sciendo Economics and Business Review
https://www.ebr.edu.pl
Vol. 9 (1), 2023: 119-141
https://doi.org/10.18559/ebr.2023.1.5

Privacy frontiers in customers' relations with banks

Dariusz Piotrowski[1]

Abstract

The widespread use of digital technologies in banking allows banks to obtain and analyse huge amounts of data from different communication channels. While this phenomenon is conducive to improving the quality of services it also increases the risk of privacy breaches. The aim of this study is to identify what factors determine consumer acceptance of banks' use of public access personal data found on social media accounts. The results indicate the importance of the financial incentive and consumers' assessment of banks' information activities regarding the processing of personal data. Determinants relating to the technological sophistication of respondents were also found to be significant, with a particular focus on the ethical evaluation of decisions made by Artificial Intelligence algorithms. The results of the work may be used by banks in practice to adapt the area of personal data management to the requirements of e-privacy and Trustworthy Artificial Intelligence.

Keywords

- privacy
- personal data processing
- Artificial Intelligence
- banking ethics
- social media

JEL codes: A13, G21, O33

Article received 13 January 2023, accepted 7 April 2023.

This research was funded by Nicolaus Copernicus University in Toruń under Grant no. FUTURE/07/2020.

Suggested citation: Piotrowski, D. (2023). Privacy frontiers in customers' relations with banks. *Economics and Business Review*, *9*(1), 119–141. https://doi.org/10.18559/ebr.2023.1.5

[1] Department of Financial Management, Faculty of Economic Sciences and Management, Nicolaus Copernicus University, ul. Gagarina 13a, 87-100 Toruń, Poland, darius@umk.pl, https://orcid.org/0000-0001-8482-8064.

Introduction

The provision of financial services involves the processing of customers' personal data. This area has changed dramatically as a result of the significant involvement of banks in the digital transformation of the economy (Rodrigues et al., 2022). Customers' intensive use of e-banking and in particular mobile banking applications has significantly increased the amount and type of data collected by banks (Wottrich et al., 2019). These institutions also use external sources of customer data such as social media and geo-location (Cambridge Centre for Alternative Finance, 2020). The data is usually collected in digital form, which allows for in-depth analysis using Artificial Intelligence (OECD, 2021). Machine learning algorithms detect consumer behaviour patterns and anomalies that can be used to improve service quality and better match customer preferences and expectations (Financial Stability Board, 2017; Giza & Wilk, 2021). The implementation of Artificial Intelligence technology by banks has also created an opportunity for banks to offer financial services to customers using chatbots and robo-advisors (Hasal et al., 2021; Waliszewski & Zięba-Szklarska, 2020). However, market regulators have noticed that the processing of personal data can be a source of many irregularities; hence, for instance, banks were obliged to protect customer privacy (Hacker, 2021).

The aim of this study is to identify what factors determine consumer acceptance of banks' use of public access personal data found on social media accounts. It analysed factors relating to customers' experiences and attitudes towards the use of financial services and digital technologies. In particular it considered the legal and ethical aspects of the processing of personal data and the importance of a financial incentive. The present work makes a significant contribution to information privacy research through the use of original empirical data showing consumers' perspectives on the processing of personal data by banks. The paper uses a contextual analysis of consumer privacy the advantages of which were pointed out by Acquisti, Brandimarte et al. (2015). The work is novel thanks to the inclusion in the research of variables relating to decisions made by Artificial Intelligence operating within the bank. The uniqueness of the research relates to the ethical aspects of the assessment made by consumers regarding the results of the processing of personal data using Artificial Intelligence. A multilevel ordered logit model was used to identify statistically significant variables affecting the willingness to share a wide range of personal data with banks. This model is an appropriate research tool due to the qualitative nature of the dependent variable.

The remainder of this paper is organised as follows. In the next section a literature review is conducted focusing on the processing of personal data and privacy issues in the digital world. The subsequent section provides a de-

scription of data obtained through the CATI (computer-assisted telephone interviewing) survey, presents the research hypothesis and the research method used in the analysis. Next the estimation results are presented identifying determinants of the willingness to share personal data with banks and a discussion is carried out indicating their originality. The main conclusions as well as the theoretical and practical implications are presented in the last part of the paper.

1. Institutional background

The issue of personal data processing has been widely regulated in the European Union. This section indicates the most important legal regulations that banks are obliged to comply with. According to Articles 11–14 of the Directive regarding anti-money laundering and countering the financing of terrorism (European Parliament, 2018), when establishing a business relationship a bank is obliged to identify the customer and verify the customer's identity on the basis of documents, data, or information obtained from a reliable and independent source. By doing so the bank initiates the processing of customers' personal data. Article 4(1) of the General Data Protection Regulation (GDPR, 2016) defines personal data as any information relating to an identified or identifiable natural person whereby an identifiable natural person is one who can be identified, directly or indirectly and in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Banks obtain customers' personal data through access to official documents proving customers' identities as well as through the provision of financial services to them. In addition, to the customer's name, gender, date and place of birth, place of residence and nationality, banks are able to obtain data on the financial situation in the customer's household, shopping and payment habits and assets by analysing transactions made on personal accounts, credit card accounts and in the process of granting credit and monitoring repayment (Credit Suisse, 2020). When analysing the sources of obtaining data on consumers it is worth mentioning the new opportunities created by Payment Services Directive 2 (2015). Open banking allows for the exchange of data between banks and third parties helping financial institutions to gain a better understanding of consumer attitudes, behaviour, and preferences. The increasing use of digital technology and in particular mobile devices and applications has given banks access to consumer data

well beyond the realm of finance, i.e., personal biometric data such as fingerprints, face shape, images of the iris or retina which are the source of sensitive and confidential information (Nguyen & Dang, 2019; Piotrowska, Polasik, & Piotrowski, 2017).

