REGULAR ARTICLE

In a world of Open Finance, are customers willing to share data? An analysis of the data-driven insurance business

Laura Grassi[1]

Abstract

In the financial system, the customers' willingness to share their data is pivotal, because otherwise, banks and insurance companies are powerless to build on customer data. The key step now is to understand whether there is such willingness and what form it takes. In this study, we investigate how willing customers are to share various kinds of data (on physical health, home, driving style, travel, family, social networks) with their insurance company, in return for different rewards (customised products and services, reduced insurance claims risk and insurance premiums adjusted to personal habits and behaviour). Applying the privacy calculus framework to 1501 responses in a web-based survey, we found that rewards, especially when financial, such as insurance premium benefits, play a pivotal role in driving customer decisions about sharing data. Furthermore, customers associate the data they are asked to share with different levels of privacy, influencing their willingness to share. We also found that, when customers are asked to share various kinds of data in return for different rewards, their own personal innovativeness comes into play. Our findings suggest that, in the data-driven insurance business, different rewards offered in return for specific types of data could help companies minimise the "data acquisition cost" and maximise the data collected. In the era of open data, insurers can explore the many opportunities for segmentation, but new kinds of financial exclusion could emerge, resulting in potential biases and thus misinterpretations should analytics and artificial intelligence models be built upon these premises.

✉ Laura Grassi[1]
laura.grassi@polimi.it

1   Politecnico di Milano, Milan, Italy

Published online: 18 March 2024

 Springer

1 Introduction

The appetite for consumer data sharing is a critical part of modern business, and is driven by technological advancements and increasing digitisation. In the insurance industry, the impact of digital transformation in practice means enhancing the customer experience, improving business processes, offering new products, and preparing for competition with other industries (Eling & Lehmann, 2018). The industry is always innovating (Lanfranchi & Grassi, 2021), businesses are developing new products and processes, exploiting existing technology and tapping into their customers' needs (Lanfranchi & Grassi, 2022). As such, data and data sharing are today at the basis of most economic activity (Loi et al., 2022).

Consumer data are now a defining force pervading every aspect of financial businesses (He et al., 2023). Data have been central to the insurance industry for years, although they were mainly used to assess risks and calculate premiums (Campo & Antonio, 2022; Gordon et al., 2003; Hosein, 2023; Lledo & Pavia, 2022). More recently, advancements in data analytics and the emergence of new data sources, among which telematics devices (e.g. black boxes), connectivity and wearable technology, have enabled insurers to access more granular, behavioural and real-time data about customers (Baecke & Bocca, 2017; Feng et al., 2022). Data collected from sensors, IoT devices and similar sources were added to the traditional information already in the insurers' hands. The data now available are highly accurate, integral, and ensure continuity of service (Handel et al., 2014); they improve safety and security, help to prevent accidents or mishaps and lower the risk of accidents and injuries (and so claims) (Saliba et al., 2021; Van der Boom, 2023; Wiegard et al., 2019). Fitness trackers, smart watches, smart clothing and other such wearable devices are another source of customer data that can be used by insurers to predict and assess the risks associated to each customer, adjust their premiums and offer personalised insurance products (McCrea & Farrell, 2018; Paluch & Tuzovic, 2019). The availability of these data has opened the way to new usage-based insurance policies, new pricing models and more customised policies (Ayuso et al., 2019; Husnjak et al., 2015; Verbelen et al., 2018).

In return, this situation has brought up questions concerning discrimination, as, on the one hand, usage data could matter more than demographic information such as gender (Ayuso et al., 2016), but, on the other, using these data could potentially reduce a person's life chances or erect barriers to universal rights such as healthcare (Banerjee et al., 2018). An additional negative side effect of data sharing is that it introduces security vulnerabilities, including the risk of data breaches and cyberattacks (Klumpes, 2023) that target sensitive privacy information, leading to potential theft, manipulation or unauthorised financial transactions, particularly in illicit markets such as the dark web. Moreover, data sharing exposes individuals to heightened identity fraud risk (Piquero et al., 2011), enabling malicious actors to misuse shared data for criminal activities or to disclose private information that may adversely impact a person's reputation or public image. As a consequence, the regulators started limiting the usage of consumer

data to protect the consumers' privacy and prevent personal data from misuse linked to discrimination, and other such improper use (Delcaillau et al., 2022).

A number of regulations were put in place, including Europe's General Data Protection Regulation (GDPR) and Data Act. The GDPR is designed to protect natural persons and set restrictions on personal data and the free movement of such data (European Commission, 2016), where personal data is any piece of information that can identify an individual, including digital identifiers such as IP addresses, cookies, digital fingerprinting and location data (Goddard, 2017). Under the GDPR, only the minimum amount of data needed for a specific purpose can be collected, and these data must be checked for accuracy, kept updated and stored in a secure way. The European Data Act enables connected device users to access and share the data they have generated and share such data with third parties to provide aftermarket or other data-driven innovative services (European Commission, 2022). Another of the regulation's aims is to prevent companies in a dominant position from resorting to unfair practices to obtain data from weaker organisations, and it also puts the spotlight on the compensation due to businesses for making data available.

This corpus of regulations is intertwined with the Open Finance framework, whose arrival in the financial industry has placed customers and their willingness to share data at the centre of operations in a range of services, from banking and insurance to asset management (De Pascalis, 2022; Grassi et al., 2022a; Standaert & Muylle, 2022). On the contrary, in the past with Open Banking, the only sphere involved was bank account information (Chan et al., 2022). Similarly to Open Banking, Open Finance is based on the principle that data supplied by and created on behalf of financial services customers are owned and controlled by the customers themselves (FCA, 2022), increasing the democratisation of finance, in that customers can provide raw financial data to their current financial services providers and also, critically, to the latter's competitors (Zetzsche et al., 2020). Other challenges for insurers are the risk of disintermediation, loss of reputation and transformational failure (Gozman et al., 2018). In Europe, the legal position is that customer data can only be accessed and reused with the customer's consent (European Commission, 2020), including when the purpose is to provide a range of financial services, and data are always subject to data protection rules and security safeguards (European Commission, 2021; European Commission, 2023).

In previous studies on Open Banking, this topic was either perceived in technical terms (Farrow, 2020), or else it dealt with industrial competition (Buckley et al., 2020; Ramdani et al., 2020) or potential new sources of risk (Chan et al., 2022). In this paper, we are saying that the debate is ready to move on. Customer centrality, or, better still, the customers' willingness to share data, has become strategically significant in the financial system, because, if customers are reluctant to do so, banks and insurance companies will be powerless to build on their data. Consequently, understanding whether such willingness exists is now fundamental, as is what form such willingness takes according to the data to be shared or the expected benefits of such sharing. On this point, this paper is, to the best of our knowledge, one of very few studies that considers the customers' point of view on digitalisation and Open Insurance, capturing this significant feature alongside upcoming works such as that by Kandil et al. (2024).

Gaining this insight is thus the focus of this study, where we investigated the sharing of data and, more specifically, how willing customers are to share data with their insurance company. To ensure that our results were sound, we varied the type of data to be shared (in our case, data on the person's physical health, safety and security measures installed at home, driving style, journeys and travels, concerning their family and linked to their social network profiles). We also varied the rewards underpinning why customers are willing to share their data (proposals for personalised products and services that meet a specific need, lowering their perceived insurance claims risk and insurance premiums adjusted to their habits and behaviour). After formulating our research questions about people's willingness to share their data, we explored the topic using information retrieved from a large-scale survey on 1501 consumers.

After these initial considerations, the study detailed in this paper sets out an outline of the theoretical background (Sect. 2), followed by the description of the underlying methodology (Sect. 3), and the presentation and discussion of the results (Sect. 4). Lastly, the main points emerging from the study are drawn together in our contribution (Sect. 5) and conclusions (Sect. 6).

2 Theoretical background and research questions development

While the authorities and the financial players (incumbents and new fintech entrants) are turning to Open Finance (Adke et al., 2022), as of today, there is very little published work on the central role held by customer data in this industry.

So far, data-centricity in the financial industry has been studied mainly along three streams. The first is "open data in finance", and it relates to publishing financial information data (e.g. accounting data, budget data, personal income data) in public databases or ledgers (e.g. Bolgov & Filatova, 2022; Parkhimovich & Minina, 2017). The second stream concerns "openness" in the sense of transparency in data tracing systems—for example blockchain ledgers or distributed ledger technology—that underpin decentralised financial systems (Ali et al., 2019) and DeFi (Grassi et al., 2022b; Smith, 2021). The third stream is open data as the basis for developing new areas of financial crime and fraud (De Koker & Goldbarsht, 2022). What is lacking in all three streams is a thread that concentrates on analysing the customers' willingness to share their data, which is the keystone principle on which Open Finance is built, as is all future regulation, because Open Finance seeks to give customers back the control of their financial data. Where there are no particular technological matters about data sharing—in the sense that Open Finance is built on Application Programming Interfaces (API)—others crop up in the field of human will and privacy considerations, or in relation to the final goal, e.g. what specific innovative product, what specific new service.

