online platforms to delete their web activity data. After that, we were left with 19 data points out of 37. So, we did all the processing on 19 remaining data points.

Next, we assign five answer options to WTP-W question a numerical value from 0 to 4 in the following way:

- The “nothing, I can't afford to pay.” option was assigned a value of 0.
- The “1 - 235 Rupees per month.” option was assigned a value of 1.
- The “236 - 470 Rupees per month.” option was assigned a value of 2.
- The “471 - 705 Rupees per month.” option was assigned a value of 3.
- The “706 and more Rupees per month” option was assigned a value of 4.

WTP-W variable as a result became an ordinal variable with the values, 0,1,2,3, and 4. Now, we can perform statistical analyses on both privacy literacy and WTP-W variables.

To determine the relationship between privacy literacy and WTP-W, we need to see whether the privacy literacy and the WTP-W variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.343. WTP-W is shown to be not normally distributed as its value of significance is less than 0.001. This is shown in Figure 4-37. Since WTP-W is not normally distributed, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Literacy Total Score	.152	19	.200*	.946	19	.343
WTP for Web Activity Data Ordinal	.271	19	<,001	.757	19	<,001

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-37: Normality tests for privacy literacy and the WTP for web activity data

In order to check if privacy literacy and WTP-W have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.197, which is statistically not significant. Hence, there is no linear relationship between privacy literacy and WTP-W. Moreover, deviation from linearity has a significance value of 0.195, which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-38.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
WTP for Web Activity Data Ordinal * Privacy Literacy Total Score	Between Groups	(Combined)	16.833	9	1.870	1.836	.189
		Linearity	1.979	1	1.979	1.943	.197
		Deviation from Linearity	14.854	8	1.857	1.823	.195
	Within Groups		9.167	9	1.019		
	Total		26.000	18			

Figure 4-38: Linearity test for privacy literacy and the WTP for web activity data

Furthermore, we would visually check for a monotonic relationship between privacy literacy and WTP-W by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and WTP-W either, as shown in Figure 4-39.

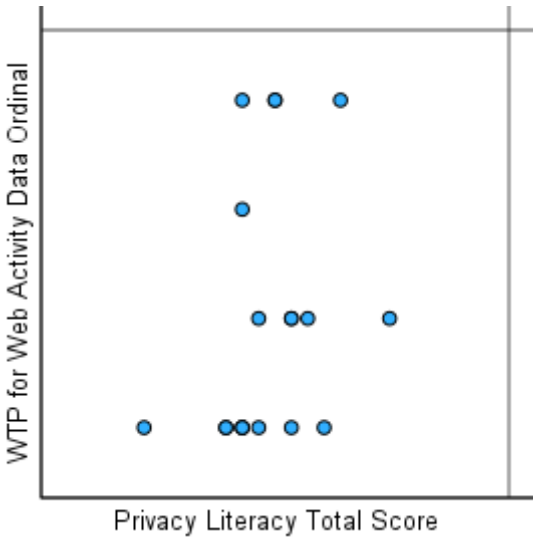

Figure 4-39: Scatter plot for privacy literacy and the WTP for web activity data

There is a small positive statistically non-significant correlation between privacy literacy and WTP-W, as shown by Spearman's rank correlation coefficient of 0.319 and Kendall's tau correlation coefficient of 0.302. This is shown in Figure 4-40. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on WTP-W among Pakistanis.

Correlations

			Privacy Literacy Total Score
Kendall's tau_b	WTP for Web Activity Data Ordinal	Correlation Coefficient	.302
		Sig. (2-tailed)	.116
		N	19
Spearman's rho	WTP for Web Activity Data Ordinal	Correlation Coefficient	.391
		Sig. (2-tailed)	.098
		N	19

Figure 4-40: Correlation between privacy literacy and the WTP for web activity data

4.4.3 Relationship between privacy literacy and privacy behaviour

Here we will determine the relationship between privacy literacy and the privacy behaviour. For privacy literacy, the sum of the correct answers given by each participant will be used as their privacy literacy score. All the calculations and analyses referring to privacy literacy will use this score. For privacy behaviour, unlike the Boerman et al, paper (Boerman et al., 2021), we will count a "never" response as a 0 and a "very often" response would be counted as a 4. So, numerically, the responses will have numerical values from 0 to 4. This is done to align

our privacy behaviour scale with our privacy literacy scale, which has an absolute zero. A "Do not know" response will still be counted as a missing response as done in the paper from which we took our privacy behaviour scale (Boerman et al., 2021). Then the average will be calculated for all the responses of an individual, excluding the "Do not know" responses, so that an individual is not penalised for the "Do not know" answers. Now our privacy behaviour scale and our privacy literacy scale will both start from 0. The privacy literacy score will range from 0 to 40 and the privacy behaviour (after taking the average) score will range from 0 to 4.

