A C T A U N I V E R S I T A T I S N I C O L A I C O P E R N I C I
DOI: http://dx.doi.org/10.12775/AUNC_ZARZ.2018.012 ZARZĄDZANIE XLV–NR 1 (2018)

Pierwsza wersja złożona 20.02.2018
Ostatnia wersja zaakceptowana 29.03.2016

ISSN (print) 1689-8966
ISSN (online) 2450-7040

Karolina Małagocka[*]

WHO IS THE PAYER? THE VALUE OF PRIVATE INFORMATION FROM THE PERSPECTIVE OF CUSTOMERS AND COMPANIES.

A b s t r a c t: In the knowledge-based economy data has become an important part of building competitive advantage. The private and public sectors are demonstrating enormous interest in acquiring increasingly greater amounts of information. From growing sets of unstructured, seemingly disconnected data, one can extract information that can not only identify a given person, but also determine their demographic, socio-geographical, behavioral or mental characteristics, learn their shopping preferences, track their daily schedules and habits. In this sense, it becomes attractive to any kind of company operating online, including advertisers. On the other side of the stage there are consumers for whom private information is a resource that can be exchanged for various tangible and intangible benefits. Irrespective of the fact that some of the private information is perceived as more sensitively or more worthy than other, customers, as evidenced by numerous studies, choose money over data. The value of information depends on who owns it, who wants it, and who and how much is willing to pay for it. The aim of the paper is to present the concept of the value of private information from the perspective of customers and companies.

K e y w o r d s: privacy, privacy concerns, Privacy Segmentation Index, willingness-to-protect, willingness-to-accept

J E L C l a s s i f i c a t i o n: L21

INTRODUCTION

As a result of technological progress, the development of the online channel and the commonly available access to the Web and mobile devices, not only the amount but also the quality of data that can be acquired is on the rise. Data processing and storage methods are also rising quickly. At the same time, the methods of aggregating and analyzing data, as well as the methods of making business decisions based on this data, are becoming complex enough that information asymmetry between managers and customers is increasing. In the knowledge-based economy, data has become an important part of building

[*] Adres do korespondencji: Karolina Małagocka, Akademia Leona Koźmińskiego,Studia Doktornackie - Zarządzanie, ul. Jagiellońska 57/59, 03-301 Warszawa, k.malagocka@gmail.com

one's competitive advantage. The private and public sectors are demonstrating enormous interest in acquiring increasingly greater amounts of information concerning individuals, which in turn sparks concerns over the possibility of controlling citizens and consumers' private space.

Private information has become a new currency, or, as some journalists describe it in media publications, the "new oil". It represents a certain monetary value , as well as in terms of reflections on determining and defining one's own self. From growing sets of unstructured, seemingly disconnected data, one can extract information that can not only identify a given person, but also determine their demographic, socio-geographical, behavioral or mental characteristics, learn their shopping preferences, track their daily schedules, habits, etc.

Such data, collected in data bases and acquired from various sources, such as social media, cookies, credit card payments, sensor networks or various kinds of metadata, is not just a group of individual pieces of information in the classic sense of "raw numbers and facts reflecting a single aspect of reality" (Griffin, 1997, p. 676). Data does not have any inherent meaning; it takes on a specific meaning through the process of contextualization, categorization, calculation, correction and condensation (Devenport and Prusak, 1998, after: Grabowski, Zając, 2009). In this way, aggregated and processed data meets the definition of information as "data interpreted in a meaningful way" (Griffin, 1997, p. 676). Data becomes information after it is collected, ordered, and then structured, or optionally also linked with other data, as well as embedded within a context. In this sense, it becomes attractive to any kind of company operating online, including advertisers.

From a company's perspective, it enables to optimize its business processes, including acquiring and retaining customers, to develop pricing strategies, to target its offer at specific customers, etc. Due to the wide use of data transformed into private information, its value can be determined depending on who uses this data, and for what purpose.

To consumers, information regarding themselves is an asset that they have at their disposal, and any disclosure of such information is often seen as a cost of participation in the digital world (Ackerman, 2004; White, 2004). It is exchanged for specific benefits, sometimes expressed as monetary values, such as discounts, special prices, or as non-material benefits, such as belonging to specific communities or making everyday life easier through various applications that help users find specific places, make choices based on recommendation systems, etc. (Smith, Diev, Xu, 2011).

