DNB Working Paper

No 794/ November 2023

The Use of Financial Apps: Privacy Paradox or Privacy Calculus?

Hans Brits and Nicole Jonker

DeNederlandscheBank

EUROSYSTEEM

The Use of Financial Apps: Privacy Paradox or Privacy Calculus?

Hans Bits and Nicole Jonker*

* Views expressed are those of the authors and do not necessarily reflect official positions of De Nederlandsche Bank.

Working Paper No. 794

November 2023

De Nederlandsche Bank NV
P.O. Box 98
1000 AB AMSTERDAM
The Netherlands

The Use of Financial Apps: Privacy Paradox or Privacy Calculus?*

Hans Brits and Nicole Jonker

De Nederlandsche Bank (DNB), the Netherlands

November, 2023

Abstract

This paper examines whether the 'privacy paradox', i.e. a dichotomy between privacy intentions and privacy behaviours, is visible amongst users of financial services apps. Using a survey among Dutch consumers, we study to what extent people share financial data with third parties, and whether their data sharing activities are in line with their privacy concerns. We find that paradoxical usage of financial apps as measured by the privacy paradox metric is low, most users seem to make a rational calculation of benefits versus privacy risks. Paradoxical non-usage is substantial. This could be an efficiency issue, but is not a problem from a risk perspective. Regression analysis shows that app usage correlates positively with its perceived benefits and negatively with privacy risks. Furthermore, usage of certain types of apps depends on people's trust in the app providers. Overall, the results point to privacy calculating behaviour amongst the users of the data sharing apps in this study rather than to paradoxical behaviour.

Keywords: Financial apps; Consumer choice; Discrete Choice Modelling; Metric; Personal Data; Privacy Calculus; Privacy Paradox; PSD2; Westin Index

JEL classifications: C35; D12; D80; G21; G23; G28; E42; O31

* We like to thank Miquelle Marchand for her help with collecting the data. Comments by Maurice Bun, Sophie Cohen Tervaert, Carin van der Cruijsen,Willem Heeringa and Jelmer Reijerink and seminar participants at DNB are gratefully accepted. The views expressed in this paper are ours and do not necessarily reflect those of the Nederlandsche Bank or the European System of Central Bank. All remaining errors are our own.

1. Introduction

Acquisti et al. (2016) describe the privacy paradox as an ‘apparent dichotomy between privacy attitudes, privacy intentions, and actual privacy behaviours’. According to Carrière-Swallow and Haksar (2019), privacy in an economic sense can be understood as giving people the control over the personal data that they share. If people act rationally, they will weigh the privacy loss of sharing personal data against the benefits they obtain by doing this. In the case of using certain apps, these benefits are the value they obtain from the service that is provided. When people share data with a service provider, they have to take the risk into account that the data are used in unintended ways, for instance because of improper behaviour of the service provider or data leaks.

It is often mentioned that, on the one hand, consumers indicate that they consider the privacy of their personal data to be very important and, on the other hand, that they share these personal data with third parties fairly easily. There appears to be a discrepancy between stated intentions and actual behaviour, especially in online environments. Whereas unintended compromising of personal data is cause for concern, such concerns are aggravated if financial data are compromised, as this would entail not just privacy but also financial risks to consumers. Consumers appear to realize this, as they perceive financial data as very privacy sensitive (Bijlsma et al., 2023). In Europe, current and forthcoming legislation facilitates the development of online financial and information services that ask the user consent to share personal financial data with third parties. To some extent this is already happening in the Netherlands.

The aim of this paper is to examine to what extent Dutch households already share financial data with third parties, whether their data sharing activities are in line with their privacy concerns, and which factors can explain the use of financial apps that require the sharing of personal financial data.

Sharing of personal financial data has been facilited by legislation in Europe, in particular the revised Payment Services Directive (PSD2) has played a major role. This directive, that became law across Europe in 2018,[1] introduced a new type of regulated payment services: account information services. With permission of the payment service user, a third party is allowed access to the user’s payment account information to provide information services. Third party service providers can use the access to these data to build applications that offer services to their customers. They could combine payment account data with data from other sources. They could also make a combined

[1] Some countries were late, including the Netherlands (February 2019).

service offering with another type of payment service that PSD2 introduced: payment initiation. This allows the third party service provider to initiate a payment on behalf of the user, to be executed by the user's bank. Adoption of these services may have disappointed policy makers,[2] yet the number of service providers offering PSD2 services has risen considerably (Konsentus, 2023) and its use is large enough to allow a meaningful first empirical analysis based on actual app use.

In this study, we take into consideration two types of apps that require the sharing of personal financial data. The first are financial information apps, that ask users to provide financial data, and in particular access to their payments account, so that the third party service provider can provide information services to their users, based on their payment transactions. The second concerns mobile payment apps, that can be used to make payments online or offline and which give the third party service provider access to certain financial data of the user.[3] We can expect further adoption of apps processing personal financial data when service offerings improve and get wider traction. Many jurisdictions have implemented or are in the process of developing initiatives with regard to open banking and open finance which facilitate broader financial data sharing (AFM and DNB, 2022; OECD, 2023). The European Commission's proposal for a framework for Financial Data Access will provide a further stimulus by broadening access to other financial data.[4]

In November 2022 we held a survey among consumers in the Netherlands. We asked the respondents about their opinion with respect to data protection and privacy, and about their actual usage of financial information apps, mobile payment apps and – for comparison reasons - activity tracking apps in the past 12 months. Furthermore, we polled them about possible benefits and privacy risks related to using such apps. The resulting dataset allows us to assess to what extent Dutch consumers make use of financial apps and activity tracking apps, and whether they behave rationally in the sense that they weigh the possible benefits they expect to derive from using such apps against possible risks of privacy loss by sharing personal data with the app providers. We use the privacy paradox metric (PPM) developed by Gimpel et al. (2018) to assess to what extent Dutch consumers' usage of financial apps can be characterized as 'privacy paradoxical'. Furthermore, we compare the PPM-scores between people varying in general privacy attitudeaccording to a categorization, introduced by Westin.[5] In addition, we examine in more detail whether differences in general privacy attitude, differences in perceived benefits, as well as differences in perceived

[2] Keynote speech by Commissioner McGuinness at event in European Parliament 'From Open Banking to Open Finance: what does the future hold?', Brussels, 21 March 2023.

[3] In this case the third party often doesn't need a license itself, it can act as 'technical service provider' to a licensed bank.

[4] eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0360

[5] See Kumaraguru and Cranor (2005).

possible risks of privacy loss influence consumers' usage of financial apps in real life, using discrete choice regression models. Using both the PPM-methodology and discrete choice modelling allows for a better understanding of whether and how people trade the benefits and privacy risks associated with using financial apps in which they share personal financial data.

We find that that the share of app using respondents showing privacy paradoxical behaviour to be relatively small. The share of paradoxical non-users of apps is higher, especially for financial information apps. Overall, the majority of the users of financial apps seem to have made a rational choice and this also seems to hold for many users of the activity tracking app. When distinguishing between people belonging to different Westin groups, it turns out that paradoxical behaviour among app-users is relatively high among privacy fundamentalists, but is hardly observed among privacy unconcerned people. The opposite holds for paradoxical behaviour among non-users of the apps. The regression results which shed more light on the factors driving respondents' decisions show that app usage correlates positively with its perceived benefits, and negatively with privacy risks. This holds for all three types of apps in our study. Overall, the outcomes based on the PPM metric and the regression results indicate that the Dutch do not lightly engage in using apps in which they share personal data, but that they weigh up the pros and cons – consciously or not. In that sense, their choice to use a financial app seems rather be based on 'privacy calculating' than on 'privacy paradoxical' behaviour.

Our work contributes to several strands of literature. First, we add to the literature on consumers' propensity to make use of the growing possibilities that open finance may offer and we relate it to the literature on the privacy paradox. As far as we know, we are the first to study the relationship between consumers' actual usage of financial data sharing apps and the perceived benefits and privacy risks associated with using such financial apps. Papers that are closely related to ours are Chen et al. (2021), Bijlsma et al. (2023) and Rosati et al. (2022). Chen et al. (2021) combine survey and actual behavioural data of Alipay users and analyse their actual data sharing choices with third party providers of mini-programs in Alipay. They find that people with relatively strong privacy concerns authorize more data sharing with third parties than less privacy concerned users, confirming the privacy paradox. They also find that both people's privacy concerns and demand for digital services increase over time, suggesting that users develop data privacy concerns once they become more experienced. This may also explain why more active users of mini-programs are also more likely to cancel their initial consents for data sharing. Bijlsma et al. (2023) and Rosati et al. (2022) study consumers' intention to share payment account data with third parties. Bijlsma et al.

(2023) find that financial incentives and trust in the service provider correlate positively with Dutch consumers' intention to adopt account information services. Rosati et al. (2022) report a positive relationship with people's expected performance of such account information services, social influence and facilitating conditions and a negative relationship with their risk perceptions. Furthermore, they find significant cross-country differences. Van der Cruijsen (2020) examines consumers' attitudes towards the usage of their payment data. She finds that people's willingness to give third parties access to their payments data depends on the purpose of the data usage and the type of user. For example, most people support the usage of their data by their own bank to enhance security or improve services. However, they do not agree with their bank selling their data to other companies for commercial purposes.

Second, we contribute to the growing literature on the privacy paradox. The findings in the literature are mixed. For instance, the outcomes of Chen et al. (2021) described above and the results by Barth et al. (2019) support the existence of the privacy paradox. Barth et al. (2019) set up a field experiment on downloading and using a mobile phone app among technically savvy students, who are aware of privacy risks and who are provided with sufficient money to buy a paid-for app. Even under these 'extreme and ideal' conditions they find privacy paradoxical behaviour among the participants in the experiment. In their considerations for selecting and downloading apps, privacy aspects did not play a significant role, whereas functionality, app design and the costs of using the apps did. One could question whether such behaviour should be called paradoxical. In the words of the authors, 'functionality and design seem to outweigh privacy concerns' which could just as well point to rational considerations. In our study, we try to dig deeper into the considerations that steer the behaviour of app users. Athey et al. (2017) conclude from an experiment amongst MIT students that small incentives suffice to make participants relinquish their personal data. The outcomes of the longitudinal study by Dienlin et al. (2023) among a representative sample of the German population do not support the existence of the privacy paradox. Germans who are more concerned about their privacy than others are a little less inclined to share personal information about themselves online, and those who consider sharing personal information as insensible disclose substantially less information. Furthermore, they find that when an individual's privacy concerns are higher than usual, this person also shares slightly less information online than usual, and people who develop a more positive attitude towards online data sharing than usual, also share more personal data online than usual. So both between-person and within-person results do not support the existence of the privacy paradox. Gimpel et al. (2018) have developed a metric reflecting paradoxical app usage behaviour among individuals and find that paradoxical behaviour differs per type of app. Their approach takes in account criticism of Solove (2021), already mentioned by Acquisti et al. (2016) on some privacy paradox research, that compare general attitudes with respect to privacy to specific and contextual behaviour. The privacy paradox metric allows comparing specific risk considerations with regard to the use of apps that require the sharing of personal data with the benefits the respondents obtain from the use of these apps. Our study uses this metric in two different variants - one with a subjective and one with a partially objective risk measure respectively. Acquisti et al. (2016) suggest that the apparent dichotomy between privacy attitudes and actual behaviour is the result of many coexisting and not mutually exclusive different factors. In our regression analysis, we attempt to capture at least a number of these factors while also looking at their possible interrelationships.