To determine the relationship between privacy literacy and privacy behaviour (our second research question), first, we need to see whether the privacy literacy and privacy behavior variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is statistically insignificant for that variable. We can see that privacy literacy variable is normally distributed as shown by the significance value of 0.365. Privacy behaviour is shown to be normally distributed as well, but by a narrow margin as the value of significance is 0.058. This is shown in Figure 4-41. Since privacy behaviour is shown to be normally distributed by a small margin, we decided to perform a non-parametric correlation analysis.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Behavior	.149	37	.038	.943	37	.058
Privacy Literacy	.117	37	.200*	.968	37	.365
Privacy Concerns	.162	37	.015	.923	37	.014

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 4-41: Normality tests for privacy literacy, privacy behaviour and privacy concerns

In order to check if privacy literacy and privacy behaviour have a monotonic relationship, first, we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.813, which is statistically not significant. Hence, there is no linear relationship between privacy literacy and privacy behaviour. Moreover, deviation from linearity has a significance value of 0.264, which shows that there is no non-linear relationship between the two variables. This is shown in Figure 4-42.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
Privacy Behavior * Privacy Literacy	Between Groups	(Combined)	4.686	11	.426	1.222	.323
		Linearity	.020	1	.020	.057	.813
		Deviation from Linearity	4.666	10	.467	1.339	.264
	Within Groups		8.714	25	.349		
	Total		13.401	36			

Figure 4-42: Linearity test for privacy literacy and privacy behaviour

Furthermore, we would visually check for a monotonic relationship between privacy literacy and privacy behaviouir by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy literacy and privacy behaviour either, as shown in Figure 4-43.

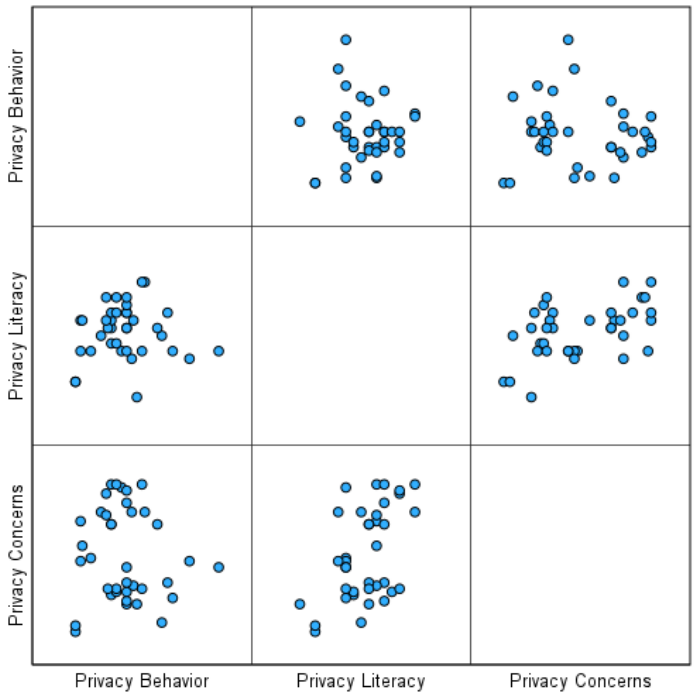

Figure 4-43: Scatter plot for privacy literacy, privacy behaviour, and privacy concerns

There is slightly positive statistically non-significant correlation between privacy literacy and privacy behavior as shown by Spearman's rank correlation coefficient of 0.031 and Kendall's tau correlation coefficient of 0.032. This is shown in Figure 4-44. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy literacy has no significant effect on online privacy protection behaviour among Pakistanis.

Correlations

			Privacy Behavior	Privacy Literacy
Kendall's tau_b	Privacy Literacy	Correlation Coefficient	.032	
		Sig. (2-tailed)	.791	
		N	37	
	Privacy Concerns	Correlation Coefficient	-.050	.325**
		Sig. (2-tailed)	.673	.007
		N	37	37
Spearman's rho	Privacy Literacy	Correlation Coefficient	.031	
		Sig. (2-tailed)	.854	
		N	37	
	Privacy Concerns	Correlation Coefficient	-.075	.440**
		Sig. (2-tailed)	.658	.006
		N	37	37

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 4-44: Correlation between privacy literacy, privacy behaviour, and privacy concerns

4.4.4 Relationship between privacy concerns and privacy behaviour

To calculate the privacy concern score of a respondent, first each privacy concern question will be assigned a numerical value, ranging from 0 to 6, where 0 would denote "Strongly Disagree" response and 6 would denote "Strongly Agree" response. Then the sum of all 8 responses to the privacy concern questions, will be the privacy concern score of a person. The privacy concern score will range from 0 to 48. This privacy concern score will be used for analysis and calculations going forward. We will calculate the privacy behaviour score in the same as we have described before (by taking the average).