The value of their data to consumers clearly depends on their perceived sensitivity (Phelps, Nowak, Farrell, 2000). Consumers often have no full knowledge of how even rudimentary information can be linked with other data to create a relatively complete image of themselves as buyers or citizens.

Paradoxically, however, the only part of the process of exchanging data and turning it into information that can be used to define a person, which is not interested in paying for privacy protection is consumers themselves. This is demonstrated by both research on the gap between the willingness to protect and the willingness to accept (in this case, a specific amount of money in exchange for private information), as well as the low take up rate of online privacy solutions.

The goal of the author's reflections on the value of private information, including customers and companies' perspectives, against the backdrop of increasing information aggregation and exploitation possibilities is to discuss certain problems connected with customers' rising concerns over disclosing data. The paper shows how privacy itself and privacy concerns are perceived, the above-mentioned disproportion between consumers' willingness to protect data versus selling or exchanging it for benefits, as well as the marketing and managerial perspectives.

PRIVACY AND CUSTOMERS – IS EVERYBODY A FUNDAMENTALIST WHEN IT COMES TO PERSONAL DATA?

Privacy is described in literature in the fields of law, sociology, psychology, information technology and management. The authors emphasize the multidimensional nature of the phenomenon and its chronological variability, as well as its context-based interpretation. In their works, researchers use varied terminology, often relevant to their specific fields, using terms such as "personal data", "private information" or "private data". The differences between these descriptive phrases can be found most often in legal literature, because the concept of personal data was invented in the field of legal regulations. It is legal discourse that includes a hierarchy where private data includes personal data, but in other areas the two phrases are used interchangeably. In marketing terms, the definition of privacy should focus on personal data or, in other words, information about a person (Calin et al., 2012). In literature, catalogs of data regarded by respondents or researchers as private appear in two forms:

1. As data used to research behavior related to openness and privacy concerns,
2. As data indicated in research and regarded by respondents as private.

The perception of privacy has evolved over the years. One of the most often quoted, in both academic papers and popular science articles, definitions of privacy was proposed by one of the first scholars who studied the subject, A. Westin: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). In this sense, the author departs from the purely physical understanding of privacy, although chronologically, it is exactly physical privacy

that appeared first. It gradually became obvious that information about individuals and groups was being collected and used, therefore people started to view privacy in terms of information. In the United States or the European Union, individuals have no right to privacy in general. Thus, privacy is interpreted as the right to protect the information sphere, which is rooted in its definition as "the right to be left alone" (Warren and Brandeis, 1890). Information privacy seems to be much more relevant in virtual transactions. It includes an individual's ability to control the collection, use and distribution of information about themselves (Stone et al., 1983).

The U.S. privacy theoretician and researcher Westin, in his papers and a series of more than 30 studies, defined the concept of privacy further in terms of exerting control over the flow of information, and especially over the extent to which it is communicated to others. The author assumed that individuals in their relations with companies and government institutions have the need to maintain a certain level of privacy. He is the author of the segmentation that assumes the division into the three below-described categories (Harris, 2001):

1. Fundamentalists, i.e. people with a strong need to protect their private sphere, even at the cost of potential benefits. They are in favor of restrictive regulations in this area, and expect the government to provide support in customer-company relations. They only very rarely see any positive sides to sharing information about oneself.
2. Unconcerned, i.e. those who accept the situation where the exchange of goods is accompanied by the exchange of information. They most often do not see any need for excessive regulation in this area, nor do they feel overly used by companies, accepting the results of aggregating and processing of information in the form of personalized messages sent by companies.
3. Pragmatists, i.e. those who weigh the benefits of sharing private information against the costs. This group cares about the value of information, and expects being treated as a partner to the exchange, instead of companies taking advantage of the edge that new technologies may give them over individuals.

The author of the segmentation developed a way to assign individuals to specific groups that is known in literature as the Privacy Segmentation Index. It serves to define general privacy concerns, finding numerous applications in empirical research in this area. Currently, scholars, mostly international, use it as a benchmark to determine the attitude of each category to disclosing private information, and to estimate the related costs (e.g. Woodruff, 2014).