From a theoretical perspective, privacy calculus theory suggests that consumers evaluate the trade-off between the perceived benefits of sharing their personal data and all the associated privacy risks. It follows that consumers are only willing to share their data when the perceived benefits outweigh the potential loss of privacy (Gao et al., 2015; Liu et al., 2016; Ryu, 2023) and that privacy is not an absolute

value (Jabbar et al., 2023). In order to make an impact on the final weight, organisations wishing to increase the likelihood that their customers will share personal data may take actions relating to perceived benefits and costs, such as improving rewards and limiting the effect of costs. For instance, personalised benefits and social and monetary rewards were all found to play a role in the customers' decision process (Blakesley & Yallop, 2020; Li et al., 2010; Tang & Ning, 2023). Additionally, customers do not take their decision once and for all for each organisation, but are free to express their choice every time that organisation asks for (personal) information (Dinev & Hart, 2006; Laufer & Wolfe, 1977; Vimalkumar et al., 2021), potentially leading to a situation where people change their minds continuously. What is more, individuals can even base their decisions on personal features (Trepte et al., 2017). The context also matters, both in terms of trust, requesting stakeholder and purpose for which the data is to be used, and also in relation to perceived control over the situation and kind of data (Anderson & Agarwal, 2011; Gutierrez et al., 2019; Rahman, 2019).

Although privacy calculus theory has been widely employed to examine consumers' self-disclosure in technological contexts (e.g. e-commerce websites, location-based services, social networking sites, and so on), the financial industry has been largely overlooked (von Entreß-Fürsteneck et al., 2019; Yang et al., 2020), and only a few papers explore the subject. Yang et al. (2020) found that people using mobile payment apps felt that revealing personal information gave them access to beneficial financial services, but, conversely, it was often linked to lesser perceived value and lower mental well-being. Yuan et al. (2022) introduced the concept of trust in institutions, as a structural assurance for consumer rights, the protection of which is an obvious insurance industry feature. Chatterjee et al. (2023) highlighted the customers' feelings of misuse when sharing data with financial institutions. In the insurance industry, the extant literature has mostly focused on car- and health-related customer data. For example, Festic et al. (2021) looked at the Swiss willingness to share tracking-device data with insurance companies in exchange for a financial benefit, concluding that Swiss people rate the benefits higher than the potential risks. The authors established that 43% would generally be willing to share their data, finding no significant difference in education, but a weak tendency among older people and women to be less willing to do so. Von Entreß-Fürsteneck et al. (2019) analysed a sample of 103 respondents in a scenario-based experiment, showing that the positive effects of privacy benefits are partly dependent on data sensitivity. As the level of sensitivity for different kinds of data can be instrumental in people's willingness to share data, because data can be perceived with varying privacy trade-offs, we formulate our first research question as follows:

RQ1 Is the type of data related to the customers' willingness to share their data?

Thus, under the privacy calculus theory, customers will accept loss of privacy if it rewards them in ways they would not otherwise secure (Fernandes & Costa, 2023). What also emerges is that a specific reward can play a part in driving the customer's decision about their willingness to share data (Hsieh & Li, 2022).

Similarly, Tenopir et al. (2011) found that willingness to share data can be linked to given conditions, as in a transaction where consent is given in exchange for personalised services (Huang & Huang, 2023; Kang & Namkung, 2019; Lv & Wan, 2019), or monetary rewards (Bijlsma et al., 2023; Huang & Huang, 2023; Tsarenko & Rooslani Tojib, 2009). According to Beke et al. (2022), rewards can be grouped by type into, for instance, performance, psychological and financial dimensions. Sharing performance-type information helps companies gain a clearer understanding of their customers' needs and preferences, and thus create personalised products and services (Simonson, 2005; Wedel & Kannan, 2016). At the same time, when customers share information, it affects how they feel about the firm, producing psychological consequences (Acquisti et al., 2015) that range from feeling they are special, to having the sensation that they are under observation and being controlled. Lastly, sharing data can bring customers monetary gains or lower costs (Ravula, 2022), meaning that some rewards are more strictly associated to the financial dimension. Apropos of financial rewards, von Entreß-Fürsteneck et al. (2019) found that they are a strong positive indicator for a customer's willingness to disclose self-tracking data. It follows that we can formulate our second research question thus:

RQ2 Are different reward dimensions related to the customers' willingness to share their data?

Aligned with privacy calculus theory, a consumer's decision and willingness to share personal data hinge upon multifaceted factors, prominently innovativeness, individual characteristics and pre-existing knowledge (Fox et al., 2022; Kehr et al., 2015; Yuan et al., 2022). Today's digitally empowered landscape, with heightened expectations for personalised and empathetic services (Adke et al., 2022), includes a spectrum of openness towards novel concepts (Agarwal & Prasad, 1998), exemplified by variations in people's positive reception to innovations in services such as insurance (Gironda & Korgaonkar, 2018). A person's inclination towards innovativeness and early adoption is intricately linked to his or her knowledge and experience in the relevant domain (Briones de Araluze, 2022), and these are considered pivotal factors in shaping an individual's behaviour (Karjaluoto et al., 2002). More broadly, personal features were found to be both relevant and significant when investigating customer decisions relating to innovation in finance (Karjaluoto et al., 2002). Van Dijk (2020) found that younger, more affluent male members of a society tend to reap more benefit from their internet usage and know how to manage the associated risks more effectively than other users. Chen et al. (2023) observed a gender gap in people's use of innovative financial products, in their willingness to use new financial technology and readiness to switch to a new entrant. Women are also found to be more conservative about their privacy, more concerned about sharing information and generally more anxious about the implications of data-sharing on their personal safety (Armantier et al., 2021; Cho & Hung, 2011; Rowan & Dehlinger, 2014). Age is also relevant in matters of innovation and data sharing, as it influences

the risk–benefit trade-off (Fernandes & Costa, 2023; Wottrich et al., 2018). Tenopir et al. (2011) found that there is a younger vs older difference in the likelihood of agreeing to share one's data, Goldfarb and Tucker (2012) highlighted "large" effects, and Wottrich et al. (2018) noted that privacy is more important for older than younger people. Self-disclosure behaviour was found to differ between younger and older individuals (Parker & Parrott, 1995). It emerges overall that older people are much less likely to reveal personal information than younger people, they have higher privacy concerns, and are more cautious about sharing their data. Education is another factor frequently considered under privacy calculus theory (e.g. Duan & Deng, 2021; Fox, 2020; Tran & Nguyen, 2021). Al-Ashban and Burney (2001), Suoranta and Mattila (2004), and Howcroft et al. (2002) found that education plays a part in financial innovation and in the adoption and use of innovative services, and Or and Karsh (2009) that it impacts on people's privacy concerns and adoption intentions. The possible explanation according to Belanger and Crossler (2011) is that more highly-educated people may be more aware of the potential benefits and risks associated with data sharing. Additionally, there is apparently a kind of cultural predisposition towards being willing to share data which is linked to where a person belongs (Robinson, 2017). Putting all this information together, personal attitude is likely to affect someone's willingness to share data rather than the broader categories of features into which they can be placed (such as gender, age, occupation and geographical location). Our third research question thus is:

RQ3 Is personal innovativeness related to the customers' willingness to share their data?

3 Methodology

3.1 Data gathering

In order to achieve the purpose of our study, and explore the willingness of customers to share data, in September 2020 we conducted a web-based survey on a sample of Italian consumers who had looked up at least one thing on the internet in the one month prior to the analysis. The questionnaire was written in Italian and pre-tested by two scholars, four PhD students and research fellows, and five C-level managers at financial outfits (both incumbents and startups). All testers were encouraged to comment on the questionnaire's clarity, and on weaknesses in the survey's design and instrumentation (Ciunova-Shuleska & Palamidovska-Sterjadovska, 2019). We used a quota sampling approach to collect the answers (Bernard & Bernard, 2013; Demmers et al., 2018), in order for our sample to be significantly representative of the overall population, in terms of gender, age, geographical area of residence and occupation. In total, we received 1501 completed questionnaires. To our knowledge, this is one of the largest consumer surveys on innovative financial services conducted in Europe and the first investigating how willing customers are to share their data.