The acquisition of customers' personal data is one step within the broader processing of personal data which includes activities such as recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The GDPR (2016) provisions impose an obligation to process personal data lawfully, fairly and in a transparent manner in relation to the data subject. Furthermore, the processing of data should comply with specific principles: 'purpose limitation'—the personal data obtained may be used only for a well-defined purpose; 'data minimization'—the purpose of processing should be achieved using as little personal data as possible; 'correctness'—the data used must be accurate and up-to-date; 'storage limitation'—the manner in which personal data are stored should allow for the identification of the natural person necessary for the specified purpose; 'integrity and confidentiality'—ensuring adequate security of personal data; 'accountability'—identifying the person responsible within the entity for the processing of personal data. Detailed requirements also clarify the issue of obtaining consent to process personal data. The data processor should be able to demonstrate that the consumer has given informed consent (Betzing et al., 2020). The fulfilment of this condition is facilitated by the clear separation of consent to the processing of personal data from other statements as well as the clear and plain language used in the statement (Muravyeva et al., 2020).

Customer contact with the bank through electronic banking channels creates the conditions for the generation of an enormous amount of data, while the electronic form of the data favours their collection, storage and analysis to extract hidden information. The banking sector uses AI mainly in areas such as customer service, client acquisition and risk management (Cambridge Centre for Alternative Finance, 2020; Gancarczyk et al., 2022). More specific applications include reporting and record management, data analytics, credit scoring, compliance, AML/CFT (Anti-Money Laundering / Counter Financing of Terrorism), KYC (Know Your Customer) checks, anti-fraud, chatbots, robo-advisors, biometric authentication and personalised products (Korol & Fotiadis, 2022; OECD, 2021).

Processing personal data using digital technologies requires banks to meet additional regulatory requirements. Thus pursuant to Article 13.2f of the GDPR (2016), the controller of personal data that will be used to make automated decisions is obliged to inform the data subject of this together with an indication of the modalities of such decision-making and the envisaged consequences of such personal data processing for the data subject.

With this requirement in mind the European Commission (2019) formulated recommendations addressed to those responsible for the development, deployment and use of AI which aim to ensure that Artificial Intelligence operates in accordance with the law and ethical principles. The regulations contained in the Ethics Guidelines for Trustworthy AI refer to universal principles and values such as the right to privacy, fairness, transparency, accountability and confidentiality. The closing years of the 20th century saw a tremendous increase in the importance of the Internet in the functioning of societies and economies almost all over the world (Yamin, 2019). The European Union, recognising the need to regulate the area of electronic communications networks and services, adopted the Framework Directive (2002), which applied, inter alia, to electronic banking services. The development of digital technologies and their growing use meant that interpersonal communication services, including Internet telephony, instant messaging and email services were also regulated in subsequent years (Recast, 2018). The indicated regulations as well as the Directive on privacy and electronic communications (2002) and the Proposal concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (European Commission, 2017) set out requirements for the processing of personal data in electronic communications to ensure the protection of consumer privacy. However, none of the aforementioned regulations explicitly define the concept of privacy, hence the need to refer to the literature in this regard.

2. Literature review

2.1. Privacy in electronic communications

According to Belanger and Crossler (2011) and Yee (2017) privacy refers to a person's ability to control the processing of data concerning them. Loh (2018) emphasises the importance of autonomy of decisions and life choices in the distribution of information. Pollach (2005) defines informational privacy as the right of individuals to decide when, to whom, how and to what extent information concerning them will be shared. Elsewhere Martin (2016) considers privacy as a kind of social contract obliging individuals to follow rules adopted in the community relating to access to information and how it is used. Nissenbaum (2009) and Martin (2011) present a contextual view of privacy where the situations in which individuals find themselves and the relationships between them affect which behaviour is acceptable and which

is treated as an invasion of privacy. Floridi (2006) points out that the analysis of information privacy should take into account the cultural context, the responsibility of the individual taking into account legal norms, religious beliefs and epistemic practices as well as the definition of the adequate scope of the right to privacy so that the processing of any personal data is not defined as an invasion of privacy. According to Margulis (2003) the development of digital technologies has also made the issue of privacy in the public sphere important.

The privacy literature covers the collection, sharing and use of data. Obar and Oeldorf-Hirsch (2020) show that privacy policies of electronic service providers are infrequently read because they are often difficult to comprehend and too long. With the cognitive problems of consumers in mind Solove (2013) criticises the privacy self-management approach to cookie acceptance. He suggests embracing paternalistic regulations regarding the collection, use and disclosure of personal data. Elsewhere the work of Pentina et al. (2016) analyse the phenomenon of the privacy paradox. It is characterised by a contradiction between the stated concern for privacy protection and the actual actions of consumers that pose a risk of privacy violation (Barth & De Jong, 2017). Acquisti and Grossklags (2006) point out that consumers tend to take into account short-term benefits when making decisions about sharing personal data while showing little concern for the protection of privacy that is in fact based on managing information over the long term. Consumers' behaviour can also be explained by the fact that they attribute little value to the data they transmit while failing to recognise the serious privacy risks in doing so. Conversely, Tene and Polonetsky (2013) believe that consumers are aware of the value that personal data represent. They are therefore prepared to offer access to them in return for a specific consideration which may take the form of money or, for example, access to selected electronic services (Fife & Orjuela, 2012). Moreover, in the Balaban and Mustățea (2021) study respondents assessed the said practice as fair given the current practice of data collection by providers of electronic communication services. As a counterpoint to the views presented Roessler (2015) points to the moral limitations of treating personal data as tradable goods.