Westin was the first to define privacy as a state that may be accessible for evaluation in empirical research. His categories were based on identifying the construct that is privacy concerns. His interpretation continues to inform reflections on the subject of privacy. According to the definition proposed by

Westin, and later accepted by the creators of an academically approved scale used to analyze privacy concerns, the term is understood as *the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*, (Westin, 1967 after Malhotra et al., 2004, p. 337). In short, the term "privacy concerns" refers to concerns over the possible loss of privacy as a result of disclosing information about oneself (Xu et al., 2008).

In literature, privacy concerns are associated with beliefs about risks and benefits of disclosure and so-called trusting beliefs. Customer trust is built through the feeling that the private information that has been disclosed will not be misused or used contrary to the entrusting party's best interest, and that it will be stored safely (Dinev and Hart, 2006). Individuals differ greatly in the intensity of experiencing online privacy concerns, which is illustrated at the level of general concerns by the division into categories in the Privacy Segmentation Index. Research so far has shown that customers may be more inclined to disclose their identity in exchange for monetary prices; then, their privacy concern level is moderated by the value of the prize (Steinfeld, 2015). At the same time, there have been numerous studies using the survey method which point to strong concerns, especially over the collection and misuse of private information (Min and Kim, 2015; Min, 2016).

Customers differ from each other in the degree of their privacy concerns; at the same time, they decide to disclose some information in various situations. In literature, customers' decision-making process aiming to achieve cost-efficiency between the benefits of disclosing information and the risk seen as a cost is known as privacy calculus (Dinev and Hart, 2006). It draws on certain principles of economic theories. Risk estimation among customers is based on defining the probability of negative consequences of information disclosure and its perceived harmfulness. Privacy calculus assumes a significant degree of rationality of the person who makes the decision and who attempts to strike a balance between the perceived benefits and losses. Information is disclosed at all or to a larger extent only if the decision-maker believes that the benefits exceed the losses. Academic research on privacy is based on the principles of privacy calculus and examining the impact of the intensity and circumstances of disclosing private information (Krasnova et al., 2012). There is a significant body of research that demonstrates a positive influence of the familiarity of the party asking for information on the willingness to communicate it, and a negative effect of the perceived risk on the intent to conduct a transaction (e.g. Norberg et al. 2007; Pavlou, 2003). While privacy calculus is a concept is rooted in reflections on privacy, it is not free of criticism. Especially controversial is the rational aspect of decision-making among customers, who may not have full knowledge concerning information processing methods, who may be subject to various emotions, and at least some

of whom may be not equipped with the capabilities necessary to judge the possibilities that modern technology provides. The lack of balance in information access between customers and suppliers is mentioned by researchers in Poland and internationally (Acquisti, 2016; Sznajder, 2014).

Putting privacy calculus on the map of reflections on privacy, one needs to take into account a construct that is one of the best described and well established in literature, i.e. privacy paradox. It describes the gap between the attitudes and behavior exhibited by customers in the area of online privacy. The phenomenon can be explained through customers' tendencies toward discounting future risk with a strong drive toward instant gratification (Acquisti, 2004), the reliability based on trust in a brand or company (Metzger, 2004; Norberg et al., 2007), as well as certain gaps in consumers' knowledge (Dommeyer and Gross, 2003; Pötzsch, 2008). However, it has been increasingly proposed that this paradox does not exist, and that it is impossible to draw conclusions from customers' behavior on the basis of their explicit privacy attitudes (Woodruff et al., 2014). This is the reason why privacy calculus understood as customers' decision-making process constitutes the theoretical frameworks of most empirical studies.

The value of private information can be judged based on different factors. The willingness to disclose it is related not only to the degree of concern, but also to positive stimuli, such as trust in the asker, positive experience with a brand or company, as well as prizes and benefits offered in exchange for data. It does not change the fact, however, that judging value is a complex and often ambiguous process due to negative aspects such as data misuse, database leaks or, last but not least, the disproportion between companies and customers' capabilities to process and store data.

PRIVACY AND CUSTOMERS – WHO IS THE PAYER?