We asked the respondents individually about their willingness to share data for a reward, specifically scrutinising six types of data in our study, each type reflecting a different level of privacy (i.e. physical health, home safety and security, driving style, travel, family information and social network profiles). Looking at the rewards offered, our survey covered three situations where customers can share their data with their insurance company, namely proposals for personalised products and services that meet a specific need, a lower perceived insurance claims risk and insurance premiums adjusted to the customers' habits and behaviour. We thought that these three situations would clearly outline the benefits for customers of sharing their data, and ensure that the trade-off with the perceived benefits was perfectly plain. In each situation, the respondents were either willing to share their data (code 1) or had no intention to do so (code 0). The answers were all coded and recorded in the database.

3.2 Data analysis

Considering our research questions and the richness of our data, we opted for a test of independence for both RQ1 and RQ2. Because we are dealing with categorical variables relating to different kinds of data to be shared plus a variety of rewards, in order to test for independence of choice in statistical terms, we performed a bivariate analysis using Pearson's chi-square test, a method frequently used to test relationships between categorical variables (Adam et al., 2018; Mishra et al., 2019).

For RQ3, we opted for a multivariate multiple regression, as this would give us multivariate results. We ran three distinct models simultaneously, modelling the consumers' willingness to share their data in return for a given reward. Model 1 relates to proposals for customised insurance products and services (*Custom*). Model 2 relates to the customer being seen as a lower perceived insurance claims risk (*Risk*). Model 3 relates to the customer securing insurance premiums adjusted to personal habits and behaviour (*Premium*). This enabled us to examine the differences from case to case, instead of using separate probit regression analyses for each outcome variable. Operationally, we used MANOVA and mvprobit in Stata to explain the variation in the likelihood that people share data as a function of the consumers' personal innovativeness and demographic characteristics.

Consistently with previous literature relating to privacy calculus theory, our independent variable is the consumer's personal innovativeness (*innovativeness*), while we controlled for gender (*gender*), age (*age*), education (*educ*), occupation (*job*) and geographical area. The geographic area is a combination of two items, the area where the consumer is located (*geo_area*) and the size of his or her town or city (*geo_scale*). We explicitly asked respondents about all these items in the survey. The consumers' personal innovativeness (*innovativeness*) was measured on the basis of several digitally-enabled insurance services. The services we tested were buying insurance where the premium as calculated on behaviour (z_1), buying on-demand insurance (z_2), managing claims on a smartphone (z_3), altering insurance cover digitally (z_4), accessing telemedicine services/remote medical consultations as part of the insurance policy (z_5), and buying/renewing insurance policies digitally (z_6). For

each service, participants could either answer "I've never heard of it" (code 1), "I'm not familiar with it but I've heard about it" (code 2) or "I'm very familiar with it" (code 3). In our sample, 86 respondents (5.7%) achieved the maximum score, meaning that they were rated as highly innovative, while 157 (10.5%) only reached the minimum score, showing a poor mental openness to innovation. However, these data are highly correlated, so we clustered the different types of information together through factor analysis to obtain a smaller set of uncorrelated variables, and also to create an index that we could use to measure people's innovativeness. We obtained a single factor (Eigenvalue 3.69, Table 1), which we labelled *innovativeness*. This variable weighs about equally for each of the variables (factor loadings from 0.74 to 0.84), thus, the higher its value, the more a person is receptive to innovation.

3.3 Data modelling

As shown in Table 2, we obtained three simultaneous regressions (our three models), each with six specifications based on the six types of data we were examining (i.e. physical health, home safety and security, driving style, travel, family information, social network profiles):

$$
\begin{aligned}
Custom_j = {} & \beta_{1,j,0} + \beta_{1,j,1} \times innovativeness_j + \beta_{1,j,2} \times gender_j \\
& + \beta_{1,j,3} \times age_j + \beta_{1,j,4} \times educ_j + \beta_{1,j,5} \times job_j + \beta_{1,j,6} \times geo\_area_j \quad (1) \\
& + \beta_{1,j,7} \times geo\_scale_j + e_j \quad per\,each\,j\,data
\end{aligned}
$$

$$
\begin{aligned}
Risk_j = {} & \beta_{2,j,0} + \beta_{2,j,1} \times innovativeness_j + \beta_{2,j,2} \times gender_j + \beta_{2,j,3} \times age_j \\
& + \beta_{2,j,4} \times educ_j + \beta_{2,j,5} \times job_j + \beta_{2,j,6} \times geo\_area_j \quad (2) \\
& + \beta_{2,j,7} \times geo\_scale_j + d_j \quad per\,each\,j\,data
\end{aligned}
$$

$$
\begin{aligned}
Premium_j = {} & \beta_{3,j,0} + \beta_{3,j,1} \times innovativeness + \beta_{3,j,2} \times gender_j \\
& + \beta_{3,j,3} \times age_j + \beta_{3,j,4} \times educ_j + \beta_{3,j,5} \times job_j + \beta_{3,j,6} \times geo\_area_j \quad (3) \\
& + \beta_{3,j,7} \times geo\_scale_j + t_j \quad per\,each\,j\,data
\end{aligned}
$$

where $Custom_j$, $Risk_j$, and $Premium_j$ stand for the three different cases of $y_{i,j}$, i.e. willingness to share data j with one's insurance company for proposals for customised

Table 1 Factor loadings in the factor analysis, i.e. the weights between each variable and the single factor (*innovativeness*)

Variable	Factor 1 loadings
z_1	0.7539
z_2	0.7741
z_3	0.8158
z_4	0.8395
z_5	0.7750
z_6	0.7441

Table 2 Description of the different models estimated simultaneously

Willingness to share j data for a i reward	i reward		
	Proposals for customised products and services ($Custom_j$)	Lower risk of insurance claims ($Risk_j$)	Insurance premium adjusted on the basis of personal habits and behaviour ($Premium_j$)
j data			
Physical health	Model 1	Model 2	Model 3
Home safety and security			
Driving style			
Travel			
Family information			
Social network profiles			

products and services (y_{1j}, *Custom$_j$*), for one's insurance claims risk being lowered (y_{2j}, *Risk$_j$*) or for insurance premiums being adjusted according to one's personal habits and behaviour (y_{3j}, *Premium$_j$*). These three situations and relative rewards also vary by type of *j* data shared (i.e. physical health, home safety and security, driving style, travel, family information, social network profiles) where *innovativeness* is the independent variable, and *gender, age, educ*, *job, geo_area* and *geo_scale* are the control variables, *i* represents the three rewards, *j* represents the six types of data, β are the coefficients to be estimated and e_j, d_j, t_j are the error terms.

4 Results and discussion

Looking at the study sample (Table 3), the participants are between 18 and 74 years of age, with an average age of 44, and gender is well-balanced, with 761 women and 740 men. On average, they are well-educated and hold at least a secondary school diploma (80.4%). A good percentage of people in the sample describe themselves as white collar employees with a permanent employment contract (402 participants, 26.8%), while there are fewer doctors (5, 0.3%) and farmers/labourers (8, 0.5%).

From an initial descriptive analysis on our dependent variables (y_{ij}), the data show some meaningful patterns. Out of the total sample, 314 respondents (20.9%) are willing to share their data, irrespective of the data or reward (i.e. any data and reward are acceptable). On the contrary, several are not willing to share their data, no matter what kind of data is shared or what reward is offered (290 cases, 19.3%). These people apparently perceive only the risk associated with data sharing, without taking into account the level of perceived privacy for each piece of information and the associated benefit. Age is apparently not a factor, with respondents ranging from 19 and 74, and neither is gender, as 126 are men and 164 women, although home makers and unemployed people make up a higher quota than in the sample overall (12% and 17% vs 8.8% and 10.7%, respectively). In this group, the share of respondents with a secondary school diploma is slightly above the sample average (57.6% vs 52.6%), while the share of those with a degree is slightly lower (21.0% vs 27.8%).