2.2. Data disclosure in social media

The development of digital technologies and in particular the Internet has given society wide and rapid access to large amounts of information. The advent of social media has broadened insights into the lives of others and has additionally created the opportunity to share information from one's own life with multiple audiences (Shadbolt & Hampson, 2018). Various factors influen-

cing the use of social media have been identified in the literature. Muhammad, Dey and Weerakkody (2018) reported privacy and security, personal behaviour, social influence and technological solutions. Whiting and Williams (2013) emphasised the importance of relaxation, expression of opinions and intrinsic psychological needs of entertainment. The study by Trivedi et al. (2018) showed the importance of a desire to connect, communicate and collaborate with others.

The benefits of a social media presence have also been recognised by banks (Kirakosyan, 2015). These institutions use social platforms in the area of marketing, as a communication channel, to find out consumers' opinions on the services provided and the execution of financial transactions (Parusheva, 2017). Twitter, Facebook, LinkedIn, and YouTube are used to present banking products and to gauge consumer reactions. Information gleaned from social media provides a better understanding of consumer needs and contributes to banks' competitiveness (Askar et al., 2022).

The use of social media is also analysed in the literature in the context of privacy. Research includes users' willingness to share information online, the extent of disclosure of personal information and how access to information is controlled (Cheung et al., 2015). Some social media users overlook the fact that their activity on the platforms leaves numerous digital footprints. They show a lack of due consideration about what content they post online (Azucar et al., 2018). The willingness to disclose data about oneself and the low assessment of privacy risks stems from a false belief in one's own effectiveness in managing privacy (Chen & Chen, 2015). The attitude presented hampers the management of personal data and significantly increases the risk of privacy breaches (Acquisti, Taylor et al., 2016).

The literature also points to more conscious and deliberate actions by social media users in terms of privacy management. The study by Shane-Simpson et al. (2018) showed a different extent of self-disclosure and public or private profile preference depending on whether the respondent was a Facebook, Twitter, or Instagram user. Elsewhere a study by Xie and Karan (2019) yielded that social media user behaviour varied depending on the type of information. Users displayed greater propensity to share everyday life and entertainment information in contrast to personal contact information where significant restrictions were applied to its dissemination. The paper by Stutzman, Gross and Acquisti (2013) revealed that Facebook users increased the amount of personal information shared with friends while applying restrictions on this to other users. McGuinness and Simon (2018) additionally highlighted the practice of social media users applying varying online privacy settings.

The research also identified factors influencing the intention to share digital footprints on social media platforms. Muhammad, Dey, Syed Alwi et al. (2022) analysed constructs such as: perceived relative advantage, perceived

social influence, perceived control, enjoyment, self-enhancement and trust, highlighting the importance of the latter factor. Mutimukwe et al. (2019) further considered the effect of organisational privacy assurances. Keith et al. (2013) examined the impact of variables such as perceived benefits, perceived privacy risks, intent to disclose and awareness of privacy risks. They discovered that disclosure intentions are determined by perceived privacy risks on a larger scale than by perceived benefits. Elsewhere, Dinev and Hart (2006) proved that there is a negative impact of perceived privacy risk on an individual's intent to disclose information through an application while it is positive with perceived benefits. According to Chai and Kim (2012), the propensity to give information may also depend on the ethical culture—the norms and values shared in a social media community. Chai (2020) found that users' information-sharing behaviour on social media is positively associated with ethical culture, while information privacy is perceived negatively.

Another area of research is related to the ethical aspects of personal data processing (Floridi & Taddeo, 2016). Social media are a source of scores of information about their users contained in photos, videos, and comments. The use of Artificial Intelligence techniques makes it possible to learn about the behaviour and preferences of specific individuals including sensitive areas such as racial and ethnic origin, religious and worldview beliefs, political views, as well as feelings and health status (Batrinca & Treleaven, 2015). Culnan and Bies (2003) pointed out that consumers' willingness to share data depends on the perceived fairness of corporate information practices. The need to consider ethical issues when managing digital privacy was also highlighted by Sarathy and Robertson (2003). Cai et al. (2020) recognised the threat of advertising attacks while Steppe (2017) and Zuiderveen Borgesius and Poort (2017) cited price discrimination as an example of the use of personal data that is incompatible with consumer interests. Behrendt and Loh (2022) pointed to the danger of algorithmic discrimination when using big data and Artificial Intelligence in automated decision-making. The problems of discrimination, unequal treatment and exclusion associated with the use of digital technologies in the field of data processing were also signalled by Royakkers et al. (2018).

Artificial Intelligence is increasingly being used in decision-making that includes an ethical component (Bejger & Elster, 2020). This raises the need for moral programming of the technology and the definition of responsibility for decisions made by Artificial Intelligence (Martin, 2019). According to Wernaart (2021), programming should relate to everyday cases where the results of decisions have more subtle consequences going beyond the laboratory or life-or-death situations. He also draws attention to the need to distinguish between moral programming and the ethical issues arising from its application. Millar (2017) analyses the matter from another angle pointing to different expectations and assessments of AI performance depending on

whether the situation / decision involves high or low stake ethical settings. Although artificial morality has been explored in the literature (Misselhorn, 2018), the ultimate assessment of actions, including decisions made using Artificial Intelligence algorithms is made by consumers with varying degrees of moral sensitivity or moral imagination (Reynolds, 2008).