Customers who are users of products or services offered by companies that to a large extent work through the virtual channel differ when it comes to judging the value of private information. While at least some can effectively estimate the value of their data, and even expect an adequate reward for them, much fewer are willing to pay for privacy protection. Unlike giants such as Google or Facebook, which monetize access to information about millions of users, there are companies whose business model is based on opposite principles, building customer value upon high privacy guarantees, such as FastMail versus Gmail or Zoho as an alternative to Google Docs. Nevertheless, they remain within a market niche, and the dominant model relies on access without fees expressed in currencies while profit is gained from the data acquired.

Customers' willingness to pay for protection of private information expressed in the term "willingness-to-protect" (WTP) is juxtaposed with the willingness

to accept a specific amount for sharing private information, i.e. willingness-to-accept (WTA). Research undertaken by scholars dealing with behavioral economy, including privacy economics, revealed a gap between these two values (e.g. Acquisti, 2004, 2016). Conclusions from the Acquisti and Grossklags studies prove that people prefer money over data; they not only agree to be paid for data more often than they pay for information protection, but also the amount offered in exchange can be incredibly low compared to the estimated price of the information. In the above-mentioned study, 25 cents was enough, while Malhotra offered 10 dollars in his scenarios, and as proven in an analysis of the results, the customers found both sums convincing (Acquisti and Grossklags, 2007; Malhotra, 2004). No such research has been carried out in Poland so far.

WTP was examined in the context of users' willingness to pay for avoiding privacy abuse, for example, they asked Facebook users how much they would pay for protecting personal information. The responses suggested that nearly half of the respondents would not be willing to pay for such protection while realizing the value of the information disclosed in the social medium (Spiekermann et al., 2012). In turn, WTA was analyzed in the context of data leaks. The respondents were asked to estimate the value of certain information that had been leaked online, according to the study scenario (Kim and Yeo, 2010). On the other hand, Acquisti proposes a study with closed questions, to which the answer is either "yes" or "no", or specifying a certain sum of money. It is this study that suggests that while a significant number of respondents would decide to sell their data for as little as 25 cents, they would not spend even this much on protecting them (Aquisti and Grossklags, 2007).

PRIVACY AND COMPANIES – INFORMATION IN THE EYES OF MANAGERS

In the times of digital transformation, characterized by continuous appreciation of data, it is regarded as an economic category and resource that determines a company's competitiveness, development, or even survival. A consequence of the progress and popularization of technology is a change of the development paradigm, i.e. a shift from industrial economy to knowledge-based economy. A fourth production factor has emerged alongside the traditionally defined factors of land, capital and labor, i.e. information (Pomykalski, 2001), or in resultative terms, data and information that constitute knowledge (Muraszkiewicz, 2002). The factor that creates value is information defined as a company's material asset or non-material asset. Essentially, any company can be seen as a group of assets, including material assets such as money or technical means, and non-material assets such as know-how, brand, trademarks, the reputation of a company or its products and services, corporate culture, as well as information (Penc, 1997).

They also determine the strengths and weaknesses of a company (Fazlagić, 2004), therefore some of them can be seen as more important than others, or even strategically important, i.e. offering a clear market advantage.

In turn, the starting point for perceiving information as a productive factor is the techno-economic paradigm describing a "shift from a technology based primarily on cheap inputs of energy to one predominantly based on cheap inputs of information derived from advances in microelectronics and telecommunications technology" (G. Dosi et al. 1988, p.10 after Castells, 2007). Here, information is a resource, a type of fuel, and is processed using technologies. Drawing on this paradigm, information is seen as a currency in the digital world, and even increasingly often compared with oil, while analytic tools are likened to the role that the steam engine once fulfilled in human development. Alongside profitability or market share, close relationships with other entities, relationships with customers, and acquiring information, preferably unique or enabling non-standard choices, have become additional benchmarks for measuring the success of a company.