4.1 Relevance of kinds of data and rewards in the customers' willingness to share their data

If we consider the role of perceived privacy associated with the kind of data to be shared (of the six types of data we tested), it seems that while people can be more or less willing to share data on physical health, house safety and security, and driving style, the average percentage follows a similar pattern, and it flips to the inverse situation (i.e. from positive to negative, and vice-versa) for data on social network profiles and family, while travel-related information straddles the cross-over point (Fig. 1). It also emerges clearly that customers are particularly reluctant to share their social network data, as the peak for willingness to share these data was the lowest of the six types of data (about 40%, and the result is consistent for any reward or benefit). This finding does not sit immediately well with the fact that social network

Table 3 Variables description and descriptive statistics

Categorical variables	Label. category	Observations (frequency %)	Observations
Personal innovativeness (*innovativeness*)	1. I've never heard of it 2. I'm not familiar with it but I've heard about it 3. I'm very familiar with it	See Table 1	1501
Gender (*gender*)	1. Man 2. Woman	740 (49.3%) 761 (50.7%)	1501
Education (*educ*)	1. Degree (bachelor's or master's) 2. Diploma/upper secondary education 3. Primary and lower secondary education	417 (27.8%) 790 (52.6%) 294 (19.6%)	1501
Occupation (*job*)	1. Entrepreneur/business owner	22 (1.5%)	1501
	2. Self-employed professional (architect, engineer, accountant, lawyer, etc.)	87 (5.8%)	
	3. Director, upper management (public or private sector)	21 (1.4%)	
	4. Middle management (office manager, head of service, technician with significant responsibility)	30 (2.0%)	
	5. White-collar worker (in a public or private company, salesperson, etc.) with a permanent contract	402 (26.8%)	
	6. White-collar worker (in a public or private company, salesperson, etc.) on another type of contract	71 (4.7%)	
	7. Merchant/trader/manager of a commercial operation	41 (2.7%)	
	8. Manual worker/artisan	112 (7.5%)	
	9. University lecturer/school manager	5 (0.3%)	
	10. Teacher (primary and secondary schools)	38 (2.5%)	
	11. Officer in the armed forces or police	11 (0.7%)	
	12. Members of armed forces or police below the rank of officer	9 (0.6%)	
	13. General practitioner or specialist doctor	4 (0.3%)	
	14. Registrar (undergoing training in a specialisation)	1 (0.1%)	
	15. Farm owner/manager	7 (0.5%)	
	16. Farm worker/labourer	1 (0.1%)	
	17. Home maker (no outside occupation)	132 (8.8%)	
	18. Pensioner	76 (5.1%)	
	19. Unemployed or job seeker (first job)	161 (10.7%)	
	20. Student	157 (10.5%)	
	21. Other	113 (7.5%)	
Area (*geo_area*)	1. North-west Italy 2. North-east Italy 3. Central Italy 4. Southern Italy	439 (29.3%) 261 (17.4%) 288 (19.2%) 513 (34.2%)	1501
Scale (*geo_scale*)	1. to 8. Small town (less than 250,000 inhabitants) 9. Large town or city (more than 250,000 inhabitants)	1183 (78.8%) 318 (21.2%)	1501

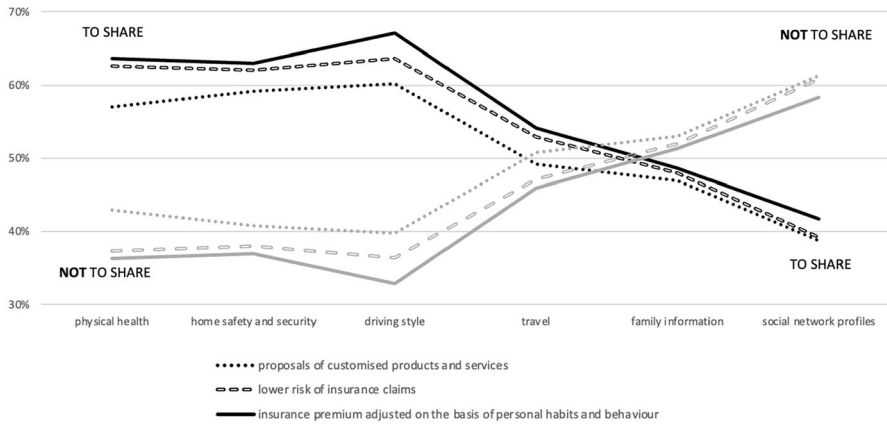| Continuous variable	Mean	Std.dev	Min	Max	Observations
Age (*age*)	43.9	13.9	18	74	1501

Fig. 1 Willingness to share or not to share *j* data (physical health, home safety and security, driving style, travel, family information, social network profiles) for *i* rewards (proposals for customised products and services, lower risk of insurance claims, insurance premiums adjusted to personal habits and behaviour)

data are intrinsically data to be shared, they are public by definition but above all by choice, and the related level of privacy should be as low as possible. There could thus be two explanations for this situation. (i) While social network data are innately shared data (Giovannetti & Hamoudia, 2022), customers may not *rationally* understand that their social network data are public anyway (and can be accessed by insurance companies, and any company in general). (ii) Alternatively, it could be that customers' are thinking about and so referring to the more private part of their social network, where information is exchanged bilaterally or in small groups. People's behaviour runs along similar lines for data about their family (their willingness to share this information is about 50%). Conversely, people are much more ready to share information on their driving style (60–67%), which we explain through the mechanism of black boxes installed in cars.

We believe that current decisions are also influenced by a customer's normal interaction with his or her insurance company. While customers already have to give their insurance company data on their physical health, house safety and security, driving style and travel in order to access certain policies (life, health, fire, car, travel insurance), as of today, they share their data on social network profiles and family with their insurers only very infrequently. Customers may perceive these data as more sensitive in part for this reason, seeing more risks than benefits for themselves, as set out in privacy calculus theory.

Our preliminary descriptive analyses show also that the reward plays a significant part in the customers' decision. Regardless of the kind of information shared, people are always more willing to share specific information if the associated benefit is linked to the insurance company offering premiums adjusted to their personal habits and behaviour (Fig. 1). At the same time, they are always less willing to share these data if the reward is a proposal for customised products and services. Between the two lies a lower risk of insurance claims, which results in a better reward (i.e. seen to have a more favourable risk–benefit trade-off than proposals for customised

products and services, but worse than a customised insurance premium). The implication is that customers (and consumers more in general) seem most attracted by financial rewards, followed by psychological rewards and lastly by those related to performance, in line with the classification given by Beke et al. (2022). As shown in Fig. 1, the maximum peak in data-sharing willingness relates to customers sharing data in exchange for their insurer adjusting the premium on the basis of their personal habits and behaviour, with the most common method so far being for them to share data on their driving style via black boxes installed in their cars.

For insurers (and indeed others), knowing that they can offer alternative rewards and collect the same kind and potentially more or less the same amount of data, could help to bring down the collection cost while maximising the amount of data collected. While the discussion so far has been about customer acquisition costs (Gupta et al., 2004), in the new Insurtech landscape (Stoeckli et al., 2018), and in an economy where data are considered the new oil (Hirsch, 2013), the "data acquisition cost" will be very central to understanding how the modelling evolves, especially artificial intelligence modelling, riding the technology wave of Open Data (O'Leary et al., 2021; Perkmann & Schildt, 2015).

4.1.1 Chi-square test of independence

We started from analysing people's willingness to share different kinds of data for a specific reward (those listed previously). We specifically want to understand whether, if we take the reward as a constant, the end users' decisions about sharing their data or not depend on the data they are asked to share (RQ1). The three analyses gave us a p-value of 0.000 in each case (chi-square with five degrees of freedom = 212.7345, 294.2543 and 300.7776, respectively), allowing us to conclude that not only is there a statistically significant relationship between the kinds of data to be shared and willingness to share them, for each given reward, but also that this statistically significant relationship is consistent for all the rewards. This finding implies that we have found a relationship between the kind of data to be shared and people's willingness to share the data, and this relationship holds for different rewards.

Similarly, we tested people's willingness to share a given kind of data considering all the various rewards one by one i.e. we tested whether there is a relationship between the reward and consumers' willingness to share data, to help us understand whether the risk–benefit trade-off in the decision is dependent on the reward (RQ2). Here, there are differences for the six kinds of data (physical health, house safety and security, driving style, travel, family information, and social network profiles). The results indicate that there is no statistically significant relationship between the type of reward promised and willingness to share data if the data relates to social network profiles (chi-square with two degrees of freedom = 3.2590, p-value = 0.196) or is family information (chi-square with two degrees of freedom = 0.8454, p-value = 0.655). This result means that, when people are asked to share social network and family data, varying the rewards has no effect on inducing the sharing of data and the willingness to do so will be, on average, quite negative (see Fig. 1).

On the contrary, there is a statistically significant relationship between the type of reward promised and willingness to share data if the data concerns physical health (chi-square with two degrees of freedom $=16.1776$, p-value $=0.000$), home safety and security (chi-square with two degrees of freedom $=5.0956$, p-value $=0.078$), driving style (chi-square with two degrees of freedom $=15.2741$, p-value $=0.000$) or travel (chi-square with two degrees of freedom $=7.7220$, p-value $=0.021$). Returning to privacy calculus theory, we can conclude that consumers associate different levels of privacy to the different kinds of data they are asked to share, and this level of privacy for each of the six kinds of data affects the risk–benefit trade-off. Thus, we could divide data into more privacy-sensitive and less privacy-sensitive information.