3. Research methodology

The use of the computer-assisted telephone interview method allowed the author to obtain the empirical data used in the study. The survey was conducted by a professional research agency—Interactive Research Center Sp. z o.o. in October 2020. It included a sample of 911 Polish citizens aged 18–65. The sample was representative of Polish society in terms of gender, age and place of residence. Table 1 presents the variables used in the analysis and the structure of the responses given by the respondents. The dependent variable Data Sharing (Y) refers to consumers' attitudes towards banks' use of public access personal data found on their social media accounts. This variable reveals consumers' attitudes towards privacy. The explanatory variables relate to the socio-demographic characteristics of the respondents, the experience of using banking services, the respondents' attitudes towards ICTs and the bank's activities in the area of personal data processing as well as the ethical aspects of decisions made using Artificial Intelligence technology. The Exchange Rate and Drink variables included in the study were designed in such a way that the first indicates the benefits perceived by consumers from the operation of Artificial Intelligence in banks, while the second variable allows us to know the respondents' evaluation of a situation where the decision of Artificial Intelligence generates negative consequences for the individuals whose personal data were analysed.

The paper adopts the following research hypothesis: The use of a financial incentive significantly increases consumer acceptance of banks' use of public access personal data found on social media accounts. A multilevel ordered logit model was used to identify the variables most influencing consumers' decisions to provide data to banks for analysis. Such a model is usually applied when the dependent variable takes a number of finite and discrete values that contain ordinal information (Arfan & Khan, 2017; Wooldridge, 2010). It is assumed that the ordered response variable Y can take on any of the $J + 1$ values $0, 1, \ldots, J$, and it is supposed that underlying the observed response is a latent variable (Cottrell & Lucchetti, 2014):

$$Y^{\star} = X\beta + \varepsilon$$

Table 1. Characteristics of variables and the structure of responses obtained in CATI (*N* = 911)

Variable	Variable description	Responses	%
Data Sharing (Y)	Willingness to consent to the bank's analysis of the content posted on a public profile in social media	Definitely not Rather not It's hard to say Rather yes Definitely yes	71.7 16.4 7.6 3.0 1.3
Gender	Gender	Female Male	50.2 49.8
Age Group	Age group	18–24 25–34 35–44 45–54 55–65	8.5 23.9 24.7 20.0 22.9
Residence	Place of residence	Village Village-suburban area City up to 20,000 inhabitants City with 20,001–100,000 inhabitants City with 100,001–500,000 inhabitants City over 500,000 inhabitants	28.8 7.9 13.3 20.2 17.8 12.0
Education	Education level	Primary and below Lower secondary and basic vocational Secondary Higher	2.0 18.5 40.4 39.1
Internet Use	Frequency of using Internet	No or less than once a year Several times a year Several times a month A few times a week Several times a day	3.7 1.4 6.4 12.7 75.8
Social Media Use	Frequency of using social media	No or less than once a year Several times a year Several times a month A few times a week Several times a day	22.5 1.3 5.9 15.2 55.1
Internet or Mobile Banking Use	Frequency of using Internet or mobile banking services	No or less than once a year Several times a year Several times a month A few times a week Several times a day	15.5 0.9 18.7 40.0 24.9
Investment Advisory	Use of bank advisory services related to savings and investment	Yes No	33.5 66.5

Variable	Variable description	Responses	%
Loan Advisory	Use of bank advisory services related to obtaining financing in the form of a loan	Yes No	53.9 46.1
Processing Rules	The rules for the processing of personal data of customers are presented by banks in a concise and understandable way	Definitely not Rather not It's hard to say Rather yes Definitely yes	5.3 17.6 24.2 42.6 10.3
Exchange Rate	The bank, using Artificial Intelligence, analyzed the client's transactions and noticed that he often travelled abroad, which is why it offered favorable exchange rates. Do you consider the bank's operation as ethical?	Definitely not Rather not It's hard to say Rather yes Definitely yes	9.8 13.5 20.5 38.6 17.6
Drink	The bank, using Artificial Intelligence, analyzed the customer's transactions and noticed that in recent months he was buying alcohol very often and therefore refused to grant the customer a loan. Do you consider the bank's operation as ethical?	Definitely not Rather not It's hard to say Rather yes Definitely yes	41.6 31.8 15.9 8.3 2.4
Cash Bonus	Consent for the bank to analyze the content posted on the social media account in return for receiving a one-off amount of PLN 500 from the bank	Definitely not Rather not It's hard to say Rather yes Definitely yes	54.3 21.4 13.3 8.0 3.0
Social Media Ethics	Obtaining information about consumers by the bank by analyzing photos, videos and comments posted by them in public access on social media is ethical	Definitely not Rather not It's hard to say Rather yes Definitely yes	42.7 29.8 17.1 8.2 2.2

Source: Own research.

The "cut points" $\alpha_1 < \alpha_2 < \cdots < \alpha_J$ are defined, such that:

$$\begin{cases} Y = 0 \text{ if } Y^* \le \alpha_1 \\ Y = 1 \text{ if } \alpha_1 < Y^* \le \alpha_2 \\ \vdots \\ Y = J \text{ if } Y^* > \alpha_J \end{cases}$$

Using the Gretl software package for econometric analysis the unknown parameters α_j and βs were estimated based on the statistical method of ma-

ximum likelihood estimation. The backward elimination procedure identified significant variables in the multilevel ordered logit model. In the first phase of the study, all the variables considered were applied to the model. In subsequent phases of the iterative procedure the least significant variables were removed from the model. Finally, only the variables for which the z-statistic was significant at the 5% level remained in the model (see Table 2).