The basis for estimating the value of information is the amount for which market players are willing to buy it. This usually refers to customer data collected within sets called databases. More than once, the contents of a database determined the value of an entire company, as demonstrated by Facebook's acquiring WhatsApp or Instagram. As the value of information is seen in its usefulness for business activity and in increasing a company's operational range, the net value of the data collected by a company is taken into account. According to comparative studies, companies often believe that it is unprofitable to carry out the lengthy process of acquiring, collecting and analyzing data if some services based on aggregation and processing can be purchased from external entities (Jaising et al., 2008). Cooperating with third parties is just one of the possible solutions. Another is to acquire other companies or invest in existing enterprises. The market value of some companies, especially those operating online, is closely related to the quality of their databases. In light of such valuation, WhatsApp was acquired for 19 billion dollars, or around 30 dollars per each of its 600 million users. The price was based not only on the amount of user data acquired by the company, but also on its quality, which enables future offers to be developed based on analyses of the data. There are further examples of estimating the market value of companies based on the user data, such as Microsoft's acquiring Minecraft or Facebook's acquiring Instagram.

Another method of estimating the value of information used by companies is to estimate the profit that their customers make currently and their potential profit in the future, which is described as the Customer Lifetime Value. To this end, managers and decision-makers often use data about transactions, such as value, frequency or recurrence. The Customer Lifetime Value is based not only

on the amount of data acquired by a company but also on its quality, which may inform the company's future relationships with customers. This approach combines the maximum scope of evaluation of customer data with relationship potential.

PRIVACY AND COMPANIES – WHAT WILL MARKETERS DO WITH CUSTOMER INFORMATION?

Over the last two years, there has been a shift from focusing on the subject of an advertising message to focusing on target groups and their characteristics. People responsible for creating and carrying out marketing operations, similarly to other market participants, have realized the potential of data-informed decisions. Technologies such as cookies, RFID, GPS and sensor networks enable companies to identify users, as well as acquire detailed data concerning their behavior, daily schedules, choices, and shopping decisions (Ohkubo et al., 2005).

Due to the progress of technology, which enables collecting large amounts of high-quality data, analyzing human behavior to define their characteristics has become an important part of companies' operations, providing a foundation for dividing consumers into groups and predicting their behavior at the level of relatively accurately selected groups. Profiling is nothing more than generalizing combined with typifying. Effective marketing operations today require not only intuition and ingenuity but also selecting a suitable target group. This is especially important in the age of global markets, when it is often pointless to restrict a company's operations to its physical presence in a specific geographical location. An offer may be targeted at people with specific characteristics, who, however, do not necessarily have to inhabit the same area.

Personalized ads and offers today represent an added value for the customer. Their contents correspond to the recipient's preferences, future choices, behavior and lifestyle. One of the definitions of personalization quoted in literature describes it as the "ability to provide content and services that are tailored to individuals based on knowledge about their preferences and behaviors" (Adomavicius and Tuzhilin, 2005, p. 84). Personalization based on data analysis is possible when a company is capable of acquiring and processing customer information while customers are open to sharing information and using personalized services. Building a unique offer and raising the effectiveness of marketing operations in the age of digital economy rely on a company's ability to collect, analyze and use information. To this end, companies need access to as much data as possible. On the other hand, customers often welcome tailored offers while expressing their willingness to disclose as few facts from the sphere that they see as private as possible (Adomavicius and Tuzhilin, 2005). Communication in the virtual channel enables synthesis of data from a user's history of visited

sites, as well as data acquired by filling forms or based on analysis of behavior or preferences often expressed in another medium. It is worth noting that customers are not always a party to the exchange of data between entities operating online and sometimes have no control over sharing and aggregating of data collected (Acquisti, 2016). An example is combining the potential of social media targeting with the conclusions drawn from the behavior of customers visiting a given online store or web page. Data-informed marketing operations aim to display messages to users who belong to the group of people with increased probability of reacting positively and taking the step that the advertiser expects.

Profiling, personalization or behavioral targeting are some marketing trends that are closely connected with the use of private information which marketing managers deem critical to the success of their operations. In today's world, characterized by the high intensity of stimuli and information noise, where reliable and true messages are intermingled with fake news, and customers are bombarded with persuasive messages, the ability to rivet a customer's attention and make them take a specific action is not only a result of a good concept and an even better method of funding it. In order for such a message to be noticed, fished out of the sea of others, it seems necessary to target it at a precisely selected group about which the sender knows much more than the recipient often suspects.