4.2 Relevance of personal innovativeness for the customers' willingness to share their data

Overall, the multivariate analysis of variance (MANOVA) in all three situations (a customer's willingness to share their data in return for proposals for customised products and services, for lowering their designated risk of insurance claims, and for their insurance premium to be adjusted on the basis of their personal habits and behaviour) yielded significant results in the multivariate test statistics. In the three situations, Wilks' Lambda, Pillai's trace, Lawley–Hotelling's trace and Roy's largest root all have 0.0000 p-values, confirming that all the equations—for each type of data—are together statistically significant.

Several interesting results emerged from the mvprobit estimation (Table 4), which can be grouped into the following observations.

Firstly, the results are robust in supporting our findings that personal innovativeness is related to the consumers' willingness to share their data (RQ3). The statistical significance is always below 1%, independently of the data shared and the reward expected. Furthermore, in all cases, the coefficient β always has a positive impact. It is worth remembering that a maximum score for innovativeness means that that a person's overall innovativeness level is very high. Thus, the positive β must be read as the fact that the more consumers are familiar with innovative insurance services, the more they are willing to share their data. In other words, if someone is open to innovation, that person will be more ready to share any data (of the six types tested) and for any reward (of the three tested). Our interpretation of these findings is that, set against the background of privacy calculus theory, there are in reality some aspects that will weigh heavily on the risk–benefit balancing act, both personally and recursively for society. In substance, it is as if the more innovative people, those most familiar with innovative insurance services, weigh up the specific rewards and benefits that sharing their data could bring them, and consequently move immediately in a direction that is certain, that of sharing their data, regardless of the data in question or the specific reward. The result is even more significant for policyholders, who are investing extensively to spread and increase financial innovativeness and education among consumers across the world. For insurance companies, this result could

Table 4 Results of the multivariate probit model estimations

	Proposals for customised products and services (*Custom$_j$*)		Lowered risk of insurance claims (*Risk$_j$*)		Insurance premium adjusted to the policy-holder's personal habits and behaviour (*Premium$_j$*)	
	Coefficient	p-value	Coefficient	p-value	Coefficient	p-value
Physical health						
Gender	0.06	0.347	0.02	0.733	0.01	0.855
Age	−0.00*	0.057	−0.01***	0.009	−0.00	0.132
Educ.	0.08*	0.099	0.02	0.628	−0.02	0.687
Job	−0.00	0.444	−0.01	0.137	−0.01	0.283
Geo_area	0.03	0.339	0.02	0.392	0.00	0.887
Geo_scale	−0.02**	0.024	−0.02*	0.058	−0.01	0.263
Innovativeness	0.34***	0.000	0.31***	0.000	0.32***	0.000
Constant	0.23	0.256	0.65***	0.002	0.65***	0.002
Home safety and security						
Gender	0.08	0.243	0.01	0.926	−0.03	0.681
Age	0.00	0.494	0.00	0.973	−0.00	0.384
Educ.	0.01	0.785	−0.03	0.561	−0.04	0.443
Job	−0.00	0.710	−0.00	0.367	−0.00	0.545
Geo_area	0.01	0.695	−0.01	0.584	−0.02	0.514
Geo_scale	−0.02	0.108	−0.01	0.442	−0.00	0.689
Innovativeness	0.35***	0.000	0.32***	0.000	0.30***	0.000
Constant	0.11	0.595	0.47**	0.019	0.62***	0.002
Driving style						
Gender	−0.04	0.567	−0.07	0.268	−0.06	0.338
Age	−0.00	0.737	−0.00	0.998	−0.00	0.949
Educ.	0.01	0.898	0.00	0.967	−0.02	0.622
Job	−0.00	0.314	−0.00	0.360	0.00	0.650
Geo_area	0.02	0.462	0.03	0.263	0.03	0.316
Geo_scale	−0.00	0.820	0.00	0.962	−0.00	0.873
Innovativeness	0.31***	0.000	0.29***	0.000	0.29***	0.000
Constant	0.36*	0.072	0.42**	0.036	0.50**	0.013
Travel						
Gender	−0.04	0.574	−0.03	0.647	−0.11*	0.075
Age	−0.01***	0.000	−0.01***	0.000	−0.01***	0.000
Educ.	0.13***	0.008	0.06	0.237	0.02	0.726
Job	−0.01	0.208	−0.00	0.374	−0.00	0.417
Geo_area	0.05*	0.079	0.05*	0.077	0.03	0.221
Geo_scale	−0.00	0.939	−0.00	0.728	0.00	0.876
Innovativeness	0.29***	0.000	0.27***	0.000	0.27***	0.000
Constant	0.08	0.660	0.37*	0.057	0.54***	0.005
Family information						
Gender	0.04	0.507	0.04	0.544	0.01	0.850

Table 4 (continued)

	Proposals for customised products and services (*Custom$_j$*)		Lowered risk of insurance claims (*Risk$_j$*)		Insurance premium adjusted to the policy-holder's personal habits and behaviour (*Premium$_j$*)	
	Coefficient	p-value	Coefficient	p-value	Coefficient	p-value
Age	−0.01***	0.008	−0.01***	0.001	−0.01***	0.000
Educ.	0.08	0.117	0.10**	0.044	0.02	0.623
Job	−0.01	0.122	−0.01*	0.077	−0.01*	0.053
Geo_area	0.01	0.583	0.05*	0.053	0.05**	0.047
Geo_scale	−0.02	0.137	−0.02*	0.088	−0.01	0.526
Innovativeness	0.32***	0.000	0.31***	0.000	0.31***	0.000
Constant	0.09	0.634	0.07	0.706	0.30	0.118
Social network profiles						
Gender	−0.07	0.308	−0.09	0.169	−0.15**	0.024
Age	−0.01***	0.000	−0.01***	0.000	−0.01***	0.000
Educ.	0.11**	0.021	0.14***	0.007	0.10**	0.040
Job	−0.01	0.300	−0.01	0.106	−0.01*	0.059
Geo_area	0.07***	0.009	0.06**	0.023	0.09***	0.001
Geo_scale	−0.01	0.340	−0.01	0.254	−0.01	0.632
Innovativeness	0.35***	0.000	0.39***	0.000	0.35***	0.000
Constant	−0.04	0.831	0.14	0.472	0.29	0.143

p-values: ***significant at the 1% significance level, **significant at the 5% significance level, *significant at the 10% significance level

mean that, to convince customers to share their data more than they do today, they could first act on their customers' knowledge of financial innovation, and be the bridge connecting to greater openness in sharing data.

Looking at the control variables, similarly to Chang et al. (2022)'s suggestion that different value dimensions are relevant at different points in the purchase-related decision-making process, we found that different customer features are relevant in terms of sharing different kinds of data associated with a variety of rewards.

Our results show that gender is statistically significant only when people share data on their social network and about travel, but, even then, only when the reward is about adjustments to their insurance premium (β = −0.15 and β = −0.11, p-value = 0.024 and 0.075, respectively). As we found, men are more willing than women to share their social network data, but this is nothing new. Taddicken (2014), especially, noted that gender differences in disclosing sensitive data only exist when such data can be publicly accessed, which is the situation for social network data. Our research expanded the argument, showing that the same also applies to other sensitive data, those linked to journeys and travels. Looking at the rewards, the fact that there is no specific gender factor can be linked

to men and women being "virtually indistinguishable in their typical insurance coverage" (Brown & Finkelstein, 2007), meaning that they act in almost the same way, and also to the possible changes taking place year by year. Specifically, in 1995, women were found to be generally more willing to reveal personal information and more often than men (Parker and Parrott, 1995), a difference that today seems more tenuous albeit still there, obviously after controlling for other factors.

Secondly, the regression coefficients and their respective statistical significance show that age matters when sharing data. Age plays a substantial part in a person's willingness to share social network data, travel data or family data, whatever the reward (p-value ranging from 0.000 to 0.008). Additionally, the coefficient is always negative, meaning that younger people not only act differently to older ones, but also that people's willingness to share these data decreases as they get older. Said otherwise, younger people are more open to sharing these data, in return for a reward, in all situations where age plays a significant part in a person's willingness to share data. Additionally, age comes into play when people share their health data to receive customised products ($\beta = -0.005$ and p-value$=0.057$) and to reduce their classified risk of insurance claims ($\beta = -0.006$ and p-value$=0.009$).