Third, we contribute to studies using the privacy indices as developed by Alan Westin from the late 1970's. His methods of dividing consumers in 'privacy fundamentalists', 'privacy pragmatists' and 'privacy unconcerned', surveyed in Kumaraguru and Cranor (2005) still form a relatively simple but robust way of gauging general privacy concerns amongst consumers. In the context of research on the privacy paradox, it was used e.g. by Barth et al. (2019) and Schomakers et al. (2019). The outcome of the segmentation of specific samples may depend on the point in time, the group surveyed and the scale used. But roughly speaking the privacy pragmatists form the largest group, around 60-70% of the respondents, privacy fundamentalists come second with around 25-30%, and the group of privacy unconcerned is the smallest, around 10%. Outcomes in our study are within this range. Although as mentioned above, one might question whether general privacy concerns can predict behaviour in specific situations, our results show that taking into account specific privacy risks and perceived benefits, the segments do differ in actual behaviour and the use of a general privacy concern index remains of value.

And finally, we contribute to the literature on trust. Related papers are Armantier et al. (2021) and the already mentioned Van der Cruijsen (2020) and Bijlsma et al. (2023). Van der Cruijsen (2020) finds that consumers' attitudes towards payments data usage by banks depend on the purpose of data use. People do not mind if banks use their payments data to enhance security, but they are not in favour of banks using their payments data in a commercial way . If banks would sell people's payments data to other companies, this would result in a decline of their trust in banks. Armantier et al (2021) find that Americans have most trust that traditional financial institution safeguard their personal data, followed by government agencies and fintechs, and that they have least trust in bigtechs. Furthermore, they find that people from racial minorities have less trust in traditional financial institutions than white Americans, and trust in fintechs declines with age. Bijlsma et al (2023) find that Dutch consumers' intention to share their payments data with parties other than their own bank is low, and is positively related with their trust in these third parties. We find that trust in the providers of financial information apps does not correlate with the actual adoption of such apps, but trust in the providers of mobile payment and activity tracking apps does correlate positively with the actual usage of these apps. A possible explanation may be that in contrast to mobile payment apps and activity tracking apps, financial information apps are relatively new, and most people do not know these apps yet, nor their providers, resulting in low usage and a less developed notion of how well these providers can be trusted.

The remainder of the paper is organized as follows. Section 2 describes the survey design and our data. Section 3 introduces the Westin index, the privacy paradox metrics and presents and discusses the outcomes. Section 4 introduces the econometric model and the variables used to explain actual app usage, and presents and discusses the estimation results. Finally, section 5 summarizes the main findings and concludes.

2. Data and survey design

We developed a unique survey 'App usage and privacy' to gain insight to the extent Dutch consumers share financial data with third parties and their privacy preferences. We use the survey results to examine whether people's actual usage of data sharing apps is in line with the perceived benefits and possible privacy risks associated with sharing financial data with third parties, and which factors can explain the use of financial apps that require the sharing of personal financial data.

2.1 Data collection

The survey was held between 7 November and 22 November 2022 among 3,179 members of the CentERpanel aged 16 and over. In total, 2,465 panel members participated in the survey, corresponding with a response rate of 77.5%. The questionnaire was fully completed by 2,389 panel members (75.1%) and partially by 76 panel members (2.4%). In addition, we use data collected by CentERdata on demographic and psychological characteristics of the panel members. The

CentERpanel is a representative online panel of the Dutch speaking population in the Netherlands and is managed by research institute CentERdata.[6]

2.2 Survey design

2.2.1 Type of apps examined

In the survey we distinguish between two types of financial apps and activity tracking apps. The first type of financial app concerns what we describe as financial information apps. People using financial information apps give explicit consent to licensed app providers to access their payment accounts held at banks to enable them to provide a specific financial information service, for which the app providers make use of information on the account, like the balance and the transaction history.[7] Most apps in this category are budgeting apps for households, but it also includes apps that collect information from people's payment account to support the application for certain financial services, e.g. a mortgage loan application of the payment account holder. The second type of financial apps are mobile payment apps in which people give access to their payment account to initiate a payment when they make a purchase in a physical or online store using the app. We also include questions on people's usage of activity tracking apps in order to compare the results for financial apps with those for another type of app in which people share personal data.

2.2.2 App usage

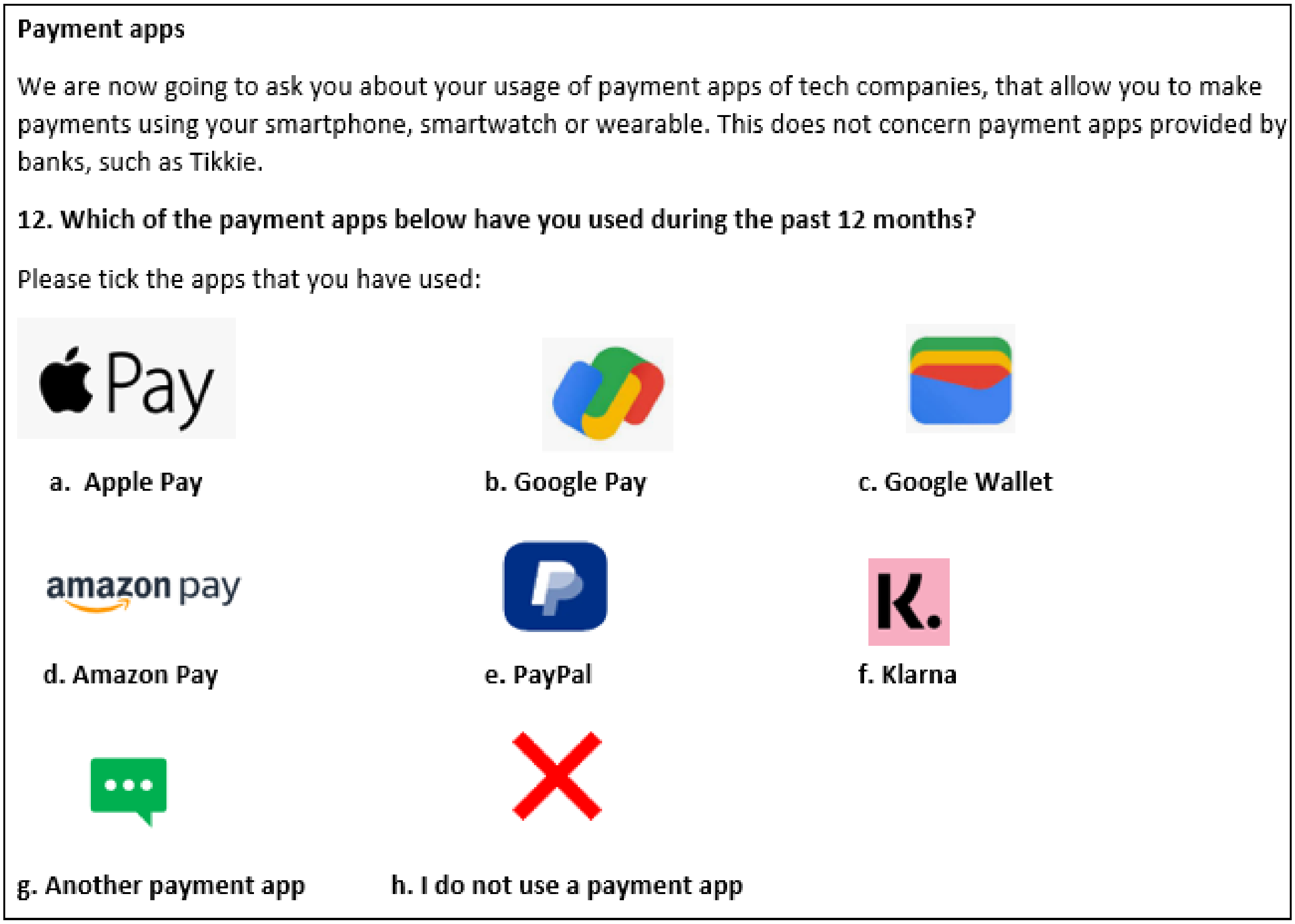
Our survey consists of several sets of questions.[8] A set of questions is on the actual usage of apps by the respondents. For each type of app, we present respondents with a list of well-known app providers, together with their app logo to increase recognisabilty and ask them which apps they used during the past 12 months. Following Gimpel et al. (2018), we only include apps which have a free version to use, in order to limit the length of the survey and to ensure homogeneity of the apps, including the business models of the app providers. Regarding mobile payment apps, we did not include the proprietary mobile payment apps provided by banks as for these apps the data is not shared with a third party. Note that respondents can use more than one app within a specific category. Therefore, they are allowed to tick more than one app. They can also indicate that they used an app that is not on the list. In that case, we ask them to provide the name of the app. Of course, it is also possible to indicate that they had not made use of such an app. Below we present an example of how we presented this question to the respondents.

[6] For more information on CentERpanel and DHS, see Teppa and Vis (2012).

[7] These service providers have a license for account information services, according to PSD2.

[8] The survey is available upon request.

Figure 1: Example question usage of mobile payment apps in the survey



Payment apps

We are now going to ask you about your usage of payment apps of tech companies, that allow you to make payments using your smartphone, smartwatch or wearable. This does not concern payment apps provided by banks, such as Tikkie.

12. Which of the payment apps below have you used during the past 12 months?

Please tick the apps that you have used:

a. Apple Pay

b. Google Pay

c. Google Wallet

d. Amazon Pay

e. PayPal

f. Klarna

g. Another payment app

h. I do not use a payment app

Table A.1 in Appendix A provides a list of the apps presented in the survey, as well as the names of other apps which were frequently mentioned by respondents.

2.2.3 Data protection and privacy

Another set of questions is on data protection and data privacy. It includes some general questions on data protection and data privacy (see also section 3.1), and questions on the privacy sensitivity of specific pieces of personal information. In addition, we ask respondents on the severity and the likelihood of several possible cases of inappropriate use of their personal data (see Table 1). On a 5 point Likert scale ranging from 1 ‘not at all threatening’ to 5 ‘extremely threatening’, we ask respondents how threatening they would consider possible privacy breaches. And for each app respondents use, we ask on a 5 point Likert scale ranging from 1 ‘very unlikely’ to 5 ‘very likely’ how

Table 1: Overview privacy violating cases of data handling

Description inappropriate data handling	In short
1. The company uses my personal information to ask me a higher price for a product than others because it sees which products I find attractive and how much I am willing to pay for them	Price discrimination
2. The company uses my personal information to have me make impulse purchases through enticing advertisements	Impulse purchases
3. The company uses my personal information without my knowledge for anything other than what I have consented to	Inappropriate data use
4. The company sells my personal data to another company, without my knowledge	Data sale
5. The company passes my personal data to government agencies, without my knowledge	Government
6. Employees of the company peek into my personal data without my permission	Inappropriate data access staff
7. People outside the company can access my personal data if the company is hacked or due to data breaches.	Data hack / breach

likely they find that a specific privacy breach would happen to them when using this app in the next 12 months.

Furthermore, we, present respondents a list of 20 types of personal data, and ask how privacy sensitive they consider these specific types of information about themselves. The respondents could report the privacy sensitivity using a 5 point Likert scale, with 1 reflecting 'not at all privacy sensitive' and 5 reflecting 'extremely privacy sensitive'. People could also indicate that a type of personal data was not applicable to them.

2.2.4 Potential benefits

In a further set of questions we ask people, for each type of app about its possible benefits for themselves, see below:

1.I think that using a(n) [name app category] app is useful in my daily live;

2. it will be easy to use the [name app category] app;

3. it can be joyful to use the [name app category] app.

The respondents could report their level of agreement on the three abovementioned statements using a 5 point Likert scale, with 1 reflecting 'complete disagreement' and 5 reflecting 'complete agreement'. The set of possible benefits are derived from Venkatesh et al. (2003) and Venkatesh et al. (2012) and were also used by Gimpel et al. (2018).

2.2.5 Trust in app providers

Furthermore, we ask respondents for each type of app to what extent they trust that, generally speaking, the providers of such apps will treat their personal data well and confidentially. We measure the level of trust using a 5 point Likert scale with 1 reflecting 'very little trust' and 5 reflecting 'a lot of trust'.