LIMITATIONS AND POSSIBLE FUTURE RESEARCH AREAS

There is an extensive body of scientific work concerning privacy, privacy concerns and valuation of private information. Researchers take up this subject purely theoretically or in empirical reflections. In Polish literature, however, this subject has been discussed to a limited extent, which makes it impossible to base this text on analyses concerning Poland. The necessity of relying on reflections taken from foreign literature represents a limitation for this article. At the same time, the fact that privacy has numerous aspects, which makes it possible to present the phenomenon from different perspectives, makes it necessary to choose specific themes and narrow down the perspectives described to selected aspects.

One of the few studies dealing with the subject of privacy in Polish literature is the study by Mącik and Nalewajek (2014). The researchers analyzed the type of channel as an important variable which creates a context that impacts customers' perceived privacy. According to their results, the level of privacy concerns is significantly higher in the virtual channel. They did not research the impact of perceived privacy on estimating the value of information. As a result, there is a research gap encompassing empirical studies on valuating information, verifying whether customers estimate it differently or similarly, and how they motivate their behavioral decisions, understood as the willingness to disclose

data or enter into online transactions. It seems important to enrich the body of scientific work with further results of empirical research concerning Poland.

SUMMARY

The article, in line with its intended goal, discusses various perspectives on privacy in the digital world, as well as presents an outline of customers and business managers' perspectives when it comes to estimating the value of private information. The scope of access to private information by companies and the ways of using them are important subjects in the age of growing digital economy. Perceived benefits play a significant role in judging the pros and cons. Customers are willing to exchange private information even for minor benefits. At the same time, the degree of adoption of technologies used to protect the private sphere, such as VPN, is relatively low. Rationality in the decision-making process may be impaired by the lack of full knowledge about the mechanisms of acquiring, processing and using data. Simultaneously, operations aiming to increase a company's value, and win and build a market edge are based on whether it can effectively acquire and process private information. Also in marketing, the effectiveness of operations is often determined by clustering customers, aiming to better understand buyers' behavior, identifying new product development opportunities, or running suitable communication operations. It appears that today private information is prized at least by two groups: entities operating in the market and the recipients of their operations. Both groups see private information as an asset although they estimate its value differently.

REFERENCES:

Ackerman, M.S. (2004). Privacy in pervasive environments: Next generation labeling protocols. Personal and Ubiquitous Computing, 8, 430–439.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th ACM Conference on Electronic Commerce (pp. 21–29). New York: ACM Press.

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

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The economics of privacy.

Adomavicius,G., Tuzhilin, A. (2005) Personalization technologies: a process-oriented perspective, "Communications of the ACM", 48(10), 83-90

Bennett, C.J. (1995). The political economy of privacy: A review of the literature. Hackensack, NJ: „Center for Social and Legal Research".

Călin, V., Mihai, O., Carmen, A., Diana, D.(2012). Attitudes Of The Consumers Regarding Their Personal Data: What Has Changed Under The Recent Years?. " THE ANNALS OF THE UNIVERSITY OF ORADEA", 1222.

Castells, M. (2007). Społeczeństwo sieci, Wydawnictwo Naukowe PWN

Debatin, B., Lovejoy, J. P., Horn, A. K., Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. "Journal of Computer Mediated Communication", 15(1), 83-108.

Dinev, T. & Hart, P. (2006). An Extended Privacy Calculus Model for E - Commerce Transactions. "Information Systems Research",17 (1), 61- 80

Fazlagić, A. (2004). Zarządzanie wiedzą w sektorze publicznym [online]. eGov-pl – Forum Nowoczesnej Administracji Publicznej Pobrane z : www.fazlagic.egov.pl [dostęp: 27.02.2018]

Jaisingh, J., Barron, J., Mehta, S., & Chaturvedi, A. (2008). Privacy and pricing personal information. „European Journal of Operational Research", 187, 857–870.

Krasnova, H. et al. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture Intercultural Dynamics of Privacy Calculus. "Business & Information Systems Engineering", 4 (3), 127-135.

Kim, J.E., & Yeo, J. (2010). Valuation of consumers' personal information: A South Korean example. „Journal of Family and Economic Issues", 31, 297–306.