Lastly, our results support the finding that higher educated consumers are less willing to share their data, especially social network data. To start with, when significant, the coefficient is always positive, with the variable's highest values being related to the lower levels of education (Table 3). The effect becomes significant for social network data when any kind of reward is on offer ($\beta = 0.11$, 0.14 and 0.10 and p-value$=0.021$, 0.007 and 0.040, respectively), for health and travel data when the reward is to receive customised products ($\beta = 0.08$ and $\beta = 0.13$, p-value$=0.099$ and 0.008, respectively), and for family data when the reward is a lower insurance claims risk ($\beta = 0.10$ and p-value$=0.044$). Overall, the results indicate that insurance companies should leverage on well-educated and innovative customers to increase the amount of data they collect, where possible targeting younger, well-educated and preferably male customers. However, not all customers act the same when offered the same rewards. This finding highlights a good opportunity for segmentation by kind of data the insurance company would like to collect and kind of customer it wants to attract. Policy makers should be wary concerning the specific findings of this survey. If insurance companies follow them in toto when collecting data from their customers, they will gather and store data that are not representative of the entire population. As a consequence, there could be possible biases when those charged to do so interpret the analytics built on these data, and thus lead to further potential segmentation or new kinds of financial exclusion (Urueña-Mejía et al., 2023), and potential new target customers could be selected on the basis of features that drive their unwillingness to share data. By contrast, we should issue a warning to new generations and technophile consumers who may underestimate the value of their data.

5 Contribution

In this study, we refer to three streams of literature, and our intention is to contribute to all three.

Firstly, we add to the stream on Open Finance and Fintech more broadly. Briones de Araluze (2022) noted that, currently, the literature is lingering over service provider infrastructure and the ecosystems around new entrants. Against this backdrop, we decided to focus our research on the consumers' willingness to share their data, and we believe that the future of the industry will pivot around this consumer willingness. We are not making the claim that Open Finance is definitely the channel whereby the financial system will become a true electronic market, sharing Dratva (2020)'s concerns. It is also probable that there will be no single interpretation of Open Finance on the international stage, because of different regulations and contexts (e.g. advanced vs emerging economies), as was previously the case with Open Banking (Rastogi et al., 2020). What we believe, however, is that the financial industry can only go in the direction of placing the customer at its core (Grassi et al., 2022a), and the sharing and willingness to share Open Finance-enabled data will set the tone. The competitive evolution in the financial industry will also be played out in this setting, with an increase in Fintech and Insurtech startups. On their side, the Big Techs will carve out an even stronger foothold in the sector, helped by laying their hands on more customer data, without being equally committed to sharing them with third parties (He et al., 2023; Standaert et al., 2020).

Secondly, we contribute to the stream on privacy. To our knowledge, we are the first research group to apply privacy calculus theory in the field of insurance. The only antecedent we were able to find was Wiegard et al. (2019), where, however, the main purpose of the research was to analyse the success of wearable technology for insurance companies. We have made the assumption that the insurance field is a case apart and its context has an impact on our contribution to the theory. Insurance companies differ from every other kind of business because of the trust that develops between customer and insurer owing to the insurer's part in limiting potential financial losses that result from damages (Robinson & Botzen, 2022). Thus, we assume that trust in the insurance company plays a significant role in one's decision to share data (Alashoor & Baskerville, 2015; Kang & Namkung, 2019). Additionally, our study focuses on *willingness* to share data, as it has been shown in previous research that coercion to share private data with insurers is wrong because it violates the autonomous choice of a privacy-valuing client, but it could also prevent customers from acting spontaneously and authentically (Loi et al., 2022).

Thirdly, we contribute to the stream on the economics of data and incentives in data sharing, noting that theoretical frameworks on how data affect output, privacy and consumer welfare have been developed in previous research (e.g. Bergemann & Bonatti, 2019; Jones & Tonetti, 2020). However, these frameworks were not directly applicable to Open Finance for several reasons. In Open Finance, under the current regulations in force at least in Europe, it is clearly the case that (i) customers cannot be paid to sell their data, and they should not pay anyone for doing so at their request, (ii) data cannot be shared or sold to third parties, if not under the explicit request of the customer, (iii) financial institutions cannot "bribe" their customers and arrange matters so that they will be charged less in exchange for agreeing not to share their data with others.

6 Conclusion

In the financial landscape, the centrality of customer and data have become even more evident with the arrival of the Open Finance framework. Consumer data sharing has significant implications for the insurance industry, and affects a number of aspects including risk assessment, pricing, underwriting and claims management. Insurers that can secure granular, real-time data can model risks more accurately and offer insurance products tailored to their individual customers' needs. Their increased ability in this area has potentially led to improved efficiency, better risk management, cost savings and other such benefits for both insurers and customers. However, the end users' angle of perception and their willingness to share their data has never been examined with any great interest, neither in academic literature nor by the industry as a whole.

The research covered in this paper studies what influences people's willingness to share personal data with financial incumbents, adopting the consumer's perspective. We specifically studied people's willingness to share different kinds of data (data about their physical health, safety and security at home, their driving style, journeys and travels, concerning their family, and social network profiles) in return for different rewards (from proposals for personalised products and services that meet a specific need, or reducing their insurance claims risk, to insurance premiums calibrated to each person's habits and behaviour).

Our research, conducted on a panel of 1501 consumers, brings up some interesting insights. The findings shine a light on the pivotal role played by rewards—especially financial rewards such as advantageous insurance premiums—in driving the consumers' decision to share data. When people are asked to share social network and family data, varying the rewards has no effect on inducing the sharing of data (and the willingness to do so will be, on average, quite negative). On the contrary, there is a relation between the type of reward promised and the willingness to share data if the data concerns physical health, home safety and security, driving style or travel. Further, there is a statistically significant relationship between the kinds of data to be shared and willingness to share them, for each given reward. Thus, consumers associate the data they are asked to share with different levels of privacy, and the level of privacy for each data type is what influences the balance between risks and benefits, and in turn their willingness to share data. Consequently, we can classify data into more privacy-sensitive and less privacy-sensitive information. Lastly, the people most familiar with innovative insurance services weigh up the specific rewards and benefits that sharing their data could bring them, and are more ready to share information regardless.

At the same time, our findings may have implications for public policy decisions. Overall, our results suggest when and how far customers are willing to share information with insurance companies. Our findings also open a debate on fairness, potentially leading to a new kind of financial exclusion. If insurers segment their customer base on features that indicate who is more likely to share a given kind of data of interest, they will collect and store data that are not representative of the entire population, leading to possible biases in the interpretation

of the analytics and the models they underpin, especially in the era of artificial intelligence. Furthermore, for the insurers (and other interested parties) knowing that there are different weights for the different rewards offered for the same kind of data could contribute to minimising the collection cost, the "data acquisition cost", while maximising the data collected. As observed, these results open the way for a more data-driven insurance business, yet we should think about warning new generations and more technophile consumers who may be unaware of the true value of their data.

As in all studies, ours has its limitations and opportunities for future research. Our participants were recruited online so, at the very least, they had access to the internet, although we do not believe that this is a condition for inclusion or exclusion in todays' world. We conducted our survey in September 2020, an interesting year for digitalisation and digital behaviour, the upshot of the first wave of the Covid pandemic. Since then, the consumers' behaviour towards digital services may possibly have changed, as so many digital practices and applications are now mainstream, particularly in the financial sector. In addition, another limitation of this study could be the reliability of self-reported information, although the respondents knew they were anonymised, meaning that there should be no concerns about self-disclosure, transparency or honesty. Colleagues may expand on our work by analysing the more qualitative aspects, including for example, how the type of data in question relates to the consumers' willingness to share their data. Lastly, the setting of our research is the European insurance industry, which is considered to be a developed market, with acceptable concerns on privacy raised by regulators, players and consumers. Factors such as differences in regulatory environments, presence of intermediaries, level of trust, cultural attitudes towards privacy and technology adoption can influence the spread and acceptability of data sharing practices in other contexts, such as those in emerging markets.

Data availability The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Declarations

Conflict of interest The authors have no conflicts of interest/competing interests to declare.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Adam, A. M., Boadu, M. O., & Frimpong, S. (2018). Does gender disparity in financial literacy still persist after retirement? Evidence from Ghana. *International Journal of Social Economics, 45*(1), 18–28.

Adke, V., Bakhshi, P., & Askari, M. (2022). Impact of disruptive technologies on customer experience management. In ASEAN: A Review. *2022 IEEE International Conference on Computing (ICOCO)* (pp. 364–368). IEEE.

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research, 9*(2), 204–215.

Al-Ashban, A. A., & Burney, M. A. (2001). Customer adoption of tele-banking technology: The case of Saudi Arabia. *International Journal of Bank Marketing, 19*(5), 191–201.

Alashoor, T., & Baskerville, R. (2015). The privacy paradox: The role of cognitive absorption in the social networking activity. In Carte, T., Heinzl, A., & Urquhart, C. (Eds.), *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015 [1558].* Association for Information Systems. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1558&context=icis2015

Ali, S., Wang, G., White, B., & Fatima, K. (2019). Libra critique towards global decentralized financial system. In *Smart City and Informatization: 7th International Conference, iSCI 2019, Guangzhou, China, November 12–15, 2019, Proceedings 7* (pp. 661–672). Springer Singapore.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469–490.

Armantier, O., Doerr, S., Frost, J., Fuster, A., & Shue, K. (2021). Whom do consumers trust with their data? US survey evidence. *BIS Bulletin, 42*.

Ayuso, M., Guillen, M., & Marín, A. M. P. (2016). Using GPS data to analyse the distance travelled to the first accident at fault in pay-as-you-drive insurance. *Transportation Research Part C: Emerging Technologies, 68*, 160–167.

Ayuso, M., Guillen, M., & Nielsen, J. P. (2019). Improving automobile insurance ratemaking using telematics: Incorporating mileage and driver behaviour data. *Transportation, 46*, 735–752.

Baecke, P., & Bocca, L. (2017). The value of vehicle telematics data in insurance risk selection processes. *Decision Support Systems, 98*, 69–79.

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society, 34*(1), 49–57.

Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers' privacy calculus: The PRICAL index development and validation. *International Journal of Research in Marketing, 39*(1), 20–41.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*, 1017–1041.

Bergemann, D., & Bonatti, A. (2019). Markets for information: An introduction. *Annual Review of Economics, 11*, 85–107.

Bernard, H. R., & Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches*. Sage.

Bijlsma, M., van der Cruijsen, C., & Jonker, N. (2024). Not all data are created equal-Data sharing and privacy. *Applied Economics*, *56*(11), 1250–1267.

Blakesley, I. R., & Yallop, A. C. (2020). What do you know about me? Digital privacy and online data sharing in the UK insurance sector. *Journal of Information, Communication and Ethics in Society, 18*(2), 281–303.

Bolgov, R., & Filatova, O. (2022). ICT support of Open Budget as a tool to fight corruption: Cases of EAEU countries. In *Proceedings of the Central and Eastern European eDem and eGov Days* (pp. 73–77).

Briones de Araluze, G. K. (2022). Why are open banking models in Europe underperforming? *Journal of Payments Strategy & Systems, 16*(4), 347–357.

Brown, J. R., & Finkelstein, A. (2007). Why is the market for long-term care insurance so small? *Journal of Public Economics, 91*(10), 1967–1991.

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Weber, R. H. (2020). The road to RegTech: The (astonishing) example of the European Union. *Journal of Banking Regulation, 21*, 26–36.

Campo, B. D., & Antonio, K. (2022). Insurance pricing with hierarchically structured data: An illustration with a workers' compensation insurance portfolio. arXiv preprint http://arxiv.org/abs/2206.15244

Chan, R., Troshani, I., Rao Hill, S., & Hoffmann, A. (2022). Towards an understanding of consumers' FinTech adoption: The case of Open Banking. *International Journal of Bank Marketing, 40*(4), 886–917.

Chang, S. Y., Bodolica, V., Hsu, H. H., & Lu, H. P. (2023). What people talk about online and what they intend to do: related perspectives from text mining and path analysis. *Eurasian Business Review*, *13*(4), 931–956.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Hussain, Z. (2023). Usage of smartphone for financial transactions: From the consumer privacy perspective. *Journal of Consumer Marketing, 40*(2), 193–208.

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

Cho, V., & Hung, H. (2011). The effectiveness of short message service for communication with concerns of privacy protection and conflict avoidance. *Journal of Computer-Mediated Communication, 16*(2), 250–270.

Ciunova-Shuleska, A., & Palamidovska-Sterjadovska, N. (2019). Model of satisfaction involving affect and personality traits. *Eurasian Business Review, 9*(4), 485–500.

de Koker, L., & Goldbarsht, D. (2022). Financial technologies and financial crime: Key developments and areas for future research. *Financial technology and the law: Combating financial crime* (pp. 303–320). Springer International Publishing.

De Pascalis, F. (2022). The journey to Open Finance: Learning from the Open Banking movement. *European Business Law Review, 33*(3), 397–420.

Delcaillau, D., Ly, A., Papp, A., & Vermet, F. (2022). Model transparency and interpretability: Survey and application to the insurance industry. *European Actuarial Journal, 12*(2), 443–484.

Demmers, J., Van Dolen, W. M., & Weltevreden, J. W. (2018). Handling consumer messages on social networking sites: Customer service or privacy infringement? *International Journal of Electronic Commerce, 22*(1), 8–35.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dratva, R. (2020). Is open banking driving the financial industry towards a true electronic market? *Electronic Markets, 30*(1), 65–67.

Duan, S. X., & Deng, H. (2021). Hybrid analysis for understanding contact tracing apps adoption. *Industrial Management & Data Systems, 121*(7), 1599–1616.

Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*, 359–396.

European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/

European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/

European Commission. (2021). Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions. Retrieved from https://eur-lex.europa.eu/resource.html

European Commission. (2022). Data Act: Commission proposes measures for a fair and innovative data economy. Retrieved from https://ec.europa.eu/commission/presscorner/detail/

European Commission. (2023). Retrieved from https://finance.ec.europa.eu/events/data-sharing-between-authorities-eu-financial-services-2023-02-16_en

Farrow, G. S. (2020). An application programming interface model for open banking ecosystems. *Journal of Payments Strategy & Systems, 14*(1), 75–91.

FCA. (2022). Retrieved from https://www.fca.org.uk/publication/feedback/fs21-7.pdf

Feng, R., Laeven, R. J., & Lin, X. S. (2022). Editorial to the virtual special issue on emerging risks and insurance technology. *Insurance: Mathematics and Economics*, *107*, 418–421.

Fernandes, T., & Costa, M. (2023). Privacy concerns with COVID-19 tracking apps: A privacy calculus approach. *Journal of Consumer Marketing, 40*(2), 181–192.

Festic, N., Latzer, M., & Smirnova, S. (2021). Algorithmic self-tracking for health: User perspectives on risk awareness and coping strategies. *Media and Communication, 9*(4), 145–157.

Fox, G. (2020). To protect my health or to protect my health privacy? A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology, 71*(9), 1015–1029.

Fox, G., van der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2022). Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology, 73*(7), 944–967.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704–1723.

Giovannetti, E., & Hamoudia, M. (2022). The interaction between direct and indirect network externalities in the early diffusion of mobile social networking. *Eurasian Business Review, 12*(4), 617–642.

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications, 29*, 64–77.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703–705.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review, 102*(3), 349–353.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.

Gozman, D., Hedman, J., & Olsen, K. S. (2018). Open banking: Emergent roles, risks & opportunities. In *European Conference on Information Systems.*

Grassi, L., Figini, N., & Fedeli, L. (2022a). How does a data strategy enable customer value? The case of FinTechs and traditional banks under the open finance framework. *Financial Innovation, 8*(1), 1–34.

Grassi, L., Lanfranchi, D., Faes, A., & Renga, F. M. (2022b). Do we still need financial intermediation? The case of decentralized finance–DeFi. *Qualitative Research in Accounting & Management*, *19*(3), 323–347.

Gupta, S., Lehmann, D. R., & Stuart, J. A. (2004). Valuing customers. *Journal of Marketing Research, 41*(1), 7–18.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior, 95*, 295–306.

Handel, P., Skog, I., Wahlstrom, J., Bonawiede, F., Welch, R., Ohlsson, J., & Ohlsson, M. (2014). Insurance telematics: Opportunities and challenges with the smartphone solution. *IEEE Intelligent Transportation Systems Magazine, 6*(4), 57–70.

He, Z., Huang, J., & Zhou, J. (2023). Open banking: Credit market competition when borrowers own the data. *Journal of Financial Economics, 147*(2), 449–474.

Hirsch, D. D. (2013). The glass house effect: Big Data, the new oil, and the power of analogy. *Maine Law Review, 66*, 373.

Hosein, P. (2024). A data science approach to risk assessment for automobile insurance policies. *International Journal of Data Science and Analytics*, *17*(1), 127–138.

Howcroft, B., Hamilton, R., & Hewer, P. (2002). Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *International Journal of Bank Marketing, 20*(3), 111–121.

Hsieh, J. K., & Li, H. T. (2022). Exploring the fit between mobile application service and application privacy. *Journal of Services Marketing, 36*(2), 264–282.

Huang, Z. X., & Huang, T. Y. (2023). Privacy calculus theory in the Digital Government Context: The case of Taiwan's New eID Policy. *Social Science Computer Review, 41*(5), 1745–1766.

Husnjak, S., Peraković, D., Forenbacher, I., & Mumdziev, M. (2015). Telematics system in usage based motor insurance. *Procedia Engineering, 100*, 816–825.

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance, 64*, 101826.

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the economics of data. *American Economic Review, 110*(9), 2819–2858.

Kandil, O., Dessart, L., Standaert, W., & Bosma, M. (2024). A Framework to improve the digital customer experience in complex services. *Services Marketing Quarterly,* 1–29.

Kang, J. W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps: A privacy calculus perspective. *International Journal of Contemporary Hospitality Management*, *31*(2), 734–752.

Karjaluoto, H., Mattila, M., & Pento, T. (2002). Factors underlying attitude formation towards online banking in Finland. *International Journal of Bank Marketing, 20*(6), 261–272.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635.

Klumpes, P. (2023). Coordination of cybersecurity risk management in the UK insurance sector. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *48*(2), 332–371.

Lanfranchi, D., & Grassi, L. (2021). Translating technological innovation into efficiency: The case of US public P&C insurance companies. *Eurasian Business Review, 11*(4), 565–585.

Lanfranchi, D., & Grassi, L. (2022). Examining insurance companies' use of technology for innovation. *The Geneva Papers on Risk and Insurance-Issues and Practice, 47*(3), 520–537.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62–71.

Liu, Z., Shan, J., & Pigneur, Y. (2016). The role of personalized services and control: An empirical evaluation of privacy calculus and technology acceptance model in the mobile context. *Journal of Information Privacy and Security, 12*(3), 123–144.

Lledó, J., & Pavía, J. M. (2022). Dataset of an actual life-risk insurance portfolio. *Data in Brief, 45*, 108655.

Loi, M., Hauser, C., & Christen, M. (2022). Highway to (digital) surveillance: When are clients coerced to share their data with insurers? *Journal of Business Ethics, 175*, 7–19.

Lv, H., & Wan, Y. (2019). Contracting for online personalisation services: An economic analysis. *Journal of the Operational Research Society, 70*(7), 1149–1163.

McCrea, M., & Farrell, M. (2018). A conceptual model for pricing health and life insurance using wearable technology. *Risk Management and Insurance Review, 21*(3), 389–411.

Mishra, P., Pandey, C. M., Singh, U., Keshri, A., & Sabaretnam, M. (2019). Selection of appropriate statistical methods for data analysis. *Annals of Cardiac Anaesthesia, 22*(3), 297.

O'Leary, K., O'Reilly, P., Nagle, T., Filelis-Papadopoulos, C., & Dehghani, M. (January). The sustainable value of open banking: Insights from an open data lens. In *54th Hawaii International Conference on System Sciences, Kauai, Hawaii, USA, 4–8 January 2021* (pp. 5891–5901). University of Hawai'i at Manoa.

Or, C. K., & Karsh, B. T. (2009). A systematic review of patient acceptance of consumer health information technology. *Journal of the American Medical Informatics Association, 16*(4), 550–560.

Paluch, S., & Tuzovic, S. (2019). Persuaded self-tracking with wearable technology: carrot or stick? *Journal of Services Marketing*, *33*(4), 436–448.

Parker, R. G., & Parrott, R. (1995). Patterns of self-disclosure across social support networks: Elderly, middle-aged, and young adults. *The International Journal of Aging and Human Development, 41*(4), 281–297.

Parkhimovich, O., & Minina, E. (2017). Insight provoking multi-criterial visualization of Russian open finance data: from data acquisition to processing and analyzing. In *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance* (pp. 552–553).

Perkmann, M., & Schildt, H. (2015). Open data partnerships between firms and universities: The role of boundary organizations. *Research Policy, 44*(5), 1133–1143.

Piquero, N. L., Cohen, M. A., & Piquero, A. R. (2011). How much is the public willing to pay to be protected from identity theft? *Justice Quarterly, 28*(3), 437–459.

Rahman, M. S. (2019). Does privacy matters when we are sick? An extended privacy calculus model for Healthcare Technology adoption behavior. In *2019 10th International Conference on Information and Communication Systems (ICICS)* (pp. 41–46). IEEE.

Ramdani, B., Rothwell, B., & Boukrami, E. (2020). Open banking: The emergence of new digital business models. *International Journal of Innovation and Technology Management, 17*(05), 2050033.

Rastogi, S., Sharma, A., & Panse, C. (2020). Open banking and inclusive growth in India. *Indian Journal of Ecology, 47*(spl), 75–79.

Ravula, P. (2022). Monetary and hassle savings as strategic variables in the ride-sharing market. *Research in Transportation Economics, 94*, 101184.

Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics, 34*(2), 569–582.

Robinson, P. J., & Botzen, W. W. (2022). Setting descriptive norm nudges to promote demand for insurance against increasing climate change risk. *The Geneva Papers on Risk and Insurance-Issues and Practice,* 1–23.

Rowan, M., & Dehlinger, J. (2014). Observed gender differences in privacy concerns and behaviors of mobile device end users. *Procedia Computer Science, 37*, 340–347.

Ryu, S. (2023). Coupon or my privacy: How consumers choose to disclose their personal information and accept mobile location-based advertising (LBA) through privacy calculus. *Journal of Consumer Behaviour, 22*(5), 1158–1172.

Saliba, B., Spiteri, J., & Cortis, D. (2021). Insurance and wearables as tools in managing risk in sports: Determinants of technology take-up and propensity to insure and share data. *The Geneva Papers on Risk and Insurance-Issues and Practice,* 1–21.

Simonson, I. (2005). Determinants of customers' responses to customized offers: Conceptual framework and research propositions. *Journal of Marketing, 69*(1), 32–45.

Smith, S. S. (2021). Decentralized finance & accounting-implications, considerations, and opportunities for development. *International Journal of Digital Accounting Research*, *21*.

Standaert, W., & Muylle, S. (2022). Framework for open insurance strategy: Insights from a European study. *The Geneva Papers on Risk and Insurance-Issues and Practice, 47*(3), 643–668.

Standaert, W., Muylle, S., & Cumps, B. (2020). Opening the gates: A framework for an open banking strategy. *Journal of Digital Banking, 4*(4), 364–376.

Stoeckli, E., Dremel, C., & Uebernickel, F. (2018). Exploring characteristics and transformational capabilities of InsurTech innovations to understand insurance value creation in a digital world. *Electronic Markets, 28*, 287–305.

Suoranta, M., & Mattila, M. (2004). Mobile banking and consumer behaviour: New insights into the diffusion pattern. *Journal of Financial Services Marketing, 8*, 354–366.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248–273.

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems, 165*, 113881.

Tenopir, C., Allard, S., Douglass, K., Aydinoglu, A. U., Wu, L., Read, E., et al. (2011). Data sharing by scientists: practices and perceptions. *PLoS ONE, 6*(6), e21101.

Tran, C. D., & Nguyen, T. T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technology in Society, 67*, 101755.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society, 3*(1), 2056305116688035.

Tsarenko, Y., & Rooslani Tojib, D. (2009). Examining customer privacy concerns in dealings with financial institutions. *Journal of Consumer Marketing, 26*(7), 468–476.

Urueña-Mejía, J. C., Gutierrez, L. H., & Rodríguez-Lesmes, P. (2023). Financial inclusion and business practices of microbusiness in Colombia. *Eurasian Business Review, 13*(2), 465–494.

Van den Boom, F. (2023). Regulating telematics insurance–enabling car data-driven innovations. *European Business Law Review*, *34*(1).

Van Dijk, J. (2020). *The digital divide*. John Wiley & Sons.

Verbelen, R., Antonio, K., & Claeskens, G. (2018). Unravelling the predictive power of telematics data in car insurance pricing. *Journal of the Royal Statistical Society Series C (applied Statistics), 67*(5), 1275–1304.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior, 120*, 106763.

von Entreß-Fürsteneck, M., Buchwald, A., & Urbach, N. (2019). Will I or will I not? Explaining the willingness to disclose personal self-tracking data to a health insurance company.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing, 80*(6), 97–121.

Wiegard, R., Guhr, N., Krylow, S., & Breitner, M. H. (2019). Analysis of wearable technologies' usage for pay-as-you-live tariffs: Recommendations for insurance companies. *Zeitschrift Für Die Gesamte Versicherungswissenschaft, 108*, 63–88.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52.

Yang, Q., Gong, X., Zhang, K. Z., Liu, H., & Lee, M. K. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management, 52*, 102065.

Yuan, Y. P., Tan, G. W. H., & Ooi, K. B. (2022). Does COVID-19 pandemic motivate privacy self-disclosure in mobile FinTech transactions? A privacy-calculus-based dual-stage SEM-ANN Analysis. *IEEE Transactions on Engineering Management*.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance (DEFI). *Journal of Financial Regulation, 6*, 172–203.