3. Observations on app use, privacy concerns and the privacy paradox

In this section we describe the preferences and behaviour of consumers with regards to the use of certain apps on their mobile phone that require the consumer to give the app provider access to personal financial and other data. For comparison, we also examine the use of a popular non-financial type of apps, that tracks the performance of the user with regard to different kind of fitness activities, like running or cycling.

3.1 General privacy concerns: the Westin-index

People differ in the degree to which they are concerned about privacy. This difference can be expected to affect the inclination to use apps that require the sharing of personal data. A way known in the literature to measure the general privacy sensitivity of the respondents is the Privacy Index developed by Westin, as surveyed in Kumaraguru and Cranor (2005)). The 'Westin index' is calculated from the answers on three survey questions. Respondents are asked on a 5-point Likert scale, with 1 reflecting 'complete disagreement' and 5 reflecting 'complete agreement', to what extent they agree with the following three statements:

1. Citizens have lost all control over how personal information about them is circulated and used by companies;

2. Most businesses handle the personal information they collect about consumers in a proper and confidential way;

3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Following the practice in earlier surveys (Kumaraguru and Cranor 2005; Barth et al. 2019; Schomakers et al. 2019 and Waldman 2020), respondents are divided into three categories:

1. Privacy fundamentalists, who consider privacy very important and do no not believe their personal data are in safe hands when shared;

2. Privacy unconcerned, who are hardly concerned about their privacy and have little problems sharing their data;
3. Privacy pragmatists, who do have some concerns but in the same time do have a certain amount of trust that their personal data are handled properly.

Table 2 shows the outcome of the Westin index for this survey. Respondents are classified as 'Privacy fundamentalist' if they agreed on question 1 and disagreed on questions 2 and 3, including respondents that answered neutral on one and only one of the questions. Respondents are classified as ' Privacy unconcerned' if they disagreed on question 1 and agreed on questions 2 and 3, including respondents that answered neutral on one and only one of the questions. The rest is classified as 'Privacy pragmatists'. We see that 30% of the respondents is classified as privacy fundamentalist, and only 8% can be considered as privacy unconcerned. Privacy fundamentalists are more numerous amongst men and people with higher education. Privacy unconcerned people are more often female and young. The outcomes are in the same ballpark as the original Westin studies, of which the most recent one dates back to 2003, see Kumaraguru and Cranor (2005). In a small sample (66) of university students with a technical background, Barth et al. (2019) found 50% privacy fundamentalists.

Table 2: Westin Privacy Index

	Privacy fundamentalists	**Privacy pragmatists**	**Privacy unconcerned**	**Number of respondents**
All respondents	30%	62%	8%	2,465
Female	24%	66%	9%	1,213
Male	35%	59%	7%	1,252
Age 15 - 24	25%	65%	10%	110
Age 25 - 34	32%	58%	10%	198
Age 35 - 44	29%	62%	8%	310
Age 45 - 55	28%	62%	9%	437
Age 55 - 64	32%	60%	8%	475
Age 65 and over	29%	64%	7%	935
Education<BA	27%	65%	8%	1,473
Education BA or MA	33%	59%	8%	988

3.2 App use and privacy sensitivity of shared data

Table 3 shows the app usage of the respondents. More than half of them use at least one of the three types of apps. Usage varies by type of app and the general privacy attitude of the respondents. Market penetration of financial information apps is still limited - about 4% of the respondents use a financial information app. Payment apps have gained considerable ground: 35% of the respondents use one or more mobile payment apps. 40% of respondents track their fitness activities with an app. Apart from financial information apps, privacy fundamentalists make least use of apps, and privacy unconcerned people the most. The share of privacy pragmatists that use apps is 2 to 3 percentage points higher than the share of privacy fundamentalists using apps. Privacy pragmatists do not seem to differ from privacy unconcerned people in their usage of financial information apps, but they make 9 to 10 percentage points less use of activity tracking respectively mobile payment apps than the latter group. The most frequently used financial information app, is the budgetting app Grip (2%) by ABN AMRO bank[9], followed by the financial information collection app Ockto (1%). The most frequently mentioned mobile payment app is Paypal (16%), followed by Apple Pay (14%) and Klarna (13%). Of the activity tracking apps the Apple Condition (7%), Apple Activity (6%), Strava (6%) and Garmin Connect (6%) apps are the most popular. The combined share of the two apps by Apple is 10%, as many respondents use both.

Table 3: Share of respondents using apps, by app type and Westin type

	Financial information app	Mobile payment app	Activity app	At least one of the three app types
All respondents	4%	35%	40%	56%
Privacy fundamentalists	5%	32%	38%	53%
Privacy pragmatists	4%	35%	40%	56%
Privacy unconcerned	4%	45%	49%	66%

Not all data that respondents may have to supply are equally privacy sensitive. Moreover, not all apps need the same amount of personal data. Table 4 lists 20 types of personal data and provides some summary statistics on their privacy sensitivity. The median and average scores indicate that respondents perceive information on their bank balance and the transactions on their bank account

[9] ABN AMRO stopped offering the Grip app shortly after the survey was held.

as the most privacy sensitive, followed by their biometrical data, their citizen service number, their debts and their income. Data about their religion, marital status, the shops where they make their purchases and their physical activities score relatively low on privacy sensitivity.

The data needs differ per type of app. We assessed which type of personal data the providers of the different financial and activity apps collect and process for their service and present the results in Table 4, in the columns headed ‘Financial information app’, ‘Mobile payment app’ and ‘Activity app’, below ‘Data needs’. A 1 indicates that the app collects such data, a ½ reflects that the app only collects a portion of the items mentioned in the data category, and a 0 indicates that the app does not collect such information. The number of different pieces of information of the app user differs per type of app. It ranges between three for activity apps to 16 for financial information collecting apps.

Table 4: Privacy sensitivity by type of information and data needs apps

		Privacy sensitivity				Data needs			
		No. of observations	median	mean	sd	Financial information app		Mobile payment app	Activity app
	Type of information					Budgetting	Information collecting		
1	**General personal data (name, birth date, address)**	2,283	3	3.33	1.19	1	1	1	1
2	**Names family members**	2,145	3	3.46	1.14	0	1	0	0
3	**Marital status**	2,151	3	2.97	1.24	0	1	0	0
4	**Citizen service number**	2,288	5	4.41	0.96	0	1	1	0
5	**Bank account number**	2,293	5	4.32	0.98	1	1	1	0
6	**Bank balance**	2,289	5	4.53	0.84	1	1	1	0
7	**Transactions bank account**	2,284	5	4.53	0.84	1	1	1/2[10]	0
8	**Monthly income**	2,284	5	4.30	0.97	1	1	0	0
9	**Mortgage**	1,390	4	3.72	1.20	1	1	0	0
10	**Rent**	1,664	4	4.03	1.06	0	1	0	0
11	**Debts (excl mortgage)**	1,424	5	4.33	0.93	0	1	0	0
12	**Pension**	2,155	4	3.86	1.10	1	1	0	0
13	**Investments**	1,234	4	4.13	1.01	0	1	0	0
14	**Tax return**	2,254	5	4.25	0.97	0	1	0	0
15	**The shops where I make purchases**	2,296	3	3.11	1.25	1	1	1	0
16	**Religion**	1,712	3	2.81	1.38	1	1	0	0
17	**Physical activities (steps, heartbeat, sleeping pattern, etc.)**	2,161	3	3.11	1.29	0	0	0	1
18	**Health (Visits GP, drug use, etc.)**	2,288	4	4.06	1.10	0	0	0	0
19	**Biometrical data (fingerprint, face, iris scan)**	2,213	5	4.42	0.97	0	0	1/2[11]	0
20	**Location data (where I've been during a day)**	2,285	4	3.86	1.14	0	0	1	1

Note: This table presents the results on the question ‘How privacy sensitive do you consider the following information about yourself?’ for 20 pieces of personal data. Respondents could choose between 1: not at all privacy sensitive, 2: a bit privacy sensitive; 3: quite privacy sensitive; 4: very privacy sensitive and 5: extremely privacy sensitive. If certain pieces of personal information did not apply, they could choose the option ‘not applicable’. The results are based on the responses of respondents for whom personal information was applicable. Table 4 also shows which pieces of personal information are collected by the apps. This information has been retrieved by the authors by checking the data collection policies of the apps.

[10] Unlike, the financial information apps, mobile payment apps only access information which is needed to perform the payment transactions initiated by its app user, and record the specific transactions made with the app.

[11] Depending on the app and the phone.

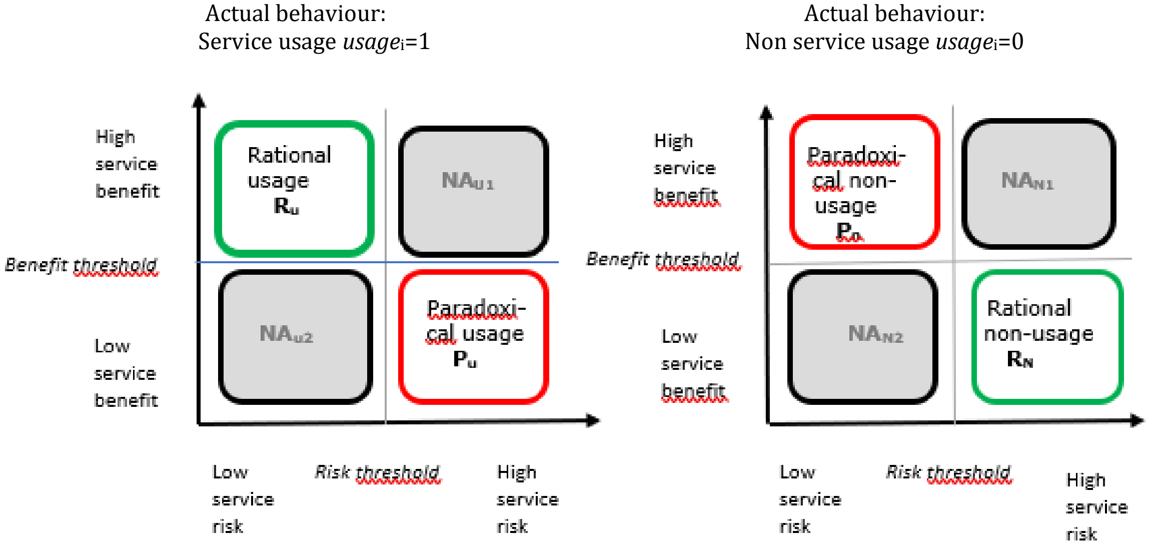
3.3 Privacy Paradox Metrics

3.3.1 Concept of the Privacy Paradox Metrics

AFM and DNB (2022), following Carrière-Swallow and Haksar (2019), define the privacy paradox in general terms as a discrepancy between the stated and the observed value individuals place on their privacy. Carrière-Swallow and Haksar (2019), Kokolakis (2017) and Solove (2021) argue that if the stated attitude towards privacy is measured in more general terms (like with the Westin Index), and the observed behaviour concerns a specific situation, such a discrepancy should not surprise and does not have to imply paradoxical or irrational behaviour. In order to investigate the existence of the privacy paradox in a more meaningful way, it is useful to tailor the measurement of privacy concerns to the specific situation related to the observed behaviour. Our survey measures two factors affecting the privacy concerns related to the use of a specific financial or non-financial app. The first factor, the 'severity factor', is the extent to which respondents would consider it a threat to their privacy if certain cases of inappropriate data handling would happen to them (see Table 1). The second factor, the 'likelihood factor', concerns the perceived likelihood that such inappropriate data handling would happen to them in the next 12 months related to the specific app(s) they actually use. People that did not make use of a certain category of apps give an estimate for the likelihood that such an incident would happen to them in the next 12 months if they would. Severity factor and likelihood factor can be combined to determine a 'privacy risk factor', specific to the use of a certain app. This risk factor can be confronted with the perceived benefits of using the app.