Table 2. Estimation results of the multilevel ordered logit model for the variable Data Sharing (Y)

Variable	Coefficient	Standard error	z-statistic	Probability
Internet Use	0.287472	0.113337	2.536	0.0112
Loan Advisory	−0.544405	0.173809	−3.132	0.0017
Processing Rules	0.262246	0.0716915	3.658	0.0003
Social Media Ethics	0.723483	0.0801545	9.026	<0.0001
Drink	0.251227	0.0821264	3.059	0.0022
Cash Bonus	0.763749	0.0734577	10.40	<0.0001
Cut1	6.60922	0.677397	9.757	<0.0001
Cut2	8.29479	0.705207	11.76	<0.0001
Cut3	9.14571	0.725231	12.61	<0.0001
Cut4	10.6251	0.785624	13.52	<0.0001
Mean dependent variable	1.385291			
S.D. dependent variable	0.810483			
Log-likelihood	−590.0483			
Akaike criterion	1200.097			
Schwarz criterion	1248.242			
Hannan–Quinn criterion	1218.478			
Number of cases 'correctly predicted'	691 (75.9%)			
Likelihood ratio test	409.257 [0.0000]			

Source: Own research.

4. Results

A preliminary analysis of the data in Table 1 suggests that the vast majority of respondents are familiar with modern ICTs. As many as 88.5% of re-

spondents use the Internet at least a few times a week while 70.3% use social media at least a few times a week. With regard to banking products 64.9% of respondents use Internet or mobile banking at least a few times a week. Less experience among respondents was observed for the other financial services included in the analysis. Advice on savings and investment products was sought by 33.5% of respondents while advice on sources of finance was used by 53.9%. The analysis of the empirical data on personal data processing reveals that a clear majority of respondents have a negative attitude towards sharing data publicly available on social media accounts with banks (a total of 88.1% of 'definitely not' and 'rather not' responses against a total of 4.3% of 'definitely yes' and 'rather yes' responses). Despite the introduction of an element of financial gratification of PLN 500 (approximately EUR 105) in exchange for giving consent only 11% of respondents would be willing to allow banks to analyse data held on social media accounts while the majority of respondents (75.7%) still express a negative stance on this issue. Against this backdrop respondents' assessments of the rules on the processing of personal data appear favourable for banks—52.9% of consumers present the view that the regulations applied by the banks are concise in form and understandable in content. Negative feelings in this respect (answers 'definitely not' and 'rather not') were expressed by 22.9% of respondents.

The next three variables included in the study combine issues of personal data processing including the use of Artificial Intelligence and the ethical evaluation of automated decisions made by banks. For the Social Media Ethics variable 72.5% of respondents perceive as unethical the banks' actions of extracting customer information from data in the public domain on their social media accounts. Far fewer respondents—10.4%—rate the aforementioned behaviour of banks as ethical, with the answer 'definitely yes' given by only 2.2% of respondents. Similarly the vast majority of respondents (a total of 73.4% of 'definitely not' and 'rather not' responses) rate as unethical the actions of Artificial Intelligence in denying credit to a person suspected of alcohol abuse. The AI decision was met with understanding (answers 'definitely yes' and 'rather yes') by only 10.5% of respondents. Assessments on the ethicality of decisions made by Artificial Intelligence when the outcome of the analyses is satisfactory to consumers are decidedly different. Offering favourable exchange rates was viewed positively by 56.2% of respondents while the decision of Artificial Intelligence was rated as unethical by 23.3% of respondents.

The proper aim of the study was to determine the factors significantly influencing the Data Sharing (Y) variable. The results of the logit model estimation are presented in Table 2. They indicate a statistically significant positive relationship between the variables: Internet Use, Processing Rules, Drink, Social Media Ethics and Cash Bonus against the variable Data Sharing and negative for the variable Loan Advisory. The estimation results can be considered sa-

tisfactory due to the high percentage of 'correctly predicted' cases (75.9%). When evaluating the aforementioned result, it should also be taken into account that, for the Data Sharing variable, respondents were able to choose from five response options.

5. Discussion

The multilevel ordered logit model estimation yields that a rise in respondents' Internet usage increases the acceptance of banks' use of public access personal data found on their social media accounts. Active Internet users are able to perceive the different forms of presentation of personal data (documents, comments, photos, videos), the different contents of the data (information on family, friends, leisure activities, political leanings), the positive and negative effects of their processing (fame, recognition, resentment, jealousy, hatred) and the speed with which information spreads in the modern world. According to the adaptive cognition theory of social network participation (Hu & Ma, 2010) active users are more predisposed to estimate the positive and negative consequences of their choices in the area of personal data processing due to their acquired knowledge and experience. Apart from rationality in privacy management the result obtained in the study can also be explained in a different way. Consumers' acceptance of banks' use of data extracted from social media may be related to the fact that they do not see this decision as a threat to their privacy or rate a privacy breach as highly improbable (Flender & Müller, 2012).

The significance of the Social Media Ethics variable indicates that an increase in the perception that banks' actions in handling data obtained from social media are ethical has a positive effect on the acceptance of banks' use of such data. As mentioned earlier people using social media are able to choose their account settings regarding access to published data. This access can be limited to a group of friends, or unlimited, public. It is then possible for any person or entity to obtain the data held in the account. Moreover regardless of the choice of settings the account holder essentially loses control over the subsequent processing of this data. It can therefore be assumed that people who knowingly post certain content on their accounts and knowingly set access to the data as public will accept the bank's actions regarding the processing of this data and perceive them as ethical. This attitude is in line with the communication privacy management theory (Petronio, 2002) where each individual subjectively sets the boundaries of his or her privacy.

Informed consumers should be knowledgeable about the processing of personal data. They can gain this knowledge by observing the online beha-

viour of other users but the primary source is knowledge of the regulations governing the processing of personal data in a given institution (in the case of this study—in banks). The significance of the Processing Rules variable indicates that familiarity with privacy policies and a positive assessment of their content and form increases respondents' acceptance of banks' processing of data obtained from social media.