To determine the relationship between privacy concern and privacy behaviour (our third research question), first, we need to see whether the privacy concerns, and privacy behaviour variables are normally distributed or not. To check for normality, we will use Shapiro-Wilk test. A variable is considered normally distributed if the result of the Shapiro-Wilk test is

statistically insignificant for that variable. We can see that privacy concerns variable is not normally distributed as shown by the significance value of 0.014. Privacy behavior is shown to be normally distributed, but by a narrow margin as the value of significance is 0.058. This is shown in the Figure 4-41. Since all of our variables are not normally distributed, we decided to use the non-parametric measures of correlation, namely Spearman's rank correlation and the Kendall rank correlation.

In order to check if privacy concerns, and privacy behavior have a monotonic relationship, first we would perform the linearity test in SPSS. The linearity shows that linearity has a significance value of 0.712 which is statistically not significant. Hence, there is no linear relationship between privacy literacy and privacy behavior. Moreover, deviation from linearity has a significance value of 0.678 which shows that there is not a non-linear relationship between the two variables either. This is shown in Figure 4-45.

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
Privacy Behavior * Privacy Concerns	Between Groups	(Combined)	7.782	23	.338	.783	.706
		Linearity	.061	1	.061	.142	.712
		Deviation from Linearity	7.721	22	.351	.812	.678
	Within Groups		5.619	13	.432		
	Total		13.401	36			

Figure 4-45: Linearity test for privacy concerns and privacy behaviour

Furthermore, we would visually check for a monotonic relationship between privacy literacy and privacy behaviour by plotting a scatter plot between the two variables. There is no visible monotonic relationship between privacy concerns and privacy behavior either as shown in Figure 4.43.

There is slightly negative statistically non-significant correlation between privacy concerns and privacy behaviour, as shown by Spearman's rank correlation coefficient of -0.075 and Kendall's tau correlation coefficient of -0.050. This is shown in Figure 4.44. This coincides with our previous finding of the absence of a monotonic relationship. So, we conclude that online privacy concern has no significant effect on online privacy protection behavior among Pakistanis.

5 Discussion

Here we will discuss the results of our study and compare them to the existing literature.

5.1 Comparison between valuations of different data types

We found that among Pakistanis financial data is valued the highest with 68.42% of the people who were willing to pay a non-zero amount out of the total respondents who were willing to pay for the financial data. This finding coincides with a finding from a previous study published in 2021 in which Jeffrey Prince and Scott Wallsten assess the WTA for different data types in different countries namely the US, Germany and four Latin American countries (Argentina, Brazil, Columbia, and Mexico). After adjusting for currency differences, they found that people value their financial information the most across countries (Prince & Wallsten, 2022).

5.2 Endowment effect

The endowment effect is observed in our study with the overall average WTP amount and the overall average WTA amount. The overall median WTA amount is greater than the overall average WTP amount, which illustrates that the endowment effect exists among Pakistani population. This finding coincides with the existing literature as it is observed in many past studies investigating the people's willingness to pay and the willingness to accept in regard to their data (Tang & Wang, 2021; Winegar & Sunstein, 2019). It manifests as the willingness to accept amount being greater than the willingness to pay amount for the same type of data and scenario (Tang & Wang, 2021; Winegar & Sunstein, 2019). This discrepancy between the willingness to pay and the willingness to accept is found in many studies, for example, In a paper published in 2021 which investigated 710 Chinese "wechat" app users about their privacy valuation found endowment effect as average willingness to accept was found to be significantly higher than the willingness to pay (Tang & Wang, 2021). Similarly, in a paper published in 2019 which surveyed 2416 Americans, demonstrated a strong endowment effect where people, on average, were willing to pay 5 USD per month for maintain their data privacy, but would demand 80 USD per month to allow access to their personal data. This results in a ratio of 1:16 between the WTP and WTA (Winegar & Sunstein, 2019).

5.3 Relationship between online privacy knowledge and online privacy valuation

There is a moderate positive statistically significant correlation between privacy literacy and WTP-P as shown by Spearman's rank correlation coefficient of 0.518 and Kendall's tau correlation coefficient of 0.426. This shows that online privacy valuation increases with increasing online privacy literacy for the "personal" data type among Pakistani population.

This finding not only answers our first research question, but it also proves our first hypothesis to be false. We can not compare this finding to any of the previous studies because the effect of online privacy knowledge on online privacy valuation has never been studied before to the best of our knowledge.

5.4 Relationship between online privacy knowledge and online privacy protection behavior

There was no significant correlation found between online privacy knowledge and online privacy protection behavior which shows that there is no relation between online privacy knowledge and online privacy protection behavior for Pakistani population. This finding not only answers our second research question, but it also proves our second hypothesis to be true. Furthermore, this finding coincides with the previous study done on 169 students in Israel which found no association between online privacy knowledge and privacy protection behavior (Weinberger et al., 2017). At the same time, our finding does not align with some other previous studies: a paper published in 2013 which showed that among 419 American adults, internet users with more privacy knowledge are more likely to exhibit privacy protection behaviour (Park, 2013) and a meta-analysis published in 2017 done on 166 studies from 34 countries which found that users who are more literate about their privacy were more likely to use privacy protective measures (Baruh et al., 2017).