Gimpel et al. (2018) develop a method to confront benefits and risks of using a certain service, which they name the 'privacy paradox metric' (PPM) . We use this metric to analyse to what extent the respondents of our survey show paradoxical behaviour. There are two ways in which their behaviour could be considered paradoxical. First, an individual could use a certain app, whereas in their own perception, the risks of using the app are high, whereas the benefits are low. This would be a manifestation of the privacy paradox. Second, the other way around, an individual could refrain from using an app whereas she considers the potential benefits high and perceived risks low. This behaviour could also be called paradoxical, but is not a manifestation of the privacy paradox the way it is commonly defined. Respondents are considered to behave rationally if they use an app if benefits are considered relatively high and risks are perceived relatively low, or do not use an app in the opposite case. The calculation of the metric can lead to inconclusive results if a respondent considers both benefits and risks relatively high or low. The different possibilities are illustrated by Figure 2, which is derived from Gimpel et al. (2018).

Figure 2: Outcome distribution privacy metric calculation



Source: Gimpel et al. (2018)

3.3.2 Calculation with subjective risk measure

We follow the calculation of Gimpel et al. (2018). The benefits *Benefits_k* of using a specific category *k* of apps (i.e. financial information apps, mobile payment apps and activity tracking apps) are calculated for each respondent as the unweighted arithmetic mean of the answers to the three benefit questions (section 2.2). The median value of the benefit scores determines the *benefit_threshold* that represents the border between a high and a low benefit score. The risk of using a specific type of app is calculated, for each app a respondent uses, by averaging for each of the 7 potential cases *j* of inappropriate data handling (see Table 1) the perceived severity *Severity_risks_j* of the threat with the perceived likelihood $Likelihood\_risks\_k_j$ it could occur. Subsequently, a subjective risk score is calculated as the arithmetic average of the 7 subresults:

$Subjective\_risks\_k = {}^{1}/_{7} * \sum_{j=1}^{7}(0.5 * Severity\_risks\_j + 0.5 * Likelihood\_risks\_k_j)$. Similar to the benefit threshold, a *subjective_risk_ threshold* is determined by the median risk score, as the border between a high and a low risk score. In order to examine whether occurrence of the privacy paradox is affected by the general privacy concerns of the respondent, the overall PPM is calculated for each Westin type, as well as for the whole sample. Furthermore we calculate separate indices reflecting paradoxical usage PPM_u and paradoxical non usage PPM_n , see eqs (1a -1c).

$$PPM = \frac{P_u+P_n}{P_u+R_n+NA_{u1}+NA_{u2}+P_n+R_n+NA_{n1}+NA_{n2}} \tag{1a}$$

$$PPM_u = \frac{P_u}{P_u+R_n+NA_{u1}+NA_{u2}} \tag{1b}$$

$$PPM_n = \frac{P_n}{P_n+R_n+NA_{n1}+NA_{n2}} \tag{1c}$$

Table 5 provides an overview of the benefit and subjective risk thresholds along with some summary statistics. On average, privacy fundamentalists value the benefits of the use of apps lower than the total sample mean, and perceive the risk of the privacy threats higher. For the privacy

Table 5: Summary statistics benefit and risk scores by app category

	Benefits					
App category by Westin type	**Observations**	**Median**	**Mean**	**SD**	**Min**	**Max**
Financial information (all)	2,410	2.50	2.37	0.90	1	5
- Privacy fundamentalist	712	2.17	2.16	0.89	1	5
- Privacy pragmatist	1,504	2.67	2.44	0.89	1	5
- Privacy unconcerned	194	2.92	2.65	0.90	1	4.33
Payment (all)	2,840	3.33	3.25	1.93	1	5
- Privacy fundamentalist	836	3.00	3.03	1.24	1	5
- Privacy pragmatist	1,760	3.33	3.32	1.15	1	5
- Privacy unconcerned	244	3.67	3.57	1.90	1	5
Activity (all)	2,712	3.00	3.12	1.21	1	5
- Privacy fundamentalist	809	3.00	2.97	1.26	1	5
- Privacy pragmatist	1,677	3.00	3.15	1.18	1	5
- Privacy unconcerned	226	3.67	3.48	1.09	1	5
		Privacy threats - subjective				
Financial information (all)	2,410	3.50	3.51	0.78	1	5
- Privacy fundamentalist	712	3.93	3.88	0.73	1.29	5
- Privacy pragmatist	1,504	3.43	3.40	0.74	1	5
- Privacy unconcerned	194	3.07	3.09	0.72	1	4.93
Payment (all)	2,840	3.43	3.41	0.74	1	5
- Privacy fundamentalist	836	3.79	3.76	0.72	1.29	5
- Privacy pragmatist	1,760	3.29	3.30	0.69	1	5
- Privacy unconcerned	244	3.00	2.97	0.67	1	4.86
Activity (all)	2,712	3.36	3.38	0.73	1	5
- Privacy fundamentalist	809	3.71	3.70	0.71	1.29	5
- Privacy pragmatist	1,677	3.29	3.28	0.69	1	5
- Privacy unconcerned	226	3.00	2.95	0.65	1	4.86

Note: The benefit scores are based on average benefit scores reflecting the usefulness, ease of use and the joy respondents derive from using particular apps. The three benefits have been asked per app category. The scores for privacy threats are based on how serious respondents perceive seven different privacy threats associated with data-sharing, and on the self-assessed likelihood for each app that they use that they would become victim of such a threat during the 12 upcoming months. The risk score per app is equal to the average of the severity score and the likelihood score. For each app that respondents use the overall risk score is equal to the average risk scores of the seven individual privacy threats. Respondents who do not use a specific app type were asked for each privacy threat individually the likelihood that they would become a victim of such a privacy threat during the next 12 months if they did use such an app. For them, we constructed a risk score based on their severity scores and the likelihood scores for 'imaginary' app usage.

unconcerned, it is exactly the opposite: not just lower concern for privacy threats as might be expected, but also a higher value attached to the benefits the use of apps can bring.

As a result of the calculation, for each app category each individual observation represents either use or non-use of this type of app, a high or a low benefit score, and a high or low risk score. These results are summarized for the whole sample in Table 6.

Table 6: Perceived benefits versus subjective risks per app category

	Users		**Non-users**	
	Low risk	High risk	Low risk	High risk
Financial information				
High benefit	68.8%	11.6%	27.9%	19.4%
Low benefit	12.5%	7.1%	21.9%	30.8%
Mobile payment				
High benefit	48.7%	23.1%	11.6%	12.8%
Low benefit	18.3%	10.0%	29.1%	46.5%
Activity tracking				
High benefit	44.6%	30.6%	11.3%	14.6%
Low benefit	15.4%	9.4%	33.5%	40.6%

Note: The results have been calculated using the overall median scores for benefits and risks by app type.

According to our calculations, the percentages of app using respondents showing the privacy paradox in their behaviour are relatively small (PPM$_{u}$, marked in red). For app users that need to share financial data, somewhat more than 7% uses the app whereas they perceive benefits to be relatively low and risks high. For mobile payment and activity apps, which use less sensitive data, the percentage is a bit higher but not higher than 10%. The majority of financial app users appears to make a rational calculation: benefits for them are relatively high, risks relatively low.

Percentages of paradoxical non-use of apps (PPM$_{n}$, marked in orange) are higher, especially for financial information apps. This could be due to the relatively slow overall market take-up of these apps. These apps are still relatively new and unknown. Even if people think they could benefit from their use, they probably need to know more or see more use amongst peers to actually start using them. This being said, also large percentages of non-users seem to make a rational decision: for them risks are relatively high and benefits low. It should be noted that by taking the median risk and benefit scores, the respondents are categorized as perceiving respectively benefits and costs high or low relative to half of the group. Different ways of determining the dividing thresholds are possible, like taking the mean scores or by setting the minimum necessary value of the benefits and the maximum acceptable risk of app use at socially desirable levels. The data do not allow for individual comparisons of absolute values of benefits and privacy costs, which make these alternative thresholds hard to interpret.

Looking more closely at the group behaving paradoxically, we can differentiate per Westin type, to examine the effect of the general privacy concerns of respondents. The results are presented in Table 7. We observe the privacy paradox amongst app users PPM_u (column 1) the most amongst privacy fundamentalists. 12-18% of app users who consider privacy very important and do no not believe their personal data are in safe hands when shared, use the app despite perceiving benefits low relative to privacy risks. On the other hand, amongst the privacy unconcerned we hardly observe the privacy paradox. This group perceives the risks to their privacy lower and is more upbeat about benefits, resulting in little paradoxical behaviour in the use of the app.

For non-users (column 2), like we noted earlier, paradoxical behaviour as presented by PPM_n in the sense of not using an app although benefits seem to outweigh costs in general is higher than amongst users. Looking at the Westin types, this kind of paradoxical behaviour is relatively low amongst privacy fundamentalists. In contrast, this kind of paradoxical behaviour is high among privacy unconcerned people, as relatively high percentages of privacy unconcerned respondents do not use the app although they do think benefits are relatively high and risks low. As we said before, the market penetration of these apps, and financial information apps in particular, is still at an early stage, which will explain a large part of paradoxical non-use.

Table 7: Share of respondents that behave paradoxically by app category and Westin type – subjective risk scores

App category by Westin type	(1) PPM_u	(2) PPM_n	(3) PPM
Financial information (all)	7.1%	27.9%	27.0%
- Privacy fundamentalist	12.5%	13.4%	13.3%
- Privacy pragmatist	5.6%	32.7%	31.4%
- Privacy unconcerned	0%	44.3%	42.3%
Mobile payment (all)	10.0%	11.6%	10.8%
- Privacy fundamentalist	18.4%	5.6%	11.6%
- Privacy pragmatist	7.7%	13.1%	11.9%
- Privacy unconcerned	1.4%	24.8%	11.1%
Activity tracking (all)	9.4%	11.3%	10.4%
- Privacy fundamentalist	14.7%	5.7%	9.8%
- Privacy pragmatist	7.8%	12.9%	10.5%
- Privacy unconcerned	4.7%	21.7%	11.9%

Note: The results have been calculated using the overall median scores for benefits and risks by app type.

Column 3 shows the overall measure of paradoxical behaviour, the PPM, which reflects the share of all people who behave paradoxically. The largest percentages of paradoxical behaviour are found with regards to the financial information apps, which can again be attributed to the low overall use of these apps. Paradoxical behaviour is on average the highest amongst privacy unconcerned.

3.3.3 Calculation with partially objective risk measure

The calculation of the privacy metrics above compares subjective individual measures of benefits and risks. As such, it is a measure of individual consistency. Another way of looking at a possible privacy paradox is to compare the perceived benefits of app use with a more objective measure of the risks to privacy that the respondents expose themselves to. Our questionnaire lists 20 types of personal data that app users may need to share (see table 2 in sub-section 2.2.3). For each type of app, it is determined from their user policies whether users have to provide these data in order to use the app (value 1) or not (value 0). These (objective) values are weighted by the (subjective) privacy sensitivity of these type of personal data, that the respondent has indicated on a 5-point Likert-scale.

Table 8 provides an overview of the ‘objective’ risk thresholds and summary statistics. As with the subjective risk scores, we observe the highest average risk scores with the privacy fundamentalists, and the lowest with the privacy unconcerned respondents.