Malhotra, N.K. et al. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. "Information Systems Research",15 (4), 336 – 355

Muraszkiewicz M., (2002): Wybrane zagadnienia systemów baz danych, [w:] Efektywność zastosowań systemów informatycznych, pr. zb. pod red. J. K. Grabary i J. S. Nowaka, PTI, Wydawnictwa Naukowo - Techniczne.

Min, J. (2016). Personal information concerns and provision in social network sites: Interplay between secure preservation and true presentation. „Journal of the Association for Information Science and Technology", 67, 26–42.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. „Journal of the Association for Information Science and Technology", 66, 839–857.

Nalewajek, M., Mącik, R. (2014). Odczuwana prywatność a zachowania konsumenta w wirtualnym i fizycznym kanale sprzedaży w świetle wyników badań własnych. „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", (337), 109-119.

Norberg, P., Horne D. (2007) The privacy paradox: Personal information disclosure intentions versus behaviors. "Journal of Consumer Affairs". 41, no. 1: 100_26.

Ohkubo, M., Suzuki, K., Kinoshita, S. (2005) RFID privacy issues and technical challenges, "Communications of the ACM", 48(9), 66-71

Pavlou, P. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. "International Journal of Electronic Commerce", 7, no. 3: 101_34.

Penc, J. (1997). Leksykon biznesu. Placet.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. „Journal of Public Policy and Marketing", 19, 27–41.

Pomykalski, A. (2001). Zarządzanie innowacjami. Wydawnictwo Naukowe PWN

Preibusch, S. (2006). Personalized services with negotiable privacy policies. In PEP06, CHI 2006 workshop on privacy-enhanced personalization, Montreal, Canada (pp. 29-38).

Smith, H.J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. „MIS Quarterly", 35, 989–1015.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In Proceedings of the 3rd ACM Electronic Commerce Conference (pp. 38–47). New York: ACM Press.

Steinfeld, N. (2015). Trading with privacy: The price of personal information. „Online Information Review", 39, 923–938.

Sznajder, A. (2014). Technologie mobilne w marketingu. Oficyna Wolters Kluwer business.

Westin, A. F. (1967). Privacy and freedom Atheneum. New York

White, T.B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. „Journal of Consumer Psychology", 14, 41–51.

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., & Acquisti, A. (2014, July). Would a privacy fundamentalist sell their dna for $1000... if nothing bad happened as a result? the westin categories, behavioral intentions, and consequences. In Symposium on Usable Privacy and Security (SOUPS) (Vol. 4, p. 2).

Xu, X. et al. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In Proceedings of the International Conference on Information Sytems (ICIS 2008), Paris, France.

KTO JEST PŁATNIKIEM? WARTOŚĆ PRYWATNYCH INFORMACJI Z PERSPEKTYWY KLIENTÓW I FIRM

Abstrakt: W gospodarce opartej na wiedzy dane stały się ważnym elementem budowania przewagi konkurencyjnej. Sektor prywatny i publiczny wykazują ogromne zainteresowanie pozyskiwaniem coraz większej ilości informacji. Z rosnących zbiorów nieuporządkowanych, pozornie rozłączonych danych, można wyodrębnić informacje, które mogą nie tylko zidentyfikować daną osobę, ale także określić jej cechy demograficzne, społeczno-geograficzne, behawioralne lub psychiczne, poznać preferencje zakupowe, śledzić ich rozkład dnia i nawyki. W tym sensie stają się one atrakcyjne dla każdego rodzaju firmy działającej online, w tym dla reklamodawców. Po drugiej stronie znajdują się konsumenci, dla których prywatne informacje są zasobem, potencjalnie wymienialnym na różne materialne i niematerialne korzyści. Niezależnie od faktu, że niektóre prywatne informacje są postrzegane jako bardziej wrażliwe lub bardziej wartościowe niż inne, klienci, o czym świadczą liczne badania, bardziej cenią pieniądze niż prywatność danych. Wartość informacji zależy od tego, kto jest jej właścicielem, kto o nią pyta i ile chce za nią zapłacić. Celem artykułu jest przedstawienie koncepcji wartości prywatnych informacji z perspektywy klientów i firm.