The initial survey found that the use of financial gratification as a means of encouraging consumers to share their personal data is likely to impact just 11% of respondents. Despite this estimation of the multilevel ordered logit model identified the Cash Bonus variable as a significant determinant of consumers' decisions to accept banks' use of data held in social media accounts. It can therefore be concluded that the result obtained in the study confirms the theory of immediate gratifications (Du et al., 2019).

Of the two variables directly related to the operation of Artificial Intelligence in banks only the Drink variable proved statistically significant. Thus, the belief in the ethical nature of the operation of Artificial Intelligence in the case Artificial Intelligence makes a decision that benefits the consumer (Exchange Rate) does not sufficiently reinforce the willingness of respondents to share a wider catalogue of personal data with banks. Only the fact that a consumer assesses as ethical a decision made by Artificial Intelligence with adverse consequences for the consumer significantly increases the willingness to accept banks' use of data posted on social media (Ashworth & Free, 2006). However, this assessment depends on ethical sensitivity (Chowdhury, 2019; Toti et al., 2021) which is an individual characteristic of each consumer depending on demographics, psychological and ethical experience factors (Schwartz, 2016). According to Hagerty and Rubinov (2019), when we analyse how the performance of Artificial Intelligence is assessed we should also take into account the cultural and social context.

The last variable that is statistically significant is Loan Advisory. Estimation of the model showed that the fact that respondents receive advice on sources of finance negatively affects their willingness to accept banks' use of data posted on social media. The first thing to note when analysing the result obtained is the weaker negotiating position of the customer vis-à-vis the bank in the case of loans and borrowings as opposed to savings and investment products. Respondents wishing to finance their consumer or investment expenditure with a loan must take into account a bank's potential refusal. The second point is that if a consumer declares to have received credit or loan advice they have probably undergone a credit assessment procedure. Having to provide the bank with a significant amount of personal data as well as waiting for the result of the bank's assessment of their financial situation may have been a source of negative experience for many respondents. Another matter worth considering is consumers' perception of inappropriate practices by banks in the area of financial advice. Indeed Piotrowski's (2022) study found

a negative impact of the use of financial advisory on the ethical assessment of banks operating in Poland. The last issue that needs to be taken into account when analysing the Loan Advisory variable is consumers' fear of the bank knowing their true financial situation. Artificial Intelligence algorithms analysing data from social media accounts can detect signs of deterioration in the financial situation of consumers which in turn can lead to the refusal of credit, the introduction of additional collateral, or the demand for immediate repayment of already granted credit. However, Artificial Intelligence may fail to see signs of deterioration in the debtor's financial situation and decide against deferring loan instalments. The respondents' logic presented above fits into the privacy calculus theory (Kehr et al., 2015) where privacy decisions are made rationally by comparing the benefits and costs associated with the dissemination of information.

Conclusions

Privacy refers to the extent of an individual's control over the processing of their personal data. In this study, consumers' attitudes to privacy were analysed in the context of banks' use of publicly accessible personal data found on social media accounts. The results of the research helped identify factors behind consumers' acceptance of the loss of privacy to banks. Preliminary analysis showed that the vast majority of Polish residents aged 18–65 do not consent to the use of the aforementioned data by banks. It can therefore be concluded that if banks are to obtain consent to access a wider catalogue of personal data they will have to convince consumers of the potential benefits on the one hand and the absence of serious related risks on the other. This task seems very difficult in the case of those who value privacy but almost impossible in the case of those who are negative towards the banking sector. In the case of these consumers the reluctance to use social media data can be linked to the banks' unethical practices and their information and negotiating advantage vis-à-vis their customers which would be further strengthened after consenting to the analysis of said data.

The main part of the research which was based on the estimation of a multilevel ordered logit model showed the significance of the Cash Bonus variable, thus confirming the research hypothesis. While it is true that the introduction of a financial incentive significantly influences consumers' consent to data analysis this factor only determines the decisions made by a relatively small proportion of respondents.

The study yields the conclusion that a high level of knowledge about the processing of personal data and awareness of the consequences of this pro-

cess favours consumers' decision to give up some privacy. The respondents see the ethical aspects of personal data processing as equally important. Consumers with a strong conviction in the ethicality of Artificial Intelligence and guided by ethical principles themselves express a willingness for letting banks use data posted on social media accounts.

Consumers also recognise the concerns surrounding the potential for AI algorithms to cause them harm. However, these concerns are not only related to the potentially harmful effects of algorithms but also to the unethical behaviour of consumers themselves. This is because those intending to conceal their actual financial situation from the bank realise that subjecting a broader catalogue of personal data to analysis may be to their disadvantage.

In conclusion the research conducted in this article has shown that more attention needs to be paid to ethical matters in the theoretical and empirical analysis of privacy issues. This aspect assumes particular importance in the context of the increasingly widespread social and economic use of Artificial Intelligence which also extends to the financial services sector. The type of data collected, the manner in which they are acquired and in particular the decisions made by machine learning algorithms will raise difficult ethical dilemmas concerning consumer privacy in the near future thus prompting further research work in this area.

The results of the study underpin applicative conclusions for banks. The first recommendation relates to the outcome of Artificial Intelligence. Banks should increase consumer awareness of how Artificial Intelligence works, how algorithms make decisions and the effects of these decisions on consumers. In general this demand translates into banks implementing the concept of explainable Artificial Intelligence (XAI).

> *Banks should provide customers with an understandable and accessible form of explaining the pathway to AI decisions*.

Artificial Intelligence is increasingly making decisions with a specific ethical component. Beyond clear-cut cases it can be a problem for Artificial Intelligence to judge specific behaviours as appropriate or undesirable. The difficulty in evaluation stems from the multitude of possible situations giving rise to ethical dilemmas, the influence of context on the behaviour of the actors analysed and the diversity of social norms used in the evaluation. Harmonising banks' criteria for assessing customers using AI could be a helpful solution. Therefore, the second recommendation was formulated as follows:

> *Ethical standards developed by the bank reflecting the main social norms of the customers served should apply in AI training*.