Table 8: Summary statistics objective risk scores by app category and Westin type

	Privacy threats – objective					
App category by Westin type	Observations	Median	Mean	SD	Min	Max
Financial information (all)	2,336	2.25	2.21	0.56	0.03	3.25
• Privacy fundamentalist	698	2.40	2.37	0.53	0.45	3.25
• Privacy pragmatist	1,450	2.20	2.16	0.56	0.03	3.25
• Privacy unconcerned	188	2.13	2.06	0.54	0.10	3.25
Mobile payment (all)	2,762	1.43	1.37	0.29	0.13	1.75
• Privacy fundamentalist	821	1.50	1.46	0.25	0.30	1.75
• Privacy pragmatist	1,703	1.40	1.34	0.30	0.13	1.75
• Privacy unconcerned	238	1.30	1.28	0.28	0.20	1.75
Activity tracking (all)	2,631	0.50	0.50	0.15	0.05	0.75
• Privacy fundamentalist	795	0.55	0.55	0.15	0.10	0.75
• Privacy pragmatist	1,617	0.50	0.48	0.15	0.05	0.75
• Privacy unconcerned	219	0.45	0.44	0.14	0.15	0.75

Note: The scores for privacy threats are based on which data types app providers collect, and how privacy sensitive respondents have assessed these data types. The objective privacy threat score equals the sum of the assessed privacy sensitivity of all data types collected by the app, divided by 20 (the number of data types respondents were asked to rate). The objective privacy threat score of the financial information app is based on the scores for the budget apps and the Ockto app.

This objective risks measure is compared with the same benefits score as was used for the calculation in sub-section 3.3.2. The results are given in Table 9. Calculated in this way, the privacy metric shows somewhat higher scores for paradoxical behaviour, in particular for the users of financial information apps. These apps ask for a relatively large amount of privacy sensitive data. 11.6% of the users score their benefits relatively low whereas the objective privacy risk score is

Table 9: Perceived benefits versus objective risks per app category

	Users		**Non-users**	
	Low risk	High risk	Low risk	High risk
Financial information				
High benefit	47.3%	33.0%	26.6%	20.8%
Low benefit	8.0%	11.6%	24.9%	27.8%
Mobile payment				
High benefit	39.4%	32.4%	12.9%	11.5%
Low benefit	16.0%	12.3%	37.8%	37.8%
Activity tracking				
High benefit	44.1%	31.1%	14.8%	11.1%
Low benefit	15.4%	9.4%	41.6%	32.6%

Note: The results have been calculated using the overall median scores for benefits and risks by app type.

relatively high.It must be noted however that the use of these kind of apps is low. But also for mobile payment apps, the observed paradoxical behaviour is somewhat higher compared to the privacy metrics calculation with the subjective risk measure. For activity apps, the result is the same. The data that are shared for these apps, including those related to physical activities, are considered less privacy sensitive. The percentages of rational behaviour observed – either users with a low risk score and high perceived benefits or non-users with a high risk score and low perceived benefits – are lower compared to the calculations with the subjective risk measure. Still the percentages are relatively high, in particular for users.

Again, we examine the effect of the general privacy concerns of respondents, as measured by the Westin index, on the outcome of the privacy metrics now using the objective risk scores. The results are presented in Table 10. The resulting picture is comparable to the calculations by Westin type using the subjective risk scores in Table 7. In general, paradoxical behaviour observed amongst users (column 1) is lowest for the privacy unconcerned, and highest among the privacy fundamentalists. For financial information apps privacy pragmatist users show even slightly higher paradoxical behaviour than privacy fundamentalists, but as said more often, the number of observations is small. Paradoxical non-use (column 2) is highest amongst privacy unconcerned for all three types of apps. Differences between the three Westin types in overall paradoxical behaviour as measured by the PPM (column 3) are relatively small, with the exception of a lower relative number of privacy fundamentalists showing paradoxical behaviour with regard to financial information apps.

Table 10: Share of respondents that behave paradoxically by appcategory and Westin type – objective risk scores

App category by Westin type	(1) PPM_u	(2) PPM_n	(3) PPM
Financial information (all)	11.6%	26.6%	25.9%
- Privacy fundamentalist	12.5%	16.9%	16.7%
- Privacy pragmatist	12.7%	30.4%	29.5%
- Privacy unconcerned	0%	33.0%	31.4%
Mobile payment (all)	12.3%	12.9%	12.6%
- Privacy fundamentalist	20.2%	6.3%	12.8%
- Privacy pragmatist	10.4%	15.7%	13.0%
- Privacy unconcerned	2.8%	17.8%	9.0%
Activity tracking (all)	9.4%	14.8%	12.2%
- Privacy fundamentalist	13.6%	10.0%	11.6%
- Privacy pragmatist	8.4%	16.1%	12.5%
- Privacy unconcerned	3.9%	24.7%	12.8%

Note: The results have been calculated using the overall median scores for benefits and risks by app type.

4. Regression analysis

In this section we present the results of a regression analysis, which attempts to explain actual app use from factors including its perceived benefits, the privacy value of the data shared, the perceived risks that these data could be misused, the perceived chance that these risks would materialize, and the trust in the app providers. All in all, the estimation results should give a richer insight on the influence of benefits and risks of data sharing on the observed use and non-use of apps compared to the privacy paradox metrics.

4.1 Regression models and variables

4.1.1 Dependent variables

For the analysis on app usage we use three dependent variables App_{ik}, one for each type of app. Index i identifies the respondent and index *k* the type of app, with k=1 referring to financial information apps, k=2 to mobile payment apps and k=3 to activity apps. App_{ik} equals 1 if respondent i used app type k in the past 12 months and equals 0 if not.

4.1.2 Explanatory variables

We use the respondent specific dummy variables *Privacy* f*undamentalist* and *Privacy pragmatist* - referring to the type of Westin category respondents belong, to assess the influence of differences in general privacy attitudes on the actual usage of the three types of apps. The reference category are the *privacy unconcerned* people.

We use several explanatory variables related to perceived benefits and perceived privacy risks to explain actual app usage. *Benefits_k* equals the average value of the three potential benefits - usefulness, ease of use and joyfulness – associated with using app type k. *Benefits_k* is a continuous variable whose value can range between 1 and 5, with higher values reflecting higher levels of perceived benefits. For financial information apps, we take the average of the benefits associated with budgeting apps and the financial information collecting apps. *Sensitivity_k* is a continuous variable which equals the sum of the privacy sensitivity assessments by the respondent for the types of personal information handled by app type k (see Table 2). For normalization reasons, the sum is divided by 20, the number of information items listed in Table 2. The value of *Sensitivity_k* can range between 3/20, if a user of an activity app assesses the privacy sensitivity of all three information items handled by the app as ‘not at all privacy sensitive’, to 4, if a user of a financial information app assesses the privacy sensitivity of all 16 information items handled by the app as ‘extremely privacy sensitive’. *Severity_risks* is a continuous variable which is equal to the average of the severity of seven possible cases of inappropriate handling of personal data collected by apps, as perceived by the respondent. It is a continuous variable whose value can range between 1 and 5, with higher values reflecting increasing severity. The variable *Likelihood_risks_k* equals the average value of the perceived likelihood according to the respondent that (s)he will become victim of the seven possible cases of inappropriate data handling when using app type k in the upcoming 12 months. It is a continuous variable whose value can range between 1 and 5, with higher values reflecting higher perceived likelihoods of becoming victim of inappropriate data handling. By including *Severity_risks a*nd *Likelihood_risks_k* we can assess the impact of both the perceived severity and the perceived probability of becoming victim of a privacy risk associated with app usage.

The variable *Trust_k* reflects how much trust the respondent has that, in general, providers of an app (type k) will treat her personal data properly and confidentially. For both users and non-users of an type k app, we use the answer on the question of how much trust the respondent in general has that providers of app type k would treat her personal data properly and confidentially. The value of *Trust_k* ranges between 1 and 5, with increasing values reflecting higher levels of trust.

Furthermore, we include a standard set of explanatory variables reflecting the demographic characteristics of the respondents in all regressions. The variables include gender, age, educational level, net personal monthly income, whether a respondent lives in a rental or own house (proxy wealth), the urbanisation degree and the region of the respondent’s residence. The reference person is a privacy unconcerned woman, between 16 and 34 years old, with at most an intermediary educational level, a net monthly income ranging between EUR 1,001 and EUR 2,000, living in a rental home, located in the Western part of the Netherlands.

4.1.3 The regression models

We use a series of probit models to assess which factors influence respondents’ actual usage of data sharing apps App_{ik}. We estimate separate discrete choice models for the three types of apps, i.e. 1) financial information apps App_{i1}, 2) mobile payment apps App_{i2} and 3) activity apps App_{i3}.

We distinguish between the observed actual usage of app type k by respondent i in the past 12 months App_{ik}, and the underlying unobserved latent willingness to have done so App_{ik}^{*}. In the baseline model we assume that respondent's i latent willingness App_{ik}^{*} depends on her demographic characteristics x_i and an error ε_{ik}:

$$App_{ik}^{*} = \beta_k{}' x_i + \varepsilon_{ik} \tag{2}$$

The observed actual usage of app type k App_{ik} is related to the latent willingness of respondent i to have used app type k App_{ik}^{*}:

$$\begin{aligned} App_{ik} &= 1 \ \ if \ App_{ik}^{*} > 0 \\ &= 0 \ \ if \ App_{ik}^{*} \leq 0 \end{aligned} \tag{3}$$

We then have

$$Pr(App_{ik} = 1) = Pr(\beta_k' x_i + \varepsilon_{ik} > 0) = \Phi(\beta_k' x_i) \tag{4}$$

$$Pr(App_{ik} = 0) = Pr(\beta_k' x_i + \varepsilon_{ik} \leq 0) = 1 - \Phi(\beta_k' x_i)$$

The previous section 4.1.2 provides an overview of the variables included in x_i. We estimate separate discrete choice models, one for each type of app. We assume that ε_{ik} is from the standard normal distribution, with zero mean and standard deviation $\sigma_k = 1$. For a detailed description of the probit model, see e.g. Cameron and Trivedi (2010).

The maximum likelihood function of the probit model that we use to estimate β_k in the baseline model is as follows:

$$L_k = \sum_{i=1}^{N} \left[App_{ik} ln\Phi\big(\beta_k^{\prime}\ x_i\big) + (1 - App_{ik}) ln\left(1 - \Phi\big(\beta_k^{\prime}\ x_i\big)\right)\right] \tag{5}$$

As our analysis takes place at respondent level and not on household level, we cluster the standard errors by household to take potential correlation across members of the same household into account.

In the second step of our analysis, we assess the influence of differences between people in general privacy attitude on app usage. We include the dummies *Privacy fundamentalist* and *Privacy pragmatist* in our set of explanatory variables (reference: Privacy unconcerned), so that the argument in (2) becomes:

$$\beta_k' x_i + \gamma_k Privacy\ fundamentalist_i + \widetilde{\gamma_k} Privacy\ pragmatist_i \tag{6}$$

Subsequently, we add in (2) the continuous variables *Benefits_k, Sensitivity_k, Severity_risks* and *Likelihood_risks_k*

$$\beta_k' x_i + \delta_k Benefits\_k_i + \vartheta_k\ Sensitivity\_k_i\ + \theta_k\ Severity\_risks_i\ +\ \tilde{\theta}_k Likelihood\_risks\_k_i \tag{7}$$

to asses whether perceived benefits and privacy risks of using app type k influences respondents' actual usage of this type of app. Then, we add in (2) the continuous variable $Trust\_k$

$$\beta_k' x_i + \tau_k Trust\_k_i \tag{8}$$

so that we can examine the influence of trust in the providers of app type k that they will treat respondent's personal data properly and confidentially on actual app usage.

Lastly, we include the full set of explanatory variables

$$\beta_k' x_i + \gamma_k Privacy\ fundamentalist_i + \widetilde{\gamma_k} Privacy\ pragmatist_i + \delta_k Benefits\_k_i + \\ \vartheta_k\ Sensitivity\_k_i\ + \theta_k\ Severity\_risks_i\ +\ \tilde{\theta}_k Likelihood\_risks\_k_i\ + \tau_k Trust\_k_i \tag{9}$$

4.2 Regression results

4.2.1 Full sample

Table 11 shows the results of the probit regressions explaining app usage for the three types of apps for the full sample. The outcomes of the baseline regressions with respondents' demographics as explanatory variables are presented in columns 1, 6 and 11, the Westin type variables reflecting respondents' general privacy attitude are included in the second model and its outcomes are presented in columns 2, 7 and 12, the third model includes the variables reflecting respondents' perceived benefits, privacy sensitivity of the data and privacy risks associated with inappropriate data handeling and its results are shown in columns 3, 8 and 13. The fourth model includes respondents' trust that app providers will treat their personal data properly and confidentially and its results can be found in columns 4, 9 and 14. The results for the full model are presented in columns 5, 10 and 15.