5.5 Relationship between online privacy concerns and online privacy protection behaviour

There was no significant correlation found between online privacy concerns and online privacy protection behavior which shows that there is no relation between online privacy

concerns and online privacy protection behavior for Pakistani population. This finding not only answers our third research question, but it also proves our third hypothesis to be false. Furthermore, this finding does not coincide with the previous literature, a meta-analysis published in 2017 which analyzed 166 studies from 34 countries and found that users who are more concerned about their privacy were more likely to use privacy protective measures (Baruh et al., 2017).

6 Conclusion

In this thesis, we wanted to examine the effect of online privacy knowledge on online privacy protection behaviour and online privacy valuation for 5 different data types among Pakistani citizens who are residing in Pakistan. In addition, we also looked at the relationship between online privacy concern and online privacy protection behavior. For measuring online privacy knowledge, we used a modified OPLIS scale (Masur et al., 2017) in which we replaced statements about the EU and the German laws with the statements about the Pakistani laws. For measuring online privacy concerns, we chose to use the IUIPC-8 scale (Groß, 2020). For measuring privacy behavior, we used a scale proposed in 2021 (Boerman et al., 2021) which consists of ten statements, and it is assessed on a 5- point frequency scale. For data valuation, we used the willingness to pay and the willingness to accept measures for all 5 data types. The 5 data types are: financial data, location data, medical records, “personal data”, and web-activity data. The survey was conducted online using Google Forms. The survey consisted of a total of 55 questions organized into 8 different sections according to the constructs being assessed (WTP, WTA, privacy concerns, etc.). The sections were arranged on basis of the number of questions and the importance of the constructs being measured, with the section containing the more questions placed earlier in the sequence to cater for the fact that participants might get fatigued with time as they fill out the survey. We also randomized the order of the questions within a section as well as the answer choice options where

appropriate. We received a total of 42 responses over period of about 3 weeks. After data cleaning, we were left with 37 valid and complete responses only. All our analysis was done on these 37 responses. Since not all of our variables were normally distributed, we had to resort non-parametric methods of statistical analysis. Based on our analysis, we found no significant correlation between online privacy knowledge and online privacy protection behavior. We didn't find any significant correlation between online privacy concerns and online privacy behavior either. As for a relationship between online privacy knowledge and online privacy valuation, only one significant positive correlation was found between the willing to pay for the "personal data type" and online privacy knowledge, which implies that among Pakistanis, their valuation of the "personal type" of data increases with increasing online privacy knowledge. We also observed the endowment effect as the willingness to accept was higher than the willingness to pay on average.

7 Limitations and future research

Our study has a sample size of 37. So, future research on this topic should get a larger sample size. Furthermore, our survey has been done entirely in English. While English is spoken by about 49% of the Pakistani population (*Which Countries Have the Most English Speakers?*, 2017), Urdu is more widely known as it is spoken by about 75% of people living in Pakistan (*Where Is Urdu Spoken?*, 2019). So, a survey in Urdu could reach more Pakistanis than a survey in English like ours. In addition, literacy rate in Pakistan is 58% according to the World Bank (*World Bank Open Data*, n.d.). So, doing survey one-on-one with each participant, giving proper explanation where required, could give more reliable results.

8 Appendix

Master Thesis Survey

Welcome to my master thesis experiment!

The study is carried out by a master's student at the Technical University of Berlin in the Quality and Usability Lab department as a part of his master's thesis. The aim of the study is to assess how online privacy knowledge affects privacy valuation and privacy protection behaviour in Pakistanis.

The study consists of answering a questionnaire that takes about 15 to 20 minutes to complete. There are no consequences to quit the survey at any time if you wish to do so. **Answer all the questions to the best of YOUR EXISITING knowledge WITHOUT googling them or using any other sources. There are no right or wrong answers.**

Data protection information:
Data collected in this survey will only be used for scientific purposes and will only be stored anonymously. You can always request the deletion of your data using the personal code you created at the beginning of the study. If you don't remember the code, please email to sulemansamuel@protonmail.com with the subject "lost unique code". We'll send you the questions to answer to regenerate your code.
Data collected in this survey will be deleted after the completion of the master thesis. If you have any further questions or feedback, please write to sulemansamuel@protonmail.com with the subject: "about master thesis".

Thank you!

* Indicates required question

1. I have read the information on this study, and I am willing to participate in the study. *

   Mark only one oval.

   ◯ Yes

Personal Unique Code

Please follow the instructions below to create the personal code:

1. The first letter of your mother's first name:
2. The first letter of your father's first name:
3. The first letter of your place of birth:
4. The last digit of your year of birth:
5. The last digit of your birthday:

2. Please enter your personal code: *

_____

Questions about online privacy knowledge

The following questions are about your knowledge of online privacy.

3. The National Security Agency (NSA) accesses only public user data, which are visible for anyone. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

4. Social network site operators (e.g. Facebook) also collect and process information about non-users of the social network site. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

5. User data that are collected by social network site operators (e.g. Facebook) are deleted after five years. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

6. Companies combine users' data traces collected from different websites to create user profiles. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

7. E-mails are commonly passed over several computers before they reach the actual receiver. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

8. What does the term "browsing history" stand for? *

Mark only one oval.

- ◯ In the browsing history, the URLs of visited websites are stored.
- ◯ In the browsing history, cookies from visited websites are stored.
- ◯ In the browsing history, potentially infected websites are stored separately.
- ◯ In the browsing history, different information about the user is stored, depending on the browser type.

9. What is a "cookie"? *

Mark only one oval.

- ◯ A text file that enables websites to recognize a user when revisiting.
- ◯ A program to disable data collection from online operators.
- ◯ A computer virus that can be transferred after connecting to a website.
- ◯ A browser plugin that ensures safe online surfing.

10. What does the term "cache" mean? *

Mark only one oval.

- ◯ A buffer memory that accelerates surfing on the Internet.
- ◯ A program that specifically collects information about an Internet user and passes them on to third parties.
- ◯ A program, that copies data on an external hard drive to protect against data theft.
- ◯ A browser plugin that encrypts data transfer when surfing online.

11. What is a "trojan"? *

Mark only one oval.

- ◯ A trojan is a computer program, that is disguised as a useful application, but fulfils another function in the background.
- ◯ A trojan is a computer program, that protects a computer from viruses and other malware.
- ◯ A trojan is a computer program, that was developed for fun and has no specific function.
- ◯ A trojan is a computer program, that caused damage as computer virus in the 90s but doesn't exist anymore.

12. What is a "firewall"? *

Mark only one oval.

- ◯ A fallback system that will protect the computer from unwanted web attacks.
- ◯ An outdated protection program against computer viruses.
- ◯ A browser plugin that ensures safe online surfing.
- ◯ A new technical development that prevents data loss in case of a short circuit.

13. Unauthorized access, copying and transmission of any data with dishonest intention is illegal in Pakistan. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

14. Pakistan Electronic Crimes Act (PECA)... *

Mark only one oval.

- ...was passed in 2016.
- ...does not exist.
- ...is being drafted by the Pakistani parliament.
- ...solely serves as a non-committal guideline for the data protection in Pakistan.

15. Pakistani law enforcement agencies may ask residents to transfer their private data without the requirement of court warrant. *

Mark only one oval.

- True
- False
- Don't know

16. Internet service providers (ISPs) in Pakistan are obligated to retain specific traffic data for at least one year and share it with the investigative agencies upon request. *

Mark only one oval.

- True
- False
- Don't know

17. The "Dignity of man" is... *

Mark only one oval.

- ...a fundamental right of the Pakistani citizens.
- ...a philosophical term.
- ... the central claim of data processors.
- ...the central task of the National Commission for Personal Data Protection.

18. Tracking of one's own internet is made more difficult if one deletes browser information (e.g. cookies, cache, browser history) regularly. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

19. Surfing in the private browsing mode can prevent the reconstruction of your surfing behaviour, because no browser information is stored. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

20. Using false names or pseudonyms can make it difficult to identify someone on the Internet. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

21. Even though It-experts can crack difficult passwords, it is more sensible to use a combination of letters, numbers and signs as passwords than words, names or simple combinations of numbers. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

22. In order to prevent the access to personal data, one should use various passwords and usernames for different online applications and change them frequently. *

Mark only one oval.

- ◯ True
- ◯ False
- ◯ Don't know

Questions About Your Online Behaviour

The following Questions are about your behaviour while surfing the web.

23. How often do you use an ad blocker? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

24. How often do you delete cookies? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

25. How often do you decide to refrain from visiting a website because it is only accessible when you accept cookies? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

26. How often do you decline to accept cookies when website offers the choice? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

27. How often do you use the private mode in your browser? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

28. How often do you delete browser history? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

29. How often do you use opt-out websites (such as www.youronlinechoices. com) * to configure whether ads are based on personal data?

Mark only one oval per row.

	Never	Rarely	Ocassionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

30. How often do you use the “Do Not Track” function in your browser? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

31. How often do you use special software in your browser (such as Ghostery and Abine Taco) that makes it harder for companies to collect personal data? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

32. How often do you fill out wrong information about yourself (for instance, a fake name or wrong email address) when asked for such information? *

Mark only one oval per row.

	Never	Rarely	Occasionally	Often	Very Often	Do not know
Answer	◯	◯	◯	◯	◯	◯

Questions About Privacy Concerns

The following questions are about your concerns about online privacy.

33. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

34. Consumer control of personal information lies at the heart of consumer privacy. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

35. Companies seeking information online should disclose the way the data are collected, processed, and used. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

36. A good consumer online privacy policy should have a clear and conspicuous disclosure. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

37. When online companies ask me for personal information, I sometimes think twice before providing it. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

38. It usually bothers me when online companies ask me for personal information. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

39. It bothers me to give personal information to so many online companies. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

40. I'm concerned that online companies are collecting too much personal information about me. *

Mark only one oval per row.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
Answer	◯	◯	◯	◯	◯	◯	◯

Willingness to accept money in exchange for your personal data.

The following questions are about selling different types of your data to online platforms in exchange for money.

41. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access **your personal data** (e.g. your name, age, date of birth and personal registration number)?

Mark only one oval.

- ◯ 1 - 235 Rupees per month.
- ◯ 236 - 470 Rupees per month.
- ◯ 471 - 705 Rupees per month.
- ◯ 706 and more Rupees per month
- ◯ nothing, online platforms can access my personal data for free.
- ◯ nothing, I do not want to trade my personal data in exchange for money.

42. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access **your location data** (e.g. location traces collected by navigation services which reveal the daily traveling routines and places where you spent time at)?

Mark only one oval.

- ◯ 1 - 235 Rupees per month.
- ◯ 236 - 470 Rupees per month.
- ◯ 471 - 705 Rupees per month.
- ◯ 706 and more Rupees per month
- ◯ nothing, online platforms can access my location data for free.
- ◯ nothing, I do not want to trade my location data in exchange for money.

43. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access **your medical records** (e.g. data stored by health insurance companies about your individual health situations and how often you visit the doctor and for which purpose)?

Mark only one oval.

- ◯ 1 - 235 Rupees per month.
- ◯ 236 - 470 Rupees per month.
- ◯ 471 - 705 Rupees per month.
- ◯ 706 and more Rupees per month
- ◯ nothing, online platforms can access my medical records for free.
- ◯ nothing, I do not want to trade my medical records in exchange for money.

44. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access **your web activity data** (e.g. data collected by search engines like Google to create a profile about your personal interests to show relevant advertisements to you)?

Mark only one oval.

- ◯ 1 - 235 Rupees per month.
- ◯ 236 - 470 Rupees per month.
- ◯ 471 - 705 Rupees per month.
- ◯ 706 and more Rupees per month
- ◯ nothing, online platforms can access my web activity data for free.
- ◯ nothing, I do not want to trade my web activity data in exchange for money.

45. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
For what amount (in Pakistani Rupees) per month would you be willing to allow all these entities to access **your financial data** (e.g. data stored by financial services which reveal personal shopping habits and information about your financial situation)?

Mark only one oval.

- ◯ 1 - 235 Rupees per month.
- ◯ 236 - 470 Rupees per month.
- ◯ 471 - 705 Rupees per month.
- ◯ 706 and more Rupees per month
- ◯ nothing, online platforms can access my financial data for free.
- ◯ nothing, I do not want to trade my financial data in exchange for money.

Willingness to pay for the deletion of your personal data.

The following questions about paying online firms for the deletion of different types of your data from their records. Please answer as truthfully as possible.

46. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
What would you be willing to pay per month (in Pakistan Rupees) to delete all of **your personal data** (e.g. your name, age, date of birth and personal registration number) from all parties that hold it?

Mark only one oval.

- ◯ 1 - 235 Rupees per month
- ◯ 236 - 470 Rupees per month
- ◯ 471 - 705 Rupees per month
- ◯ nothing, I can't afford to pay.
- ◯ nothing, I do not want to delete my personal data held by online platforms.

47. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
What would you be willing to pay per month (in Pakistan Rupees) to delete all of **your location data** (e.g. location traces collected by navigation services which reveal the daily traveling routines and places where you spent time at) from all parties that hold it?

Mark only one oval.

- ◯ 1 - 235 Rupees per month
- ◯ 236 - 470 Rupees per month
- ◯ 471 - 705 Rupees per month
- ◯ nothing, I cannot afford to pay.
- ◯ nothing, I do not want to delete my location data held by online platforms.

48. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
What would you be willing to pay per month (in Pakistan Rupees) to delete all of **your medical records** (e.g. data stored by health insurance companies about your individual health situations and how often you visit the doctor and for which purpose) from all parties that hold it?

Mark only one oval.

- ◯ 1 - 235 Rupees per month
- ◯ 236 - 470 Rupees per month
- ◯ 471 - 705 Rupees per month
- ◯ nothing, I cannot afford to pay.
- ◯ nothing, I do not want to delete my medical records held by online platforms.

49. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
What would you be willing to pay per month (in Pakistan Rupees) to delete all of **your web activity data** (e.g. data collected by search engines like Google to create a profile about your personal interests to show relevant advertisements to you) from all parties that hold it?

Mark only one oval.

- ◯ 1 - 235 Rupees per month
- ◯ 236 - 470 Rupees per month
- ◯ 471 - 705 Rupees per month
- ◯ nothing, I cannot afford to pay.
- ◯ nothing, I do not want to delete my web activity data held by online platforms.

50. It is known that most online platforms (e.g., Facebook, Google, other digital marketers) collect user personal data. *
What would you be willing to pay per month (in Pakistan Rupees) to delete all of **your financial data** (e.g. data stored by financial services which reveal personal shopping habits and information about your financial situation) from all parties that hold it?

Mark only one oval.

- ◯ 1 - 235 Rupees per month
- ◯ 236 - 470 Rupees per month
- ◯ 471 - 705 Rupees per month
- ◯ nothing, I cannot afford to pay.
- ◯ nothing, I do not want to delete my financial data held by online platforms.

Demographic Questions

The following are some of the demographical questions about yourself.

51. Please select your gender *

Mark only one oval.

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

52. Please select your age range *

Mark only one oval.

- ◯ Below 18
- ◯ 18 - 25
- ◯ 26 - 30
- ◯ 31 - 40
- ◯ 41 - 50
- ◯ 51 - 60
- ◯ 61 and above
- ◯ Prefer not to say.

53. Please select your **personal monthly income** range *

Mark only one oval.

- ◯ None.
- ◯ Up to 50,000 Rupees per month.
- ◯ 50,001 - 100,000 Rupees per month.
- ◯ 100,001 - 200,000 Rupees per month.
- ◯ 200,001 - 300,000 Rupees per month.
- ◯ 300,001 - 500,000 Rupees per month.
- ◯ 500,001 Rupees and above per month.
- ◯ Prefer not to say.

54. Please select your nationality *

Mark only one oval.

- ◯ Pakistani
- ◯ multiple (Pakistani and other)
- ◯ Other (non-Pakistani)

55. Are you currently living in Pakistan? *

Mark only one oval.

- Yes.
- No.

---

9 Bibliography

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Aleem, Y., Tariq, M., Umar, M., Rafique, M. Z., & Ashraf, M. U. (2021). Protecting Online Privacy in Pakistan. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(6), 607–615.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bauer, C., Korunovska, J., & Spiekermann, S. (2012). On the value of information—What Facebook users are willing to pay. *Proceedings of 20th European Conference on Information Systems (ECIS 2012)*. http://aisel.aisnet.org/ecis2012/197

Beresford, A., Kübler, D., & Preibusch, S. (2010). *Unwillingness to Pay for Privacy: A Field Experiment* (SSRN Scholarly Paper 1634484). https://doi.org/10.2139/ssrn.1634484

Bernadas, J. M. A. C., & Soriano, C. R. (2018). Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy. *Journal of Information, Communication and Ethics in Society*, *17*(1), 17–30. https://doi.org/10.1108/JICES-03-2018-0025

Bhandari, P. (2020, August 12). *Ordinal Data | Definition, Examples, Data Collection & Analysis*. Scribbr. https://www.scribbr.com/statistics/ordinal-data/

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information online. *Proceedings of the 22nd International Conference on World Wide Web*, 189–200. https://doi.org/10.1145/2488388.2488406

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Donnenwerth, G. V., & Foa, U. G. (1974). Effect of resource class on retaliation to injustice in interpersonal exchange. *Journal of Personality and Social Psychology*, *29*(6), 785–793. https://doi.org/10.1037/h0036201

Downs, A. (1957). An Economic Theory of Political Action in a Democracy. *Journal of Political Economy*, *65*(2), 135–150. https://doi.org/10.1086/257897

* * (n.d.). Retrieved 11 September 2024, from https://data.imf.org/?sk=85b51b5a-b74f-473a-be16-49f1786949b3

Foa, U. G. (1971). Interpersonal and Economic Resources. *Science*, *171*(3969), 345–351. https://doi.org/10.1126/science.171.3969.345

Groß, T. (2020). *Validity and Reliability of the Scale Internet Users' Information Privacy Concern (IUIPC) [Extended Version]* (arXiv:2011.11749). arXiv. https://doi.org/10.48550/arXiv.2011.11749

Harsanyi, J. C. (1967). Games with Incomplete Information Played by "Bayesian" Players, I–III Part I. The Basic Model. *Management Science*, *14*(3), 159–182. https://doi.org/10.1287/mnsc.14.3.159

Herbert, S. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99–118.

Hu, Q., & Ma, S. (2010). Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities. *PACIS 2010 Proceedings*. https://aisel.aisnet.org/pacis2010/2

Irwin, F. W. (1953). Stated Expectations as Functions of Probability and Desirability of Outcomes. *Journal of Personality*, *21*(3), 329–335. https://doi.org/10.1111/j.1467-6494.1953.tb01775.x

Lim, S., Woo, J., Lee, J., & Huh, S.-Y. (2018). Consumer valuation of personal information in the age of big data. *Journal of the Association for Information Science and Technology*, *69*(1), 60–71. https://doi.org/10.1002/asi.23915

Loewenstein, G. (1999). Because It Is There: The Challenge of Mountaineering… for Utility Theory. *Kyklos*, *52*(3), 315–343. https://doi.org/10.1111/j.1467-6435.1999.tb00221.x

Lutz, C., & Strathoff, P. (2014). *Privacy Concerns and Online Behavior – Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses* (SSRN Scholarly Paper 2425132). https://doi.org/10.2139/ssrn.2425132

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Development and Validation of the Online Privacy Literacy Scale (OPLIS). *Diagnostica*, *63*(4), 256–268.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Nations, U. (n.d.). Specific country data. In *Human Development Reports*. United Nations. Retrieved 12 September 2024, from https://hdr.undp.org/data-center/specific-country-data

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

O'Brien, D., & Torres, A. M. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, *31*(2), 63.

O'Donoghue, T., & Rabin, M. (2001). Choice and Procrastination*. *The Quarterly Journal of Economics*, *116*(1), 121–160. https://doi.org/10.1162/003355301556365

OECD. (2013). Exploring the economics of personal data: A survey of methodologies for measuring monetary value. *OECD Digital Economy Papers*, *220*, 40.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. https://doi.org/10.1016/j.chb.2014.05.041

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms? *Journal of Economics & Management Strategy*, *31*(4), 841–861. https://doi.org/10.1111/jems.12481

Quinn, K. (2016). Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use. *Journal of Broadcasting & Electronic Media*, *60*(1), 61–86. https://doi.org/10.1080/08838151.2015.1127245

Rakhmanov, O. (2021). *A survey study on methods and techniques to measure online privacy knowledge.*

Samuelson, P. A. (1938). A Note on the Pure Theory of Consumer's Behaviour. *Economica*, *5*(17), 61–71. https://doi.org/10.2307/2548836

Savage, S., & Waldman, D. M. (2013). *The Value of Online Privacy* (SSRN Scholarly Paper 2341311). https://doi.org/10.2139/ssrn.2341311

Schmitt, V., Möller, S., & Poikela, M. (2021). Willingness to Pay for the Protection of Different Data Types. *Mensch Und Computer*.

Schwarz, N. (2012). Feelings-as-information theory. *Handbook of Theories of Social Psychology*, *1*, 289–308.

Simon, H. A. (1997). *Models of Bounded Rationality: Empirically grounded economic reason*. MIT Press.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Solove, D. J. (2020). The Myth of the Privacy Paradox. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3536265

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*, 38–47. https://doi.org/10.1145/501158.501163

Sproull, L., & Kiesler, S. (1986). Reducing Social Context Cues: Electronic Mail in Organizational Communication. *Management Science*, *32*(11), 1492–1512. https://doi.org/10.1287/mnsc.32.11.1492

Sproull, L., Kiesler, S., & Kiesler, S. B. (1991). *Connections: New Ways of Working in the Networked Organization*. MIT Press.

Staff, P. (2023, June 25). *Budget 2023-24: New Income Tax Rates for Salaried Class*. ProPakistani. https://propakistani.pk/2023/06/25/budget-2023-24-new-income-tax-rates-for-salaried-class/

Steinfeld, N. (2015). Trading with privacy: The price of personal information. *Online Information Review*, *39*(7), 923–938. https://doi.org/10.1108/OIR-05-2015-0168

Tang, Y., & Wang, L. (2021). How Chinese Web Users Value Their Personal Information: An Empirical Study on WeChat Users. *Psychology Research and Behavior Management*, *Volume 14*, 987–999. https://doi.org/10.2147/PRBM.S318139

Tönnies, F. (2012). *Studien zu Gemeinschaft und Gesellschaft*. Springer-Verlag.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 333–365). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14

Ullah, I. (2017, June 23). *First passport issued with gender-neutral 'X' option*. The Express Tribune. https://tribune.com.pk/story/1443564/historic-first-farzana-jan-gets-passport-gender-neutral-x-option

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior. *Open Information Science*, *1*(1), 3–20. https://doi.org/10.1515/opis-2017-0002

Where Is Urdu Spoken? (2019, February 26). WorldAtlas. https://www.worldatlas.com/articles/where-is-urdu-spoken.html

Which Countries Have the Most English Speakers? - K International. (2017, August 29). https://web.archive.org/web/20170829200124/http://www.k-international.com/blog/countries-with-the-most-english-speakers/

Winegar, A. G., & Sunstein, C. R. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, *42*(3), 425–440. https://doi.org/10.1007/s10603-019-09419-y

World Bank Open Data. (n.d.). World Bank Open Data. Retrieved 12 September 2024, from https://data.worldbank.org

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online Privacy Perceptions of Older Adults. In J. Zhou & G. Salvendy (Eds.), *Human Aspects of IT for the Aged Population. Applications, Services and Contexts* (pp. 181–200). Springer International Publishing. https://doi.org/10.1007/978-3-319-58536-9_16