The limitations of the research stem from the fact that only representatives of the Polish population were included. However, in the author's assessment the topicality of the e-privacy issue and the application of Artificial

Intelligence in the processing of personal data makes the conclusions formulated in the paper universal.

The literature studies and the results of the empirical study provide the basis for formulating suggestions for future research. In the author's opinion it is useful to find out what consumers understand by privacy, what data processing activities they approve of and what they consider to be an invasion of privacy. Consumer expectations of trustworthy AI should also be identified.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–515.

Acquisti, A., & Grossklags, J. (2006). Privacy and rationality. In K. J. Strandburg & D. S. Raicu (Eds.), *Privacy and technologies of identity. A cross-disciplinary conversation* (pp. 15–29). Springer.

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492.

Arfan, M., & Khan, R. (2017). Ordinal logit and multilevel ordinal logit models: An application on wealth Index MICS-Survey Data. *Pakistan Journal of Statistics and Operation Research*, *13*(1), 211–226.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*(2), 107–123.

Askar, M. A. E., Aboutabl, A. E., & Galal, A. (2022). Utilizing social media data analytics to enhance banking services. *Intelligent Information Management*, *14*, 1–14.

Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and Individual Differences*, *124*, 150–159.

Balaban, D., & Mustățea, M. (2021). Privacy concerns in mobile communication. A user's perspective. *Philobiblon*, *26*, 101–114.

Barth, S., & De Jong, M. (2017). The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Batrinca, B., & Treleaven, P. C. (2015). Social media analytics: A survey of techniques, tools and platforms. *AI & Society*, *30*(1), 89–116.

Behrendt, H., & Loh, W. (2022). Informed consent and algorithmic discrimination—is giving away your data the new vulnerable? *Review of Social Economy*, *80*(1), 58–84.

Bejger, S., & Elster, S. (2020). Artificial Intelligence in economic decision making: How to assure a trust? *Ekonomia i Prawo. Economics and Law*, *19*(3), 411–434.

Belanger, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2020). The impact of transparency on mobile privacy decision making. *Electronic Markets*, *30*(3), 607–625.

Cai, Y., Yee, G., Gu, Y., & Lung, Ch. H. (2020). Threats to online advertising and countermeasures: A technical survey. *Digital Threats: Research and Practice*, *1*(2), 1–27.

Cambridge Centre for Alternative Finance. (2020). *Transforming paradigms. A global AI in financial services survey*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2020-ccaf-ai-in-financial-services-survey.pdf

Chai, S. (2020). Does cultural difference matter on social media? An examination of the ethical culture and information privacy concerns. *Sustainability*, *12*(19), 8286.

Chai, S., & Kim, M. (2012). A socio-technical approach to knowledge contribution behavior: An empirical investigation of social networking sites users. *International Journal of Information Management*, *32*(2), 118–126.

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19.

Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279–299.

Chowdhury, R. M. M. (2019). The moral foundations of consumer ethics. *Journal of Business Ethics*, *158*(1), 585–601.

Cottrell, A., & Lucchetti, R. (2014). *Gretl user's guide. Gnu regression, econometrics and time-series library*. https://www.academia.edu/31887034/Gretl_Users_Guide_Gnu_Regression_Econometrics_and_Time_series_Library

Credit Suisse. (2020). *Data protection information*. https://www.credit-suisse.com/media/assets/private-banking/docs/uk/data-privacy-policy.pdf

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342.

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

Directive on privacy and electronic communications. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

Du, J., Kerkhof, P., & Van Koningsbruggen, G. M. (2019). Predictors of social media self-control failure: immediate gratifications, habitual checking, ubiquity, and notifications. *Cyberpsychology, Behavior, and Social Networking*, *22*(7), 477–485.

European Commission. (2017). Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

European Commission. (2019). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Parliament. (2018). Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the pre-

vention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*, 1–10.

Financial Stability Board. (2017, November 1). *Artificial Intelligence and machine learning in financial services*. https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/

Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: the privacy paradox revisited. In J. Busemeyer, F. Dubois, A. Lambert-Mogiliansky & M. Melucci (Eds.), *Quantum interaction. Lecture notes in computer science* (pp. 148–159). Springer-Verlag.

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology*, *8*(3), 109–119.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, *374*(2083), 20160360.

Framework Directive. (2002). Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=pl

Gancarczyk, M., Łasak, P., & Gancarczyk, J. (2022). The fintech transformation of banking: Governance dynamics and socio-economic outcomes in spatial contexts. *Entrepreneurial Business and Economics Review*, *10*(3), 143–165. https://doi.org/10.15678/EBER.2022.100309

General Data Protection Regulation (GDPR). (2016). Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Giza, W., & Wilk, B. (2021). Revolution 4.0 and its implications for consumer behaviour. *Entrepreneurial Business and Economics Review*, *9*(4), 195–206. https://doi.org/10.15678/EBER.2021.090412

Hacker, P. (2021). A legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, *13*(2), 257–301.

Hagerty, A., & Rubinov, I. (2019). Global AI ethics: A review of the social impacts and ethical implications of Artificial Intelligence. *ArXiv*, 1907.07892. https://doi.org/10.48550/arXiv.1907.07892

Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V., & Ogiela, L. (2021). Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation. Practice and Experience*, *33*(1), e6426.

Hu, Q., & Ma, S. (2010). Does privacy still matter in the era of web 2.0? A qualitative study of user behavior towards online social networking activities. *PACIS*, *2*, 591–602.

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.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, Ch. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Kirakosyan, K. (2015). Social media usage in banking industry and its managerial view: Case study for Mexican banking system. *Journal of Economic and Social Development*, *2*(1), 34–43.

Korol, T., & Fotiadis, A. K. (2022). Implementing Artificial Intelligence in forecasting the risk of personal bankruptcies in Poland and Taiwan. *Oeconomia Copernicana*, *13*(2), 407–438.

Loh, W. (2018). A practice-theoretical account of privacy. *Ethics and Information Technology*, *20*(2), 233–247.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261.

Martin, K. (2011). Information technology and privacy: conceptual muddles or privacy vacuums? *Ethics and Information Technology*, *14*(4), 267–284.

Martin, K. (2016). Understanding privacy online: development of a social contract approach to privacy. *Journal of Business Ethics*, *137*(3), 551–569.

Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, *160*(4), 835–850.

McGuinness, D. M., & Simon, A. (2018). Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites. *IFLA Journal*, *44*(3), 203–222.

Millar, J. (2017). Ethics settings for autonomous vehicles. In P. Lin, R. Jenkins & K. Abney (Eds.), *Robot ethics 2.0. From autonomous cars to artificial intelligence* (pp. 20–34). Oxford University Press.

Misselhorn, C. (2018). Artificial morality. Concepts, issues and challenges. *Society*, *55*(2), 161–169.

Muhammad, S. S., Dey, B. L., Syed Alwi, S. F., Kamal, M. M., & Asaad, Y. (2022), Consumers' willingness to share digital footprints on social media: The role of affective trust. *Information Technology & People*, *36*(2), 595–625.

Muhammad, S. S., Dey, B. L., & Weerakkody, V. (2018). Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: A systematic review of literature. *Information Systems Frontiers*, *20*(3), 559–576.

Muravyeva, E., Janssen, J., Specht, M., & Custers, B. (2020). Exploring solutions to the privacy paradox in the context of e-assessment: Informed consent revisited. *Ethics and Information Technology*, *22*(3), 223–238.

Mutimukwe, Ch., Kolkowska, E., & Grönlund, Å. (2019). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Nguyen, T., & Dang, T. (2019). Privacy preserving biometric-based remote authentication with secure processing unit on untrusted server. *IET Biometrics*, *8*(1), 79–91.

Nissenbaum, H. (2009). *Privacy in context: Technology, privacy, and the integrity of social life*. Stanford University Press.

Obar, J., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147.

OECD. (2021). *Artificial Intelligence, machine learning and big data in finance: opportunities, challenges, and implications for policy makers*. https://www.oecd.org/finance/artificial-intelligence-machine-learning-big-data-in-finance.htm

Parusheva, S. (2017). Social media banking models: A case study of a practical implementation in banking sector. *Economic Studies*, *3*, 125–141.

Payment Services Directive 2. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=PL

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Piotrowska, A. I., Polasik, M., & Piotrowski, D. (2017). Prospects for the application of biometrics in the Polish banking sector. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *12*(3), 501–518.

Piotrowski, D. (2022). Consumer perceived ethicality of banks in the era of digitalisation: The case of Poland. *Economics and Business Review*, *22*(1), 90–114.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, *62*(3), 221–235.

Recast. (2018). Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

Reynolds, S. J. (2008). Moral attentiveness: who pays attention to the moral aspects of life? *Journal of Applied Psychology*, *93*(5), 1027–1041.

Rodrigues, A., Ferreira, F., Teixeira, F., & Zopounidis, C. (2022). Artificial Intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60*, 101616.

Roessler, B. (2015). Should personal data be a tradable good? On the moral limits of markets in privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 141–161). Cambridge University Press.

Royakkers, L., Timmer, J., Kool, L., & Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, *20*(2), 127–142.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*(2), 111–126.

Schwartz, M. S. (2016). Ethical decision-making theory: An integrated approach. *Journal of Business Ethics*, *139*(4), 755–776.

Shadbolt, N., & Hampson, R. (2018). *The digital ape: How to live (in peace) with smart machines*. Scribe.

Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior*, *86*, 276–288.

Solove, D. J. (2013). Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, *33*(6), 768–785.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41.

Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*, 239–273.

Toti, J. F., Diallo, M. F., & Huaman-Ramirez, R. (2021). Ethical sensitivity in consumers' decision-making: The mediating and moderating role of internal locus of control. *Journal of Business Research*, *131*, 168–182.

Trivedi, N., Asamoah, D. A., & Doran, D. (2018). Keep the conversations going: Engagement-based consumer segmentation on online social service platforms. *Information Systems Frontiers*, *20*(2), 239–257.

Waliszewski, K., & Zięba-Szklarska, M. (2020). Robo-advisors as automated personal financial planners—SWOT analysis. *Journal of Finance and Financial Law*, *3*(27), 155–173.

Wernaart, B. (2021). Developing a roadmap for the moral programming of smart technology. *Technology in Society*, *64*(10), 101466.

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research: An International Journal*, *16*(4), 362–369.

Wooldridge, J. (2010). *Econometric analysis of cross section and panel data*. MIT Press.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2019). App users unwittingly in the spotlight: A model of privacy protection in mobile apps. *Journal of Consumer Affairs*, *53*(3), 1056–1083.

Xie, W., & Karan, K. (2019). Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising*, *19*(3), 187–201.

Yamin, M. (2019). Information technologies of 21st century and their impact on the society. *International Journal of Information Technology*, *11*(4), 759–766.

Yee, G. O. M. (2017). Visualization and prioritization of privacy risks in software systems. *International Journal on Advances in Security*, *10*(1&2), 14–25.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, *40*(3), 347–366.