In general, the likelihood that someone uses a data sharing app correlates with her general privacy attitude. People who care a lot about their data privacy, - the privacy fundamentalists - are 11 percentage points (column 7) less likely to make use of mobile payment apps and 9 percentage points (column 12) less likely to make use of activity apps than privacy unconcerned people – the reference group. The difference in app usage between privacy pragmatists and privacy unconcerned people is smaller, but still significant. Privacy pragmatists are 7 percentage points (columns 7 and 12) less likely to use mobile payment and activity apps than privacy unconcerned people. People's general privacy attitude does not correlate significantly with the likelihood of using a financial information app (column 2). The difference in mobile payment and activity app usage between privacy pragmatists and privacy unconcerned people disappears (columns 7 vs 10 and 12 vs 15) once we control for respondents' perceived benefits, privacy risks and trust in app providers. The likelihood that privacy pragmatists use financial information apps may even become higher than for privacy unconcerned people (columns 2 vs 5). For privacy fundamentlists this holds for all three types of apps (columns 2 vs 5, 7 vs 10 and 12 vs 15). A possible interpretation of the latter finding may be that once controlled for differences in perceived benefits and risks privacy fundamentalists actually are more likely to use data sharing apps than others. People who differ in general privacy attitude, also differ in their assessment of privacy risks associated with app usage and their trust in app providers. These findings may be in line with the relatively higher share of paradoxical app usage among privacy findamentalists, and to a lesser extent among privacy pragmatists, than among privacy unconcerned respondents.[12]

Perceived benefits associated with app usage correlate positively and significantly with app usage. However, the magnitude of the effects varies by the type of app.[13] The marginal effect of a 1 unit increase in perceived benefits associated with financial information app usage increases the likelihood of app usage by 4 percentage points (column 3), whereas a 1 unit increase in perceived benefits associated with mobile payment app or activity tracking app usage raises the likelihood of app usage by 14 respectively 17 percentage points (columns 8 and 13).

Both privacy sensitivity of the data shared with app providers and the self assessed likelihood of becoming victim of inappropriate data handling correlate negatively and significantly with app usage. By how much depends again on the type of app. To illustrate, the marginal effect of a 1 unit increase in the self assessed chance of becoming victim lowers the likelihood of financial information app usage by 2 percentage points (column 3), of mobile payment app usage by 10 percentage points (column 8) and of activity tracking app usage by 7 percentage points (column 13). The marginal effects of privacy sensitivity of the data on the likelihood of app usage are almost similar to that of the self-assessed likelihood of becoming victim of inappropriate data handling, except for the activity app, where the marginal effect of privacy sensitivity is higher than of the self-

[12] The change in estimated effects for general privacy attititude may be due to multicollineairy, even though the Variance Inflation Factor (VIF) of the explanatory variables do not suggest that. There is a moderate correlation between 0.2 and 0.3 between people's general privacy attitude, their assessment of privacy risks associated with app usage and their trust in app providers. The average VIFs for the full models range between 1.75 and 1.80, and the maximum VIFs for privacy attitude range between 3.35 and 3.74. As a rule of thumb a VIF above 10 indicates high correlation, but there are also authors who suggest a more conservative level, like 5 (Menard, 2001) or 2.5 (Johnston et al., 2018).

[13] As a robustness check, we tested for possible endogeneity between perceived benefits of app usage and actual app usage. The results are presented in section 4.3.

assessed likelihood of becoming victim of a inappropriate data handling. In contrast to our expectations, the severity of the impact of inappropriate data handling on someone's privacy does not correlate significantly with the likelihood of financial information app usage (column 3) and correlates significantly and positively with mobile payment app usage (column 8) and activity app usage (column 13).[14]

Trust in the app provider matters. The effect of trust is lowest for financial information apps. The marginal effect of a 1 unit increase in trust increases the likelihood of using a financial information app by 3 percentage points (column 4), a mobile payment app by 16 percentage points (column 9) and an activity app by 20 percentage points (column 14).

The impact of trust in app providers disappears (financial information apps, columns 4 vs 5) or strongly decreases (mobile payment and activity apps, columns 9 vs 10 and 14 vs 15) in the full model. This may be due to the positive correlation between perceived benefits of app usage and trust that app providers will treat personal customer data properly and confidentially. Mutual inclusion of both variables reduces the estimated effect of trust. The main results of the variables reflecting benefits and risks associated with app usage are unchanged. The size of the impact of benefits on the likelihood of using a mobile payment or activity app decreases a few percentage points, as well as the size of the impact of the privacy sensitivity of the data on the likelihood of activity app usage (columns 8 vs 10 and 13 vs 15). The reduced effect of perceived benefits on the likelihood of app usage is probably due to the inclusion of trust in the full model. The reduced effect is surprising, as trust should relate more to the security and well functioning of apps than to potential benefits.[15] The results of the severity of privacy risks and the likelihood of becoming victim do not change for any of the apps.

Regarding the demograhic characteristics of the respondents, we find several significant relationships with app usage. For instance, app usage correlates negatively with respondents' age and positively with their income. Gender matters too, how depends on the type of app. Males are

[14] As a sensitivity check for the results presented in Tables 6 and 7 on PPM based on benefits and subjective risks of app usage, we also used a subjective risk measure only based on the perceived likelihood of becoming victim of inappropriate data handling, because of the unexpected result for the severity of the impact of inappropriate data handling one someone's privacy. The results are presented in Tables A.4 and A.5 in the Appendix. The main results are robust to this adjustment in the risk indicator.

[15] The correlations between perceived benefits of app usage and trust in app providers range between 0.6 for activity and mobile payments apps and 0.7 for financial information apps. The results suggest that when examining the impact of trust in the provider of a service on its usage, one should also take into account potential benefits of the service in order to avoid omitted variable bias.

Table 11: Probit estimations usage data sharing apps

	Financial information apps					Mobile payment apps					Activity apps				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
	Base-line	Westin types	Benefit + risks	Trust	Full model	Base-line	Westin types	Benefit +risks	Trust	Full model	Base-line	Westin types	Benefit + risks	Trust	Full model
Privacy fundamentalist		0.01			0.05***		-0.11***			0.08**		-0.09**			0.05***
Privacy pragmatist		0.01			0.03*		-0.07**			0.02		-0.07*			0.01
Benefit			0.04***		0.04***			0.14***		0.11***			0.17***		0.15***
Privacy sensitivity			-0.01*		-0.02*			-0.10***		-0.09**			-0.19***		-0.15**
Severity risks			0.01		0.01			0.03**		0.03***			0.04***		0.04***
Likelihood risks			-0.02***		-0.02***			-0.10***		-0.09***			-0.07***		-0.07***
Trust				0.03***	0.00				0.16***	0.06***				0.20***	0.05***
Male	0.02**	0.02**	0.02**	0.02**	0.02**	0.00	0.01	-0.00	0.01	-0.00	-0.05**	-0.05**	-0.02	-0.03	-0.02
Age: 35 - 44	-0.02	-0.02	-0.01	-0.01	-0.01	-0.09***	-0.09**	0.01	-0.03	0.02	-0.09**	-0.09**	-0.02	-0.02	-0.01
Age: 45 - 54	-0.01	-0.01	0.00	0.01	0.00	-0.15***	-0.15***	-0.05	-0.09***	-0.04	-0.10***	-0.10***	-0.02	-0.03	-0.01
Age: 55 - 64	-0.04***	-0.04***	-0.02	-0.02	-0.02	-0.29***	-0.29***	-0.13***	-0.20***	-0.12***	-0.21***	-0.20***	-0.06*	-0.09**	-0.05
Age: 65 and older	-0.05***	-0.05***	-0.01	-0.02	-0.01	-0.42***	-0.41***	-0.22***	-0.30***	-0.20***	-0.27***	-0.27***	-0.08***	-0.12***	-0.07**
Education bachelor and higher	-0.01	-0.01	-0.00	-0.01	-0.00	-0.02	-0.02	-0.02	-0.02	-0.02	0.06***	0.06***	0.03*	0.06***	0.03*
Income: EUR 0 - 1,000	-0.03*	-0.03*	-0.03**	-0.03*	-0.03**	-0.05*	-0.04*	-0.02	-0.04	-0.03	-0.08***	-0.08***	-0.06***	-0.07***	-0.06***
Income: >= EUR 2001	0.02**	0.02**	0.01	0.02*	0.01	0.05**	0.05**	0.01	0.03	0.01	0.08***	0.08***	0.03	0.05**	0.03
Homeowner	-0.01	-0.01	-0.01	-0.01	-0.01	-0.01	-0.02	-0.01	-0.02	-0.01	0.07***	0.07***	0.04*	0.07***	0.05**
Degree urbanisation	0.01*	0.01*	0.00	0.01**	0.00	0.00	0.00	0.01	0.01	0.01	0.00	0.00	0.00	0.01	0.00
Region east	-0.01	-0.01	-0.01	-0.01	-0.01	-0.06**	-0.06**	-0.04*	-0.05**	-0.04*	0.01	0.01	0.01	0.02	0.01
Region north	-0.01	-0.01	-0.01	-0.01	-0.01	-0.04	-0.04	-0.02	-0.03	-0.02	-0.04	-0.04	-0.01	-0.02	-0.01
Region south	-0.01	-0.01	-0.02	-0.01	-0.01	-0.02	-0.02	-0.01	-0.02	-0.01	-0.02	-0.02	0.02	0.02	0.02
Log likelihood	-365.9	-365.7	-285.9	-348.6	-281.2	-1,314.9	-1,309.8	-1011.3	-1,210.4	-1,000.0	-1,440.4	-1,437.4	-1,1477.2	-1,298.2	-1,139.7
Pseudo R^2	0.07	0.07	0.21	0.12	0.22	0.10	0.10	0.27	0.17	0.28	0.05	0.06	0.25	0.15	0.25
No. of obs	2,257	2,257	2,246	2,257	2,246	2,270	2,270	2,112	2,270	2,112	2,256	2,256	2,255	2,256	2,255

Note: The table presents the average marginal effects of probit estimations. E.g. 0.02 for male in column 1 means that males are 2 percentage points more likely than females to use a financial information app. In columns 1 - 5 the dependent variable is a dummy equal to 1 if the respondent uses a financial information app (budgeting app or the Ockto app) and equals zero otherwise. In columns 6 – 10 the dependent variable is a dummy equal to 1 if the respondent uses a mobile payment app and equals zero otherwise and in columns 11-15 the dependent variable is a dummy equal to 1 if the respondent uses an activity app and equals zero otherwise. The reference person is a privacy unconcerned female, aged between 16 – 34 with an educational level below bachelor degree, a middle income (net personal monthly income between EUR 1001 – 2000), who does not own a house and lives in the Western part of the Netherlands. ***, ** and * denote statistical significance at the 0.01, 0.05, and 0.10 level, respectively. Standard errors are clustered at household level.

more likely than females to use financial information apps, whereas females are more likely than males to use activity apps.[16] Home owners (proxy for wealth) and people with at least a bachelor degree are more likely to use activity apps than others. Some of these variables correlate with perceived benefits, privacy sensitivity, privacy risks or trust in app providers, as the size and significance of the effects become smaller once we control for these attributes.

4.2.2 Results by Westin type

We also estimated separate regression models by Westin type. This allows us to assess the influence of perceived benefits, privacy sensitivity of the data handled by apps and subjective privacy risks on app usage by Westin type (see Table 12). In addition, results by Westin type will not be affected by any possible multicollinearity between people's general privacy attitude with other explanatory variables.

Overall, the main results presented in Table 11 also hold for the three Westin types. Irrespective of people's general privacy atititude, the likelihood that they use an app correlates positively with the perceived benefits and negatively with the perceived likelihood of becoming victim of inappropriate data handling. However, there are also a few differences. The effect of privacy sensitivity of the data shared on app usage is larger among privacy pragmatists and privacy unconcerned people than among privacy fundamentalists. This also holds for trust in the providers of mobile payment apps and activity tracking apps. Furthermore, in contrast to the other two Westin types, privacy unconcerned people seem to react relatively strong on the likelihood of becoming victim of inappropriate data handling. This indicates that even though the name of their group may suggests otherwise, these people do take privacy risks into account when deciding to use an app or not.

[16] Using survey data for 28 countries Chen et al. (2023) find that women are significantly less likely to use products offered by fintech companies than men. The gender gap narrows down significantly if they include controls for respondents'attitudes towards new financial technology, the suitability of products to respondents' lifestyle, and their willingness to use attractively priced products offered by fintech entrants. Armantier et al. (2021) find that women are more concerned about the implications of data-sharing for their privacy and personal safety than men, but Chen et al. (2023) do not find support this explains the gender gap.

Table 12: Probit estimations app usage by app and Westin type

	Privacy fundamentalists		Privacy pragmatists		Privacy unconcerned		Privacy fundamentalists		Privacy pragmatists		Privacy unconcerned	
	(1) Baseline + benefit + risks	(2) Full model	(3) Baseline + benefit+ risks	(4) Full model	(5) Baseline+ benefit + risks	(6) Full model	(7) Baseline + benefis + risks	(8) Full model	(9) Baseline + benefit+ risks	(10) Full model	(11) Baseline + benefit + risks	(12) Full model
App type	Financial information		Financial information		Financial information		Mobile payment		Mobile payment		Mobile payment	
Benefit	0.04***	0.04**	0.04***	0.03***	0.04**	0.05***7	0.13***	0.13***	0.14***	0.11***	0.11***	0.09***
Privacy sensitivity	-0.00	-0.00	-0.01	-0.01	-0.13**	-0.12**	-0.05	-0.04	-0.11**	-0.09*	-0.19	-0.20*
Severity risks	0.02*	0.02*	-0.00	0.00	0.03**	0.03**	0.01	0.02	0.03*	0.03**	-0.03	-0.02
Likelihood risks	-0.02***	-0.02***	-0.02***	-0.02***	-0.03**	-0.03***	-0.09***	-0.08***	-0.10***	-0.09***	-0.15***	-0.15***
Trust		-0.01		0.01		-0.04**		0.02		0.09***		0.05
Demographic[17] controls	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Log likelihood	-80.1	-79.9	-174.8	-174.3	-11.0	9.8	-267.9	-267.5	-644.0	-633.46	-77.3	-76.7
Pseudo R^2	0.31	0.31	0.21	0.22	0.52	0.57	0.33	0.33	0.25	0.26	0.37	0.37
Number of observations	672	672	1,395	1,395	180	180	631	631	1,306	1,306	176	176

	(13) Baseline + benefit + risks	(14) Full model	(15) Baseline + benefit+ risks	(16) Full model	(17) Baseline + benefit + risks	(18) Full model
Appp type	Activity		Activity		Activity	
Benefit	0.18***	0.18***	0.17***	0.13***	0.19***	0.17***
Privacy sensitivity	-0.15	-0.14	-0.22***	-0.17**	-0.08	-0.02
Severity risks	0.06***	0.07**	0.03**	0.04***	0.01	0.02
Likelihood risks	-0.05***	-0.04***	-0.08***	-0.07***	-0.14***	-0.13***
Trust		0.01		0.08***		0.06
Demographic controls	yes	yes	yes	yes	yes	yes
Log likelihood	-310.0	-309.9	-732.9	-723.6	-88.1	-87.5
Pseudo R^2	0.31	0.31	0.22	0.23	0.30	0.31
Number of observations	674	674	1,400	1,400	182	182

Note: The table presents the average marginal effects of probit estimations by app type and by Westin type. The standard errors are clustered at household level. The dependent variables are dummies which equal 1 if the respondent uses a financial information app, a mobile payment app, respectively an activity tracking app, and is zero otherwise. The reference person is a female, aged between 16 – 34 with an educational level below bachelor degree, a middle income (net personal monthly income between EUR 1001 – 2000), who does not own a house and lives in the Western part of the Netherlands. ***, ** and * denote statistical significance at the 0.01, 0.05, and 0.10 level, respectively.

[17] Due to estimation problems using the full set of demograhic covariates, we excluded degree of urbanization and the region dummies in the set of covariates.

4.3 Robustness checks

We have conducted several robustness checks for the regressions on the usage of financial information apps.

As a first robustness check, we employ two alternative specifications for our estimations on financial information app usage. In the first alternative version (1a) we increase the weight of budgetting apps from 50% to 75% and lower the weight of financial information collection apps from 50% to 25% in the variables reflecting respondents' perceived benefits, privacy sensitivity, subjective privacy risks associated with app usage and trust in app providers, and re-estimate equations 7 - 9. The adjusted weights reflect the share of the two types of financial information apps among the users of these two types of apps in the sample. The results are presented in Table A.3, columns 3 - 5 in Appendix A. We compare the outcomes with the results presented in Table 11, columns 3 - 5. This allows us to examine whether our initial results are sensitive to the weights given to the two types of financial information apps.

Overall, the results suggest that the main conclusions for the relationship between perceived benefits, privacy risks and trust in the app provider on financial information app usage are robust to the usage of alternative weights for the variables related to budgetting and financial information collection apps. Regarding people's general privacy attitude, we find in the re-estimated equation (9) that the influence of being a privacy pragmatist instead of a privacy unconcerned person remains unaltered, and that the influence of being a privacy fundamentalist is reduced by 1 percentage point. Furthermore, the estimated marginal effects of the benefit variables and the three privacy risks variables (privacy sensitivity, severity and likelihood becoming victim) are the same as in the regressions using equal weights. The estimated effects of trust in the app provider are also unaffected. This also holds to a large extent for the re-estimated equation 7.

In the second alternative version (1b), we explain the usage of budgetting apps, instead of financial information apps and re-estimate equations 5 - 9 only using information on perveived benefits, privacy sensitivity, subjective privcy risks and trust associated with budgetting apps. This alternative specification allows us to test whether the initial outcomes are driven by the combination of two different types of financial information apps. We present the results in Table A.3, columns 6 - 10 and compare them with the outcomes in Table 11, columns 1- 5.

Overall, the results are in line with the outcomes for both types of financial information apps. Looking at the re-estimated equation (6) we see that the effects of people's general privacy attitude have not changed. In the re-estimation of equation (9) the estimated marginal effect of being a privacy pragmatist instead of a privacy unconcerned person does not change, and the marginal effect of being a privacy fundamentalist is reduced by 1 percentage point to +4 percentage points. Regarding benefits and privacy risks in equation (7), we see that the marginal effect of a 1 unit increase in perceived benefits on app usage is reduced by 2 percentage points to +2 percentage points, and that the marginal effects of the three privacy risk variables do not change. For equation (8) we find that the impact of trust in app providers is reduced by 1 percentage point to +2 percentage points and for equation (9) we again find that trust in app providers does not correlate significantly with budgetting app usage.

As a second robustness check, we test for two possible sources of endogeneity. The first one concerns possible endogeneity between perceived benefits of app usage with app usage and the second one concerns possible endogeneity between trust in the providers of apps with app usage. People's perceptions about the benefits associated with a specific type of app may change once they make use of it. If that is the case, perceived benefits of the users may not be predetermined and correlate with the error term, leading to biased estimates. Something similar may be the case with people's trust in the providers of specific apps. We re-estimate equations (7) and (8) for all three types of apps using instrumental variables for perceived benefits and trust. As instruments for perceived benefits of financial information apps, we use perceived benefits of mobile payment apps and activity tracking apps, as instruments for perceived benefits of mobile payment app usage, we use the perceived benefits of financial information and activity app usage, and analogously, for the perceived benefits of activity tracking apps usage, we employ perceived benefits of financial information and mobile payment app usage as instruments. We use a similar approach for the selection of instruments for trust in app providers. For example, as instruments for trust in the providers of financial information apps, we use trust in the providers of mobile payment and activity trackings apps. Subsequently, we perform Wald tests of the exogeneity of the instrumented variable. The results are presented in Table A.6 in the appendix. The null hypotheses of no endogeneity of perceived benefits and trust in the providers of apps are not rejected for financial information apps and mobile payment apps, indicating that perceived benefits and trust in the providers of financial information and mobile payment apps do not suffer from endogeneity bias. However, the Wald tests reject the no endogeneity hypotheses for perceived benefits associated with using activity tracking apps (χ^2=7.57; p=0.006) and trust in the providers of activity tracking apps (χ^2=13.59; p=0.000). Based on the re-estimated IV-probit equations, the marginal effect of a 1 unit increase in perceived benefits associated with using an activity tracking app amounts to 18 percentage points (+ 1 percentage point compared to the marginal effect presented in Table 11). The marginal effect of a 1 unit increase in trust in the providers of activity tracking apps increases by 3 percentage points and becomes 23 percentage points. Both re-estimated marginal effects are significant at the 1% level. The outcomes indicate that endogeneity of benefits and trust in app providers is not an issue in the regressions explaining the usage of the two types of financial apps, and that the main results for the activity tracking app are quite robust.

5 Discussion and conclusions

In Europe, but also elsewhere in the world, legislation facilitates the development of online financial information services that ask the user consent to share personal financial data with third parties. A potential concern is that, on the one hand, people indicate that they consider the privacy of their personal data to be very important, but on the other hand, that they seem to share these personal data with third parties fairly easily. So there may be a discrepancy between people's stated intentions and their actual behaviour. This phenomenon is known as the privacy paradox.

We study to what extent Dutch households share personal financial data with third parties other than their own bank, and whether their actual data sharing behaviour may be characterised as paradoxically or not. For this purpose, we collected information about the usage, the perceived benefits and privacy risks associated with using two types of financial apps, - financial information apps and mobile payment apps - and activity tracking apps, for comparison.

Our results show that 4% of our respondents made use of financial information apps in the past 12 months, which is much lower that their usage of mobile payment apps (35%) and activity tracking apps (40%). So, the uptake of financial information apps is (still) relatively low compared to the usage of mobile payment apps and activity tracking apps.

We find that paradoxical usage of the two types of financial apps is low (7-12%), as well as the paradoxical usage of the activity tracking app (9%). In contrast, paradoxical non-usage is substantial, especially for financial information apps (28%).

Using Westin's characterisation of people's general privacy attitude, we observe the privacy paradox amongst app users is the highest amongst privacy fundamentalists and the lowest amongst privacy unconcerned people. The latter group perceives privacy risks lower and is more upbeat about the benefits, resulting in little paradoxical behaviour in their usage of data sharing apps. Amongst non-users paradoxical behaviour is lowest amongst the privacy fundamentalists and the highest amongs the privacy unconcerned people.

Using discrete choice regression techniques we find that people take both perceived benefits, privacy sensitivity of the data shared and perceived privacy risks into account when deciding to use a data sharing app. This holds for all three types of apps we consider in this study. It suggests that the Dutch do not lightly engage in using apps in which they share personal (financial) data, but that they weigh up the pros and cons. In that sense, their choice to use a data sharing app seems rather be based on 'privacy calculating' than on 'privacy paradoxical' behaviour.

The size of the effects differs per app type. We find relatively small effects of benefits, privacy sensitivity of the data and perceived privacy risks associated with financial information app usage compared to mobile payment app and activity tracking app usage. This might be due to the fact that usage of financial information apps is still fairly low, as they are relatively new on the market. Many people may not be not familiar with the possible benefits and privacy risks of these types of apps yet, in contrast to mobile payment and activity tracking apps. Finally, the results also suggest that trust in the app provider is an important driver behind people's decisions to give a provider access to their personal data.

The results by Westin type show that all three categories of people take perceived benefits and privacy risks into account in their decisions to use a data sharing app or not. They mainly differ in their assessments of the level of perceived risks, privacy sensitivity of the data and benefits of app usage.

Overall, our results show that there is no excessive paradoxical usage of financial data sharing apps in the Netherlands, but there may be an underuse. In order to enable consumers to make adequate choices, they need to be well informed about the possibilities of apps and about the risks associated with app usage. App providers, consumer organizations and financial regulators have a role here.

References

Acquisti, A, Taylor, C., and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 52(2), 442-492.

AFM and DNB, (2022). Data Mobility and the Financial Sector – Discussion Paper. Available at: Data Mobility and the Financial Sector (dnb.nl).

Armantier, O., Doerr, S., Frost, J., Fuster A. and Shue (K.) (2021). Whom do consumers trust their data? US survey evidence. BIS bulletin 42. Available at: Whom do consumers trust with their data? US survey evidence (bis.org)

Athey, S., Catalini, C. and Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. NBER Working Paper 23488. Available at: The Digital Privacy Paradox: Small Money, Small Costs, Small Talk (nber.org).

Barth, S., De Jong, M.D.T., Junger, M., Hartel, P.H. and Roppelt, J.C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematic and Informatics*, 41, 55-69.

Bijlsma, M., van der Cruijsen, C. and Jonker, N. (2023). Not all data are created equal – Data sharing and privacy. *Applied economics* (forthcoming).

Cameron, A.C., and Trivedi, P.K. (2010). Micoeconometrics using Stata, Revised edition, Texas: Stata Press.

Carrière-Swallow, Y. and Haksar, V. (2019). The economics and implications of data: an integrated perspective. Strategy, Policy and Review Department, 19/16.

Chen, L., Huang, Y., Ouyang, S., and Xiong, W. (2021). The data privacy paradox and digital demand. NBER Working Paper 28854. Available at: The Data Privacy Paradox and Digital Demand | NBER.

Chen, S., Doerr, S., Frost, J., Gambacorta, L. and Shin, H.S. (2023). The fintech gender gap. *Journal of Financial Intermediation*. 54, article 101026.

Cruijsen, C. van der (2020). Payments data: do consumers want banks to keep them in a safe or turn them into gold? *Applied Economics.* 52(6), 609 – 622.

Dienlin, T., Masur, P. and Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, 25(5), 1043 – 1064.

Gimpel, H., Kleindienst, D. and Waldmann, D. (2018). The disclosure of private data: measuring the privacy paradox in digital services. *Electronic Markets*, 28, 475-490.

Johnston R., Jones K. and Manley D. (2018). Confounding and collinearity in regression analysis: a cautionary tale and an alternative procedure, illustrated by studies of British voting behaviour. *Quality & Quantity,* 52(4), 1957-1976.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computer & Security*, 64, 122-134.

Konsentus (2023). Q1 2023 Third Party Provider Open Banking Tracker | Konsentus.

Kumaraguru, P. and Cranor, L.F. (2005). Privacy indexes: A survey of Westin's studies. Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, CMU-ISRI-5-138.

Menard S. (2001). Applied Logistic Regression Analysis. 2nd edition. Thousand Oaks, CA: SAGE Publications, Inc.

OECD (2023). Shifting from Open Banking to Open Finance (oecd-ilibrary.org).

Rosati, P., Fox, G., Cummins, M. and Lynn, T. (2022). Perceived Risk as a Determinant of Propemsity to Adopt Account Information Servcies under the EU Payment Services Directive. *Journal of Theoretical and Applied Electronic Commerce Research*, 17, 493 – 506.

Schomakers, E.-V., Lidynia, C., and Ziefle, M. (2019). A typology of online privacy personalities. *Journal of Grid Computing*, 17, 727-747.

Solove, D.J. (2021). The myth of the privacy paradox. *George Washington Law Review*, 89(1), 1-51.

Venkatesh, V., M.G. Morris, F.D. Davis and Davis, G.B. (2003), User acceptance of Information Technology: Toward a unified view, *MIS Quarterly,* 27(4), 425-478.

Venkatesh, V., Thong, J. and Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly,* 36(1), 157-178.

Waldman, A.E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 105-109.

Appendix A

Table A.1: Overview apps, by app category

	Mobile payment apps	Financial information apps	Activity apps
1	Amazon Pay	Buddy payment	Apple Activity
2	Apple Pay	Dyme	Apple Conditie
3	Google Pay/Wallet	Flow your Money	Fitbit
4	Paypal	Grip	Garmin connect
5	Klarna	iBilly	Google Fit
6	Afterpay/Riverty*	Mijn geldzaken	Ommetje lopen
7		Ockto	Runkeeper*
8		Spendle	Samsung health*
9		Spendee	Stappenteller (android)
10			Stappenteller (iOS)
			Strava

Note: the name of the apps without a * have been presented by name in the survey. The apps marked with a * were not, but have have been mentioned by several respondents.

Table A.2: Summary statistics demograhpic variables and other covariates

Covariates	Obervations	Average	Standard deviation	Min	Max
Privacy fundamentalist	2,465	0.30	0.46	0	1
Privacy pragmatist	2,465	0.62	0.48	0	1
Privacy unconcerned	2,465	0.08	0.27	0	1
Benefits: financial information app	2,419	2.37	0.90	1	5
Benefits: mobile payment app	2,437	3.12	1.20	1	5
Benefits: activity app	2,414	2.99	1.20	1	5
Privacy sensitivity: financial information app	2,406	2.62	0.49	0.63	3.75
Privacy sensitivity: mobile payment app	2,406	1.44	0.28	0.35	2.10
Privacy sensitivity: activity app	2,406	0.54	0.16	0.15	0.90
Severity risks	2,445	3.78	0.83	1	5
Likelihood risks: financial information app	2,381	3.26	1.11	1	5
Likelihood risks: mobile payment app	2,240	3.17	1.09	1	5
Likelihood risks: activity app	2,389	3.02	1.08	1	5
Trust : financial information app	2,419	2.06	0.75	1	5
Trust: mobile payment app	2,436	2.58	0.88	1	5
Trust: activity app	2,414	2.39	0.85	1	5
Male	2,465	0.51	0.50	0	1
Age: 16 - 34	2,465	0.12	0.33	0	1
Age: 35 - 44	2,465	0.13	0.33	0	1
Age: 45 - 54	2,465	0.18	0.38	0	1
Age: 55 - 64	2,465	0.19	0.39	0	1
Age: 65 and older	2,465	0.38	0.49	0	1
Education: less than bachelor	2,461	0.60	0.49	0	1
Education bachelor and higher	2,461	0.40	0.49	0	1
Income: EUR 0 - 1,000	2,346	0.21	0.41	0	1
Income: EUR 1,001 – 2,000	2,346	0.54	0.50	0	1
Income: >= EUR 2, 001	2,346	0.25	0.43	0	1
Homeowner	2,465	0.72	0.45	0	1
Degree urbanisation	2,448	3.10	1.33	1	5
Region west	2,448	0.42	0.49	0	1
Region east	2,448	0.22	0.41	0	1
Region north	2,448	0.12	0.33	0	1
Region south	2,448	0.24	0.43	0	1

Source: CentER panel: November 2022.

Note: Summary statistics of demograhpic variables of all 2,465 respondents and variables related to financial information apps, mobile payment apps and activity app which have been used as explanatory variables in the regression analyses.

Table A.3: Robustness check 1: Sensitivity probit estimations financial information apps

	Check 1a: change weights budgeting and financial information collection app					Check 1b: budgeting apps only				
	(1) Baseline	(2) Westin types	(3) Benefit + risks	(4) Trust	(5) Full model	(6) Baseline	(7) Westin types	(8) Benefit +risks	(9) Trust	(10) Full model
Covariates										
Privacy fundamentalist		0.01			0.04***		0.01			0.04***
Privacy pragmatist		0.01			0.03*		0.01			0.03***
Benefits			0.03***		0.04***			0.02***		0.02***
Privacy sensitivity			-0.02*		-0.02*			- 0.01		-0.02
Severity risks			0.01		0.01			0.01		0.01
Likelihood risks			-0.02***		-0.02***			-0.02***		-0.02***
Trust				0.03***	-0.00				0.02***	0.00
Demographic covariates	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Log likelihood	-365.9	-365.7	-285.5	-351.7	-281.8	-270.4	-270.1	-225.8	-259.3	-222.5
Pseudo R^2	0.07	0.07	0.21	0.11	0.22	0.07	0.07	0.20	0.10	0.22
Number of observations	2,257	2,257	2,246	2,257	2,246	2,327	2,327	2,247	2,290	2,247

Note: The table presents the average marginal effects of probit estimations. In columns 1 - 5 the dependent variable is a dummy equal to 1 if the respondent uses a financial information app (budgeting app or the Ockto app) and equals zero otherwise. In columns 6 – 10 the dependent variable is a dummy equal to 1 if the respondent uses a budgetting app and equals zero otherwise. The reference person is a privacy unconcerned female, aged between 16 – 34 with an educational level below bachelor degree, a middle income (net personal monthly income between EUR 1001 – 2000), who does not own a house and lives in the Western part of the Netherlands. ***, ** and * denote statistical significance at the 0.01, 0.05, and 0.10 level, respectively. Standard errors are clustered at household level.

Table A.4: Perceived benefits versus adjusted subjective risks per app category

	Users		Non-users	
	Low risk	High risk	Low risk	High risk
Financial information				
High benefit	61.6%	18.8%	27.1%	20.2%
Low benefit	10.7%	8.9%	20.9%	31.8%
Mobile payment				
High benefit	51.1%	20.6%	10.8%	13.6%
Low benefit	19.8%	8.4%	27.7%	47.9%
Activity tracking				
High benefit	53.3%	21.9%	13.3%	12.5%
Low benefit	18.2%	6.6%	39.6%	34.6%

Note: Scores in which adjusted subjective risks are only based on respondents' overall asessment of the likelihood of becoming victim of data privacy incidents.

Table A.5: Share of respondents that behave paradoxically by app category and Westin type – adjusted subjective risk scores

App category by Westin type	**(1) PPM$_u$**	**(2) PPM$_n$**	**(3) PPM**
Financial information (all)	8.9%	27.1%	26.3%
- Privacy fundamentalist	12.5%	14.1%	14.0%
- Privacy pragmatist	8.5%	31.5%	30.5%
- Privacy unconcerned	0%	40.5%	38.7%
Mobile payment (all)	8.4%	10.8%	9.6%
- Privacy fundamentalist	15.9%	5.8%	10.5%
- Privacy pragmatist	6.2%	11.6%	8.9%
- Privacy unconcerned	2.1%	25.7%	11.9%
Activity tracking (all)	6.6%	13.3%	10.1%
- Privacy fundamentalist	10.6%	7.7%	9.0%
- Privacy pragmatist	5.6%	15.2%	10.7%
- Privacy unconcerned	1.6%	21.6%	10.2%

Note: The results have been calculated using the overall median scores for benefits by app type and the adjusted subjective risks, which are now only based on respondents' overall asessment of the likelihood of becoming victim of data privacy incidents.

Table A.6: Results Wald tests on exogeneity perceived benefits and trust in app providers

	Wald test exogeneity χ^2	p-value	Re-estimated marginal effect	p-value
Financial information				
Benefit	0.92	0.337		
Trust app providers	1.51	0.219		
Mobile payment				
Benefit	0.08	0.775		
Trust app providers	1.94	0.164		
Activity tracking				
Benefit	7.57	0.006	0.18^{***}	0.000
Trust app providers	13.59	0.000	0.23^{***}	0.000

Note: The Wald tests test the hypothesis of no correlation between the error term and the variables reflecting benefits and trust in the app providers, by app type. As instruments benefits and trust in app providers of the other two types of apps have been used together with the other control variables.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl