Problemy Zarządzania – Management Issues, vol. 17, no. 5(85): 111–131
ISSN 1644-9584, © Wydział Zarządzania UW
https://doi.org/10.7172/1644-9584.85.7

Privacy Awareness Monitoring

Submitted: 03.09.19 | Accepted: 05.11.19

Małgorzata Pańkowska*

In this paper, monitoring is perceived as a way to observe how people change their attitude towards privacy, particularly in the Internet circumstances. The paper aims to analyze privacy awareness and the privacy paradox.

A systematic literature review provides the background on the privacy issues in the Internet environment. Beyond that, the paper covers a survey on the perception of new media by students from Poland, Bulgaria, and Colombia.

The systematic literature review and the student privacy awareness survey revealed the relative value of privacy and its dependence on security. The discussion included in this paper concerns the privacy paradox, which can possibly be resolved by separation, exclusion, integration, and connection.

The literature survey has allowed to present privacy in different aspects, i.e. protection modeling, tools and techniques. Researchers focus on protection systems, but they do not reveal reactions of users of the proposed solutions. On the other hand, proponents of the Internet communication encourage people to reveal personal data, without sufficient warning about the consequences of data exposure.

The privacy paradox considerations are expected to be valuable for practitioners of the organizational design because they are to be asked to cope with the privacy ambidexterity and to develop the corresponding business processes.

The important issue, i.e. the privacy paradox, is placed in contradictory concepts (i.e. freedom of exposure and protection from disclosure). The paradox is valuable as a prerequisite for further considerations on privacy in information management. In this paper, the privacy paradox is used as a strategy for theorizing on privacy.

Keywords: privacy monitoring, privacy awareness, privacy aware monitoring, privacy paradox, social media.

Monitorowanie znaczenia prywatności

Nadesłany: 03.09.19 | Zaakceptowany do druku: 05.11.19

W artykule monitorowanie jest postrzegane jako sposób obserwacji zmiany stosunku ludzi do prywatności, szczególnie w środowisku Internetu. Celem artykułu jest badanie znaczenia prywatności i analiza paradoksu prywatności.

Systematyczny przegląd literatury zapewnia podstawową wiedzę na temat interpretacji prywatności w środowisku Internetu. Artykuł zawiera ponadto wyniki badania ankietowego na temat postrzegania nowych mediów przez studentów z Polski, Bułgarii i Kolumbii.

* **Małgorzata Pańkowska** – dr hab., prof. UE, University of Economics in Katowice, Poland. https://orcid.org/0000-0001-8660-606X.

Correspondence address: University of Economics in Katowice, 40-287 Katowice, Poland; e-mail: pank@ue.katowice.pl.

Systematyczny przegląd literatury i badanie ankietowe znaczenia prywatności dla studentów ujawniły, że zagadnienia prywatności i bezpieczeństwa analizowane są jako współwystępujące. W artykule przedstawiono cztery sposoby traktowania tego współwystępowania: rozdzielenie, wykluczenie, integrację i dynamiczną równowagę.

Przegląd literatury pozwolił na ujawnienie, że badania dotyczące prywatności de facto sprowadzają się do modelowania technik i narzędzi ochrony. Jednakże zwolennicy komunikacji internetowej zachęcają użytkowników do ujawniania danych osobowych w celu umożliwienia im korzystania z oprogramowania i informacji z Internetu.

Najważniejszą kwestią jest przedstawienie paradoksu prywatności. Z jednej strony użytkownicy oczekują ochrony, z drugiej zaś – możliwości nieograniczonej swobody ekspozycji swoich danych osobowych.

Słowa kluczowe: monitorowanie prywatności, znaczenie prywatności, monitorowanie znaczenia prywatności, paradoks prywatności, media społecznościowe.

JEL: D18, D82, Q58, L86

1. Introduction

In general, people differ in their evaluation of privacy and this statement is assumed to be the main hypothesis in this paper. People may perceive privacy as an important organizational effort to ensure the protection of personal data. They appreciate the effectiveness of organizational policy designs in terms of restrictiveness and misuse prevention, but the limitations cannot result in anxiety, low autonomy, and low self-esteem. Therefore, it would be necessary to undertake activities to increase the abilities of responsible decision making for individual control of privacy.

The paper is organized as follows. Firstly, the author provides some background information regarding the existing literature and the concepts of interest. Next, the literature review results are discussed. Privacy monitoring is the fundamental literature searching keyword. This is followed by an analysis of the privacy awareness survey. This empirical research has comprised about 300 students from different countries, i.e., Bulgaria, Colombia and Poland. The author concludes the paper by discussion on privacy paradox resolution options, i.e., separation, exclusion, integration, and connection. Suggestions on future research are also added.

2. Awareness of Privacy

Information privacy is an important management issue that continues to challenge organizations. Social network portals can exist because of people who are willing to freely share personal information. There is a cultural approval of narcissistic personalities. The ubiquitous processing of digital data together with social networks development encourages individuals and government organizations to focus on privacy protection. Lately, this issue has been strongly publicized because of the implementation of the General

https://doi.org/10.7172/1644-9584.85.7

Data Protection Regulation (GDPR) (Regulation EU, 2016). The GDPR aim is to cope with the fragmentation of current regulation through the development of a uniform framework which is to provide greater control over the customers' personal data usage, as well as it is assumed to enforce penalties for non-compliance. The regulation includes the requirements of valid consent, so individuals can withdraw or refuse data processing without detriment. The consent must be specific for all usage of data. The GDPR emphasizes the accountability principle, by which organizations must be able to demonstrate and prove compliance with legal regulations. Beyond the GDPR, the Article 29 Data Protection Working Party (2015) includes principles that should be respected by data processors and controllers. Among others, the principles concern legitimate data processing purpose specification, providing clear, accessible and accurate details about the privacy management program, protection of personal data, and implementation of business processes covering monitoring and measurement to provide reports on data usage to data subjects as well as to appropriate supervisory authorities.

According to Sherif et al. (2015), privacy culture evolves as a logical response to privacy threats and is expounded by the management of social organizations to which people belong. The privacy culture is manifested in privacy protection practices and policies. It determines the level of compliance with legal regulations and the understanding of the practices and policies, as well as the acknowledgement and awareness of privacy threats to the organization. Although privacy is assumed to be determined by the social environment context, Privacy Enhancing Technologies (PETs) are expected to include mechanisms that are able to meet the legal authorities' privacy requirements.

By law, privacy is a fundamental right guaranteed by the Universal Declaration of Human Rights, which was adopted and proclaimed by the United Nations General Assembly and which emphasizes that no one can be subjected to arbitrary interference with their privacy (ONU, 1948). Kizza (2013) distinguishes three rights that an individual can use, i.e., solitude, anonymity and intimacy. Holvast (2009) mentioned that in 1891 the American lawyers Samuel Warren and Louis Brandeis described the right to privacy as a right to be let alone. In 1967, Alan Wertin argued that privacy was defined in terms of self-determination, as well 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 (Holvast, 2009). So, privacy must be voluntary. Two dimensions of privacy can be distinguished, i.e., relational and informational (Holvast, 2009). The relational dimension concerns the links one has to other people. The informational dimension is related to the collection, storing and processing of personal data because of a need to maintain control over personal space, body, and information about oneself. Ben Ayed (2014) supports the thesis that privacy is a right and a fundamental social value that protects digital identities. Merriam-Webster dictionary (Windley, 2005) subdivided privacy into three elements which are described as the quality or state of being apart from company, as the isolation, seclusion or freedom from unauthorized oversight or observation, and as a place of seclusion or retreat. Clarke (2006) perceived privacy in five different perspectives, i.e., philosophically, psychologically, sociologically, economically, and politically. Therefore, it encompasses the aspects of an individual's social needs and further can be considered as the privacy of the person, personal behavior, communication, and data. In Holvast's view, the first function of privacy is to ensure personal autonomy, which is important to the development of individuality, supports normal psychological functioning, and stable interpersonal relationships (Holvast, 2009). Personal individuality determines the emotional release, self-evaluation and decision making abilities. On the one hand, solitude and self-reflection are essential for creativity, but on the other hand, individuals look for the opportunity to share their thoughts and consider alternatives in communication with others. Their communication processes are expected to be protected because of the threat of opportunism and risks of compromising. Recent research about Transparency Enhancing Tools (TETs) presents the investigations of technical options for providing information about the consequences of personal data disclosure (Vitale et al., 2017).

Holvast (2009) as well as Yoo et. al. (2012) have written about the privacy paradox as the phenomenon whereby people present strong privacy concerns, but they are willing to reveal their personal information. Generally in management science, paradox is identified with words like contradiction, irony, inconsistency, and oxymoron. Management science specialists use the paradoxical framework to successfully uncover organizational phenomena, i.e., dichotomies of stability and change, dilemma of control and empowerment, centralization and decentralization, empowerment and alienation, flexibility and control, diversity and inclusion, exploration and exploitation, competition and collaboration, learning and doing (Quinn & Nujella, 2017). These examples show the distinction between concepts and their potential opposition. However, they can co-exist, e.g., controlled empowerment, flexible control, coopetition, or learning by doing. Paradox is accepted as a popular theme in management science and organization studies. It can be applied to deal with the pluralities, conflicts, and inconsistencies in management theory and practice (Chia & Nayak, 2017). Becker et al. (2019) named the privacy paradox as a discrepancy between individuals' intention to disclose data and their actual disclosure behavior. According to them, individuals maintain that they are concerned about their privacy and consider the risks of data disclosure, but they do not engage in protective behavior during data disclosure. However, the authors do not take into account that individuals are forced to reveal their demographic and lifestyle information to marketers who persuade them that it is in the best interest of the customer to receive the best product. Similarly, healthcare patients are required to enable access to personal health records because otherwise they will never receive the required medical service.

The theoretical background of the privacy paradox is the privacy calculus theory, according to which individuals make a calculus of the expected benefits of information disclosure and potential loss of privacy. When the benefits are perceived to be equal or greater than the risks, individuals tend to ignore privacy. An internet customer might have the desire to protect their privacy, but the feasibility of such an intention is tested during the online purchasing process. The dual process theory also explains the contradiction in decisions made under conditions of uncertainty. In the field of psychology and also in management science, the theory of cognitive dissonance has been developed to justify the psychological stress experienced by a person in a situation in which the person's beliefs and decisions are confronted with contradictive facts, and people try to resolve the contradiction and to reduce their discomfort. For example, people answer spam emails, thinking that just now it is really a good offer.

In literature, privacy is perceived from the point of view of reputation loss and facing the threat of identity theft (Greenaway & Chan, 2013). Simultaneously, perceiving privacy as a way of self-promotion is in opposition. Although there is a risk that privacy actions are potentially negative and costly to organizations, privacy revealing actions may bring positive effects and they are a good investment for individuals and business organizations. The perceived privacy risk is to be understood as uncertainty resulting from the potential of negative outcomes and the possibility of the other party's opportunistic behavior that can result in loss of reputation and money. Sources of opportunistic behavior include sharing information with third parties, misuse of personal information such as disclosure or unauthorized access or theft. Therefore, elements of control are embedded in most conceptual arguments and definitions around privacy, and they are used to operationalize privacy in protection instruments. However, personal characteristics, such as self-esteem, determine the behavior in cyberspace, so an individual who exhibits high risk aversion will perceive personal data penetration as intrusion, while another person who is more open and likes to share their personal information will not treat the same penetration as intrusion. Privacy awareness is expected to reflect the extent to which a person is informed about the consequences of revealing privacy and about the opportunities to protect personal data. Information privacy refers to the right to keep control over the use of personal information (Cavoukian & Chibba, 2018). While information security concerns protecting data assets through assertion of confidentiality, integrity and authorized availability, privacy is about information linkability and individual sovereignty in cyberspace. Although according to Solove's pragmatic approach, privacy is evaluated instrumentally, as a means of achieving certain goals, privacy should also be evaluated contextually, as benefits of practices of information collection and dissemination (Solove, 2002). According to the Cyberlibertarian school of thought, individuals in cyberspace can act in line with their personal preferences.

3. Review of the Literature on Privacy Monitoring

Usually, a literature review is placed at the beginning of a conference or journal paper, just to present the background knowledge on the discussed issues. Its main purpose is to describe earlier research work. Similarly in this case, the author would like to present a context for the empirical research problem definition. The literature review has allowed to present the research results on privacy monitoring and particularly to receive answers to the following research questions (RQ):

RQ1 What are the privacy monitoring research goals and research project results?

RQ2 Does the privacy monitoring research reveal changes in individuals' privacy awareness and in their attitudes towards responsible control of privacy?

The fundamental reviews have been done using the following publication repositories: Association of Information Systems electronic library (AIS eLib), IEEEXplore, Sage Journals, Science Direct, Scopus, and Web of Science (WoS). The literature survey covers papers published in years 2009–2019. Taking into account the RQ1-RQ2, the search was conducted via the search string "privacy" AND "monitoring". The selection of search items required significant analysis. After deduplication, the results were supplemented by literature analysis focusing on the privacy paradox. However, too many different interpretations of the word "paradox" were noticed, not directly connected with privacy.

	AIS eLib	IEEEXplore	SageJournals	ScienceDirect	Scopus	WoS
2009	138	130	582	1351	170	116
2010	136	174	608	1434	245	114
2011	162	192	633	1611	267	154
2012	178	213	735	1896	308	171
2013	182	224	793	2436	371	236
2014	215	269	699	2710	446	298
2015	224	337	855	3115	485	420
2016	235	408	907	3331	539	465
2017	323	398	1051	3813	568	510
2018	344	424	1245	4113	653	418
2019	146	73	458	2029	132	66

Tab. 1. Privacy monitoring publications in 2009–2019. Source: Own study.

Table 1 includes numbers of search results, i.e., publications on privacy monitoring, before deduplication. In Figure 1, the graph is based on standardized numbers of publications. The standardization was done in the following way (1), assuming that i = 1 … 6, *i* – repository number, t =1 .. 11, *t* – year.

$$x_{it}^{s} = x_{it} \ / \ AVG \ (x_i) \tag{1}$$

The volume of publications in repositories is systematically growing up (Figure 1). For data in all the considered repositories, the average growth rate is 1.053003, standard deviation is 0.019783. The growth rate was calculated in the following way (2).

$$x_{it}^{g} = x_{it}/x_{it-1} \tag{2}$$

The search was done in the middle of 2019. The standardization for the presentation in Figure 1 was done because of exceptionally high values of search results in the ScienceDirect repository. Next, the knowledge reviewing results were structured and key findings and implications for further empirical research were presented in Tables 2 and 3. In bureaucratic cultures, individual behavior and group performance are monitored because monitoring provides a comprehensive view to ensure a fair evaluation and permits control to be kept. The belief that technology can prevent misuse and create an ethical environment strongly sways the decision in favor of adoption. Therefore, research and implementation of solutions to protect private information are justified. Software tools are implemented to prevent disclosures of individual identity, links or their attributes.

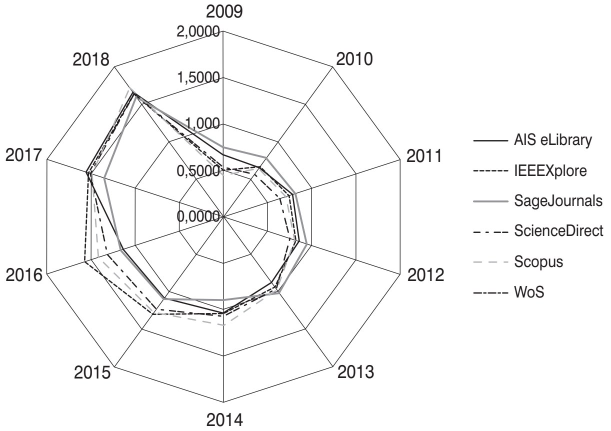

Fig. 1. Privacy monitoring publications in 2009–2018 (standardized values). Source: Own study.

Reference	Research findings
(Xie et al., 2010)	Proposal of privacy-aware monitoring system (PAMS) working as an aggregate query processor that protects the location privacy of car drivers
(Gogoulos et al., 2009)	Description of privacy-aware passive network monitoring system, focusing on the specification and performance evaluation of its access control and authorization aspects
(Amro et al., 2013)	Proposal of privacy aware collaborative traffic monitoring system (PA-CTM) that considers the privacy and security properties of VANETs (vehicular ad hoc networks) and existing infrastructures
(Preuveneers & Joosen, 2016)	Presentation and evaluation of a practical smartwatch-based lifelong application for diabetics that leverages the cloud and homomorphic encryption for caregivers to analyze blood glucose, insulin values, and other parameters in a privacy protection manner
(Lee & El-Khatib, 2009)	Proposal of a privacy-enabled architecture for an RFID-based hospital location tracing system that prevents network eavesdroppers from tracing a patient's location
(Kotler et al., 2010)	Introduction to a user-centric privacy architecture that enables the provider-independent protection of personal data. A central component of the infrastructure is an online privacy community to facilitate the open exchange of privacy-related information
(Meziane et al., 2010)	Presentation of a privacy agreement monitoring system for controlling private data usage flowing dynamically in the area of web services
(Kumar Nepali & Wang, 2013)	Proposal of a social network model, SONET, for privacy monitoring and ranking. The proposed privacy risk indicator, PIDX, is calculated in real time and the value is used for privacy monitoring and risk control
(Lin et al., 2013)	Design of a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the parties involved in mHealth and their data
(Tome de Souza & Zorzo, 2015)	Presentation of a privacy-preserving mechanism which guarantees the privacy of the data owner and the person who accesses the data. A cloud monitoring mechanism has been proposed to monitor data, including intrusion-detection scenarios available for the data owner
(Shabalala et al., 2014)	Presentation of a privacy monitoring framework to help cloud customers comprehend with what happens to their data stored in the cloud

Tab. 2. Privacy monitoring solutions. Source: Own study.

Table 2 includes the review of exemplar solutions proposed to prevent compromising privacy. These solutions are named privacy-aware monitoring solutions or privacy-preserving monitoring tools. Taking into account the literature review, an evolution of considerations on privacy monitoring development has been noticed. On the one hand, information technology (IT) solutions, models, and architecture frameworks are proposed as a proof of concept or in beta versions but, on the other hand, researchers present and discuss how important privacy protection and privacy monitoring are (Table 3). It should be emphasized that in some papers privacy is perceived as an individual choice, right, and personal value. This attitude seems to foster this paper thesis. The empirical research on privacy awareness and its monitoring is usually useful to support business information system development. For example, in a user-centered design approach, developers focus on applications with a high degree of usability; however, non-functional requirements are respected and included in the interactive system development process.

Reference	Research findings
(Ramli et al., 2012)	Application of Carew and Stapleton's Privacy Framework to Psychiatric Monitoring Systems to identify the issues related with monitoring patients' behavior. This approach is to help system developers in designing a privacy-sensitive system
(Eivazi, 2011)	Examination of employers' justification for conducting electronic monitoring because of employees' misbehavior and misuse of online services at work
(Kamada et al., 2016)	Investigation of user preferences in terms of monitoring and privacy protection. Conducted experiments show the possibility to control the levels of monitoring
(Mathiesen, 2013)	Argumentation that children have the right to privacy from their parents, because that right respects their capacities and supports their future capacities for autonomy and social relationships
(Lee Jr et al., 2013)	Investigation of the impact of monitoring mechanisms on privacy concerns and job performance when evaluating whether to participate in a BYOD (bring your own device) program
(Smith & Tabak, 2009)	Reviewing the current knowledge about e-mail monitoring regarding employee attitudes and behaviors such as organizational commitment, job satisfaction, and performance
(Wilkowska & Ziefle, 2012)	Revealing that females and healthy adults require and insist on the highest security and privacy standards compared with males
(Townsend et al., 2011)	Supporting the hypothesis that older adults are willing to trade privacy for autonomy
(Prince, 2018)	Assessment of factors that impact web users' predisposition to exert control over personal data flows. In conclusion, those people who are more likely to disclose personal data express a greater propensity to use privacy controls
(Kurkovsky & Syta, 2011)	Research work on the use of electronic communications by students at public universities. Revealing that regardless of students awareness of university policies, individuals have inherent expectations that their on-campus electronic communication will stay private

Tab. 3. Data subjects privacy awareness literature review. Source: Own study.

In general, the reviewed literature presents that researchers are interested in dealing with the privacy paradox, i.e. situations when individuals express high concerns but do not engage in privacy-protective behaviors. The conclusions presented in Table 2 and Table 3 are oriented towards privacy protection increase as well as security assertion support.

4. Empirical Research on Privacy Awareness

Crossler and Belanger (2017) have argued that past privacy invasion experience and perception of privacy norms are likely to influence the human motivation to learn about privacy protection practices. Taking it into account and assuming that information privacy refers to what extent, when and how personal information is disseminated depends on individual preferences, the questionnaire survey was conducted to support RQ2 by revealing students' attitudes towards privacy and responsible behavior for successful dissemination and protection of private identity, simultaneously. Although Internet users respect different regulations, driven by legal acts, regulatory compliance, as well as by policies, code-of-business conduct, business risk assessments, audit findings or personal privacy imperatives, people are able to take risks to reveal their privacy, just to present themselves online for personal satisfaction or in expectation of a successful partnership and social relations development. According to Xu et al. (2008), privacy should be considered as a multidimensional and dynamic concept. Therefore, in this paper, privacy awareness is defined by 24 questions, mostly connected with web services usage. The questions are slightly similar to those presented by Williams and Nurse (2016), the question set is extended and concerns cleaning the Internet browser's history, usage of Internet browser plug-ins and extensions, encryption of data, storage in Dropbox, sharing private photos on Facebook, usage of Tor and PrivBrowse software in web browsing, reading the terms and conditions on websites, providing personal data for web portal registration, checking the permissions before installing smartphone apps, removal of cookies, installation of unknown source software on private computer, opening unknown emails and attachments, checking if e-commerce websites have a green padlock, usage of antivirus software, leaving personal devices unmonitored on a train or in a waiting room, usage of mobile phones in open space, and usage of open WiFi networks.

For each of the questions, there are five optional answers, i.e., several times a day, once a day, sometimes, by chance, occasionally, and never. Students from Bulgaria, Colombia and Poland took part in the survey in summer in 2018. Beyond that, in Poland the survey was done also in 2019. Table 4 and Figure 2 cover the questionnaire research results for students from Bulgaria. Maximal values of each variable have been bolded. The values are standardized. The standardization method was presented in (1).

	Research questions: How often do you:	several times a day	once a day	sometimes	by chance	never
1	clean your Internet browser's history ?	0.038	0.038	**0.472**	0.245	0.208
2	use Internet browser plug-ins/extensions to protect your privacy?	0.208	0.000	**0.358**	0.151	0.283
3	encrypt data on your computer?	0.019	0.038	0.377	0.113	**0.453**
4	store unencrypted data (e.g., photos) within a cloud provider sych as Dropbox?	0.057	0.170	**0.453**	0.094	0.226
5	share your photos on Facebook?	0.019	0.038	**0.660**	0.113	0.170
6	share photos interesting for you on Facebook?	0.075	0.038	**0.434**	0.208	0.245
7	share photos important for you on Facebook?	0.075	0.038	**0.434**	0.208	0.245
8	share photos of historic/tourist attractions on Facebook?	0.057	0.057	**0.491**	0.132	0.264
9	share photos of mass events on Facebook?	0.057	0.038	0.358	0.151	**0.396**
10	use Tor for your web browsing?	0.000	0.019	0.094	0.094	**0.792**
11	use PrivBrowse software for your web browsing?	0.000	0.038	0.075	0.038	**0.849**
12	use encryption tools for your emails?	0.075	0.038	0.170	0.094	**0.623**
13	read the terms and conditions on websites you use?	0.038	0.057	**0.358**	0.226	0.321
14	share your personal data to register on web portals?	0.000	0.019	**0.434**	0.226	0.321
15	check permissions before installing smartphone apps?	0.113	0.151	**0.377**	0.151	0.208
16	remove cookies?	0.057	0.094	**0.396**	0.208	0.245
17	install software from unknown sources?	0.038	0.019	**0.396**	0.226	0.321
18	open unknown email addresses?	0.000	0.019	0.113	0.170	**0.698**
19	open word attachments sent from unknown email addresses?	0.000	0.000	0.094	0.132	**0.774**
20	check if the website has a green padlock?	0.170	0.113	**0.321**	0.094	0.302
21	use antivirus software?	**0.509**	0.094	0.245	0.057	0.094
22	leave your devices unmonitored on a train, in a waiting room?	0.019	0.000	0.226	0.057	**0.698**
23	use the mobile phone in open space?	**0.491**	0.057	0.245	0.094	0.113
24	use the open source network in WiFi?	0.226	0.094	**0.434**	0.151	0.094

Tab. 4. Profiling the Bulgarian students' answers concerning web services. Source: Own study.

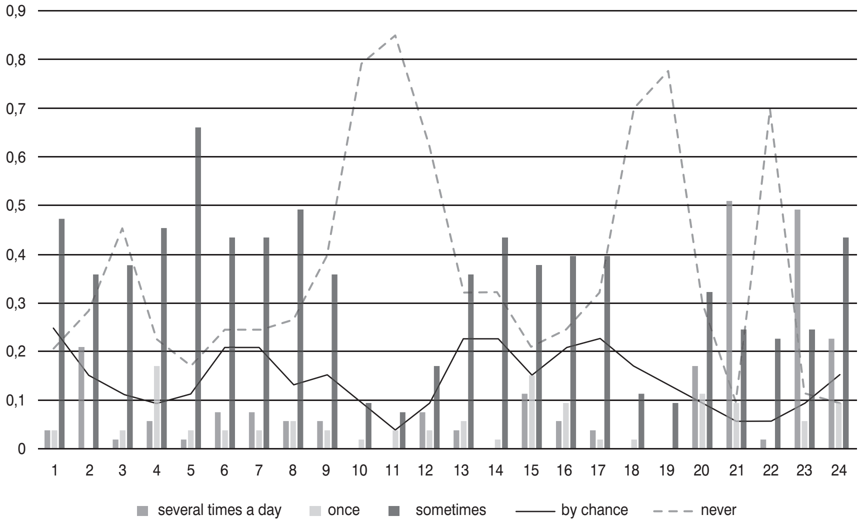

Fig. 2. Bulgarian students' answers concerning web services. Source: Own study.

In general, the student survey results instill optimism. Although student personal data is not so sensitive as bank or hospital personal data, students know how to avoid unnecessary disclosure of data in unsecured open cloud, e.g., in Dropbox. They behave carefully and responsibly. Although they use Internet services, in general, they do not admit or reveal their strong dependency on the Internet. Facebook is useful, but they do not need to post several times a day. Beyond that, they are also not excessively cautious, so they do not accept the necessity to encrypt data on their computers or use encryption tools for emails. In general, for students, Tor and PrivBrowse software programs are unknown and unused. In the survey, students admit that they share their personal data to register on a web portal. The only comment is that they are forced to provide their personal data, because otherwise the web services will not be available for them. Nowadays, business portals do not permit the use of an "opt-out" solution, which covers permission to access without prior registration. Anastasopoulou et al. (2017) distinguished three different types of privacy transactions. There are transactions for non-privacy goods, when the secondary use of personal information is optional. The second type of transactions is in the case of dissemination of free products (e.g., freebies, demo or prototype versions, online social networks offers, free cloud services). The third privacy-related transactions are supported by PET tools to protect customer data or hide their browsing behavior. Malheiros et al. (2013) in their research assigned responders to three groups, i.e., privacy fundamentalists, unconcerned and pragmatists. Students who participated in this survey seem to belong to that third group. The perception of privacy is highly individual in the case of each Internet user; however, through the individual behavior monitoring process the user's self-control is to be respected and supported. It is a very positive conclusion that 70% of students admitted that they did not open unknown emails or unknown attachments (77%) (Table 4). Similar results were obtained for students in Colombia in 2018 and Poland in 2018 and in 2019. Just to present the similarity of matrices of students' preferences, the structure taxonomy metrics has been calculated as in (3), assuming that x, y – distance objects, i.e., countries, i = 1 … 24, i – variable number, j = 1 … 5, j – variable level. This structure taxonomy metrics applies the Euclidean distance.

$$d(x,y) = \{\sum_{ij} (x_{ij} - y_{ij})^2 \}^{½} \tag{3}$$

The Euclidean distances between matrices of students' preferences in these 3 countries are presented in Table 5. The students' answers concerning web services usage in 2018 and in 2019 in Poland are similar (d = 0.8308). Colombian students' preferences are more similar to the answers of Bulgarian students than to those of Polish students. These results support the thesis about carefulness, restraint and moderation of web services usage by students in these 3 countries.

	Poland 2018	Poland 2019	Bulgaria	Colombia
Poland 2018	x	0.8308	1.033218	1.975765
Poland 2019	0.8308	x	n/a	n/a
Bulgaria	1.033218	n/a	x	1.879586
Colombia	1.975765	n/a	1.879586	x

Tab. 5. Metrics of Euclidean distance between 3 countries. Source: Own study.

However, there is still an open question of how to cope with the privacy paradox and what solutions are included in literature surveys. In this paper, the privacy paradox is placed in contradictory concepts (i.e., freedom of exposure, protection from disclosure of personal data), which exist simultaneously and persist over time.

In this paper approach, the paradox is not identified with dilemma, which is a choice of one of two or more options. The paradox should be accepted as a prerequisite to further consideration on privacy. Individual and organizational performance gets better when the privacy paradox is recognized and managed. The literature on privacy depicts the dynamic nature of this paradox by conceptualizing it in terms of four continua which can be expressed in a 2x2 grid (Table 6). According to Clegg and Pina e Cunha (2017), management science responds to the privacy paradox in four ways:

Incoherent	SEPARATION		EXCLUSION	
	(Railean & Reinhardt, 2018)	The online survey indicates that participants tend to see the Internet of Things, IoT, as computer-like devices rather than appliances. Privacy is a primary concern in the IoT adoption process, but the authors provide recommendations to IoT vendors.	(Zhong et al., 2019)	The authors consider the large-scale deployment of next-generation wireless networks, they analyze networks for cyber-physical systems and investigate the system fundamentals of security and privacy for next generation wireless networks.
	(Hatamian et al., 2019)	The authors considered the GooglePlay Store as a source to extract and quantify privacy relevant claims. They detect privacy relevant reviews and categorize them. This approach provides developers with specific knowledge about privacy threats and application functionalities.	(Alabdulatif et al., 2019)	The authors present a scalable, cloud-based model to provide a privacy preserving anomaly detection service for quality assured decision-making in smart cities. They applied homomorphic encryption to preserve data privacy during the analysis and MapReduce-based distribution of tasks, as well as parallelization to overcome computational overheads.
	(Gong et al., 2016)	The authors investigated the health monitoring privacy risks and proposed a privacy-preserving approach for genome-aware health monitoring. Therefore, users can only learn the diagnostic results based on sensitive data, while the service provider learns nothing.	(Chui et al., 2019)	The authors proposed a Big Data and IoT-based patient behavior monitoring system, although they summarized the general challenges like trust, privacy, security and interoperability in various sectors, e.g., government, research institutions, legislators.
Coherent	INTEGRATION		CONNECTION	
	(O'Connor et al., 2017)	Practical approaches in designing IoT for data collection and data sharing within the health domain.	(Morshedi et al., 2019)	The authors provide a trust model considering institutions as mediators to assess trustability of remote monitoring and management systems.
	(Bachiri et al., 2018)	The authors evaluate the privacy policies of mobile personal health record (mPHR) for pregnancy monitoring using a template covering the characteristics of privacy, security, and regulations. Consequently, they argue that apps developers are requested to pay more attention to the structure and the content of privacy policies in their applications.	(Xie et al., 2010)	The authors recognized that the traffic-monitoring system may compromise the privacy of drivers. They proposed a privacy-aware monitoring system that protects the location privacy of drivers as it anonymizes the IDs of cars.
	(Vitale et al., 2017)	The authors propose the PbD approach to maximize the user experience of the system while reducing privacy concerns of users. The authors suggest a novel experiment in a human-robot interaction setting.	(Ramli & Zakaria, 2014)	The authors noted that psychiatric patients' privacy issues get less attention in information system development. They applied Care and Stapleton's ISD framework to psychiatric monitoring systems. The researchers provided guidance to system developers.
	Interdependent		Independent	

Tab. 6. Privacy paradox resolution options. Source: Own study.

- Exclusion: one extreme is taken as realistic and the other is considered as irrelevant and selected out. For instance, privacy as freedom is privileged over security as a path of analysis. The concepts of freedom and protection are understood as independent and incoherent. They are split and unsuitable.
- Separation: contradiction is admitted, but one pole is selected over the other at a specific moment and subsequently reversed. Attention to one pole (i.e., privacy freedom) is succeeded by attention to the alternative pole (i.e., privacy protection). In general, separation manifests itself in several forms including separation in time, in space, in division of duties and roles (e.g., marketer, security officer), and in policies and regulations. Role separation occurs when members of an organization split their activities in such a way that some professionals focus on one pole, while others consider the other at the same time and place. The concepts of freedom and protection are considered as interdependent, but they are weakly balanced and incoherent.
- Integration: the opposites are viewed as interdependent. It is recognized and accepted that one concept requires the other to maintain the organization as vital (e.g., no privacy without security). At first glance, the privacy by design (PbD) approach can be recognized as a way that promotes privacy and data protection compliance from the start of data collection and the PbD method maintains such protection in the whole information system lifecycle. Beyond that, PbD is expected to increase awareness of privacy and decrease human vulnerabilities. In 2011, Cavoukian published her PbD principles, which for years have been considered as de facto standard in privacy protection and, promoted by her PbD approach, can be considered as integrating the two contradictory aspects of privacy, i.e., freedom and protection (Cavoukian, 2011). In this approach, the concepts of freedom and protection are coherent and interdependent. They are developed in stable and balanced cooperation oriented towards looking for new opportunities, innovativeness, and sustainability.
- Connection: in this approach, the organization is expected to maintain a balance between extreme poles. There is a dynamic change of orientation from one concept to another and vice versa. Proponents of this approach stress the transition from differentiating and integrating towards a dynamic equilibrium. The concepts of freedom and protection passively co-exist, they are not considered as mutually needed. They are understood as independent, but coherent.

Therefore, Table 6 includes four proposed forms of proceeding in the situation of privacy paradox. The criteria of coherence and dependency are assumed to enable the differentiation of the discussed forms. In the cells of the grid in Table 6, exemplar publications are included and they present the discussed approaches. A systematic literature review permits the exemplar list to be constantly extended. None of the proposed ways to cope with the privacy paradox dominates. They all seem to be needed for their own particular purposes. The papers in the Separation cell emphasize the division of aspects. Although papers should be on privacy, they are focused on security aspects. This approach is even more visible in papers in the Exclusion cell. The authors of the papers write on technology solutions for security. The papers on development and application of the PbD approach are included in the Integration cell. This way is nowadays strongly preferred by information system developers and combined with other methodologies focused on agile application development as well as design thinking. Other approaches are included in the Connection cell. They are not strongly oriented towards integrating different concepts, resolutions and techniques.

5. Conclusions

Powerful technologies and software can increase the efficiency of operations and services. However, there are also abuse of privacy, governmental monitoring of people's private lives, and illegal registration of political behavior. Privacy discourse involves different normative decisions on legitimate usage of private information in Internet communication processes. People have entered a new world, yet not everyone knows that or understands the implications. Fortunately, people are careful and a lack of understanding leads to unwillingness to easily accept new technology solutions.

Literature reviews revealed that privacy is combined with security and the discussion on privacy awareness involves thinking about and developing technical solutions, models and frameworks for privacy protection. Security is developed to protect information, but privacy concerns establishing a framework for deciding on personal information usage. Privacy awareness determines how security options should be implemented and what control is to be applied, but it should not reduce human freedom. Further research should focus on monitoring the changes in human attitudes towards privacy because of increased impact of mobile communications, drones and cyber-technologies.

References

Alabdulatif, A., Khalil, I., Kumarage, H., Zomaya, A.Y., & Yi, X. (2019). Privacy-preserving anomaly detection in the cloud for quality assured decision-making in smart cities. *Journal of Parallel and Distributed Computing*, *127*, 209–223. https://doi.org/10.1016/j.jcss.2017.03.001.

Amro, B., Saygin, Y., & Levi, A. (2013). Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update. *IET Intelligent Transport Systems*, *7*(4), 388–395. https://doi.org/10.1049/iet-its.2011.0212.

Anastasopoulou, K., Kokolakis, S., & Andriotis, P. (2017). Privacy decision-making in the digital era: A game theoretic review. In T. Tryfonas (Ed.), *Human aspects of information security, privacy and trust* (pp. 589–603). Cham: Springer.

Article 29 Data Protection Working Party. (2015). *01673/15/EN WP 231, Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones*. Retrieved on 30 March 2018 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

Bachiri, M., Idri, A., Fernandez-Aleman, J.L., & Toval, A. (2018). Evaluating the privacy policies of mobile personal health records for pregnancy monitoring. *Journal of Medical Systems*, *42*(8), 1–14. https://doi.org/10.1007/s10916-018-1002-x.

Becker, M., Klausing, S.M., & Hess, T. (2019). Uncovering the privacy paradox: The influence of distraction on data disclosure decisions. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, June 8–14, *Research-in-Progress Papers*. Retrieved on 30 March 2018 from https://aisel.aisnet.org/ecis2019_rip/69.

Ben Ayed, G. (2014). *Architecting user-centric privacy-as-a-set-of-services, digital identity-related privacy framework*. Cham: Springer.

Cavoukian, A. (2011). *Privacy by design. The 7 foundational principles in privacy by design. Strong privacy protection—now, and well into the future*. Retrieved on 20 March 2018 from https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Cavoukian, A., & Chibba, M. (2018). Start with privacy by design in all big data applications. In S. Srinivasan (Ed.), *Guide to big data applications* (pp. 29–48). Heidelberg: Springer.

Chia, R., & Nayak, A. (2017). Circumventing the logic and limits of representation: Otherness in east-west approaches to paradox. In W.K. Smith, M.W. Lewis, P. Jarzabkowski, & A. Langley (Eds.), *The Oxford handbook of organizational paradox* (pp. 125–142). Oxford: Oxford University Press.

Chui, K.T., Liu, R.W. Lytras, M.D., & Zhao, M. (2019). Big data and IoT solution for patient behaviour monitoring. *Behaviour and Information Technology*, 1362–1375. https://doi.org/10.1080/0144929X.2019.1584245.

Clarke, R. (2006). *What's privacy?*. Workshop at the Australian Law Reform Commission. Retrieved on 6 May 2010 from http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html.

Clegg, S., & Pina e Cunha, M. (2017). Organizational dialectics. In: M.L. Besharov, & G. Sharma (Eds.), *Paradoxes of organizational identity* (pp. 105–124). Oxford: Oxford University Press.

Crossler, R. E., & Bélanger, F. (2017). The mobile privacy-security knowledge gap model: Understanding behaviors. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4071–4080). Retrieved on 3 March 2018 from http://hdl.handle.net/10125/41651.

Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law and Security Review*, *27*(5), 516–523.

Gogoulos, F., Antonakopoulou, A., Mousas, A.A., Kaklamani, D.I., & Venieris, I.S. (2009). Privacy-aware passive network monitoring. PCI 2009. In *Proceedings of the 13th Panhellenic Conference on Informatics* (pp. 171–175). Retrieved on 3 May 2019 from https://ieeexplore.ieee.org/document/5578562.

Gong, Y., Zhang, C., Hu, Y., & Fang, Y. (2016). Privacy-preserving genome-aware remote health monitoring. In *2016 IEEE Global Communications Conference, GLOBECOM 2016-Proceedings* (pp. 4702–4708).

Greenaway, K.E., & Chan, Y.E. (2013, September). Designing a customer information privacy program aligned with organizational priorities. *MIS Quarterly Executive*, *12*(3), 137–150.

Hatamian, M., Serna, J., & Rannenberg, K. (2019). Revealing the unrevealed: Mining smartphone users privacy perception on app markets. *Computers and Security*, *83*, 332–353. https://doi.org/10.1016/j.cose.2019.02.010.

Holvast, J. (2009). History of privacy. In V. Matyas, S. Fischer-Hubner, D. Cvrcek, & P. Svenda (Eds.), *IFIP AICT: Vol. 298*. *The future of identity in the information society* (pp. 13-42). Heidelberg: Springer.

Kamada, S., Hara, S., & Abe, M. (2016). Safety vs. privacy: User preferences from the monitored and monitoring sides of a monitoring system. In *UbiComp 2016 Adjunct – Proceedings of the 2016 ACM International Joint Conference of Pervasive and Ubiquitous Computing* (pp 101–104). Retrieved on 30 April 2019 & 3 May 2019 from https://www.scimagojr.com/journalsearch.php?q=21100781851&tip=sid&clean=0.

Kizza, J.M. (2013). *Ethical and social issues in the information age* (5th ed.). New York: Springer.

Kolter, J., Kernchen, T., & Pernul, G. (2010) Collaborative privacy management. *Computers and Security*, *29*(5), 580–591. https://doi.org/10.1016/j.cose.2009.12.007.

Kumar Nepali, R., & Wang, Y. (2013). SONET: A SOcial NETwork model for privacy monitoring and ranking. In *Proceedings of IEEE 33rd International Conference on Distributed Computing Systems Workshops* (pp. 162–166). Retrieved on 22 May 2019 from https://dl.acm.org/citation.cfm?id=2570451&picked=prox.

Kurkovsky, S., & Syta, E.(2011). Monitoring of electronic communications at universities: Policies and perceptions of privacy. In *Proceedings of 44th Hawaii International Conference on System Sciences* (pp. 1–10). Retrieved on 3 May 2019 from https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5716643.

Lee, J., & El-Khatib, K. (2009). A privacy-enabled architecture for an RFID-based location monitoring system. In *MobiWac'09 – Proceedings of the 7th ACM International Symposium on Mobility Management and Wireless Access* (pp. 128–131). Retrieved on 3 May 2019 from https://dl.acm.org/ citation.cfm?id=1641776 &picked=prox.

Lee Jr., J., Crossler, R.E., & Warkentin, M. (2013). Implications of monitoring mechanisms on Bring Your Own Device (BYOD) adoption. In *Proceedings of International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design*. Retrieved on 3 May 2019 from https://aisel.aisnet.org/icis2013/.

Lin, H., Shao, J., & Zang, Ch. (2013). CAM: Cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security*, *8*(6), 985–997. https://doi.org/10.1109/TIFS.2013.2255593. Retrieved on 18 May 2019 from https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6516989&punumber=10206.

Malheiros, M., Brostoff, S., Jennett, Ch., & Sasses, M.A. (2013). Would you sell your mother's data? Personal data disclosure in a simulated credit card application. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 237–264). Berlin: Springer-Verlag.

Mathiesen, K. (2013). The Internet, children, and privacy: The case against parental monitoring. *Ethics and Information Technology*, *15*(4), 263–274. https://doi.org/10.1007/s10676-013-9323-4.

Meziane, H., Benbernou, S., Zerdali, A.K., Hacid, M., & Papazoglou, M. (2010). A view-based monitoring for privacy-aware web services. In *Proceedings of IEEE 26th International Conference on Data Engineering (ICDE 2010)* (pp. 1129–1132). https://doi.org/10.1109/ICDE.2010.5447762. Retrieved on 21 May 2019 from https://ieeexplore.ieee.org/xpl/topAccessedArticles.jsp?punumber=5443872&topArticlesDate=October%202017.

Morshedi, M., Noll, J., & Kari, R. (2019). Building trustable remote monitoring and management systems. In *Proceedings – 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC Companion 2018* (pp. 213–219). https://doi.org/10.1109/UCC-Companion.2018.00059.

O'Connor, Y., Rowan, W., Lynch, L., & C. Heavin, C. (2017). Privacy by design: Informed consent and Internet of Things for smart health. *Procedia Computer Science*, *113*, 653–658. The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH2017). https://doi.org/10.1016/j.procs.2017.08.329. Retrieved on 20 February 2019 from www.elsevier.com/locate/ procedia.

ONU. (1948). *Declaração Universal dos Direitos Humanos*. Retrieved on 30 March 2018 from http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm.

Preuveneers, D., & Joosen, W. (2016). Privacy-enabled remote health monitoring applications for resource constrained wearable devices. *Proceedings of the ACM Symposium on Applied Computing* (pp. 119–124). Retrieved on 28 May 2019 from https://dl.acm.org/citation.cfm?id=2851683.

Prince, Ch. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21–32. https://doi.org/10.1016/j.ijhcs.2017.10.003.

Quinn, R.E., & Nujella, M. (2017). Paradox in organizational theory. In: W.K. Smith, M.W. Lewis, P. Jarzabkowski, & A. Langley (Eds.), *The Oxford handbook of organizational paradox* (pp. v–vii). Oxford: Oxford University Press.

Railean, A., & Reinhardt, D. (2018). Life-long privacy in the IoT? Measuring privacy attitudes throughout the life-cycle of IoT devices. In M. Hansen et al. (Eds.), *IFIP AICT: Vol. 526. Privacy and identity* (pp. 132–149). Springer International Publishing AG. https://doi.org/10.1007/978-3-319-92925-5_9.

Ramli, R., & Zakaria, N. (2014). Privacy issues un a psychiatric context: Applying the ISD privacy framework to a psychiatric behavioural monitoring system. *AI and Society*, *29*(2), 203–213. https://doi.org/10.1007/s00146-013-0476-9.

Ramli, R., Zakaria, N., Mustaffa, N., & Sumari, P. (2012). Privacy issues in a psychiatric context: Applying the ISD privacy framework to a psychiatric behavioural monitoring system. *IFAC Proceedings Volumes*, *45*(10), 114–119.

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 (2016). European Parliament and the Council of the European Union. Retrieved on 30 March 2018 from http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Shabalala, M.V., Tarwireyi, P., & Adigun, M.O. (2014). Privacy monitoring framework for enhancing transparency in cloud computing. In *Proceedings of IEEE 6th International Conference on Adaptive Science & Technology (ICAST)* (pp. 1–7). https://doi.org/10.1109/ICASTECH.2014.7068093. Retrieved on 4 May 2019 from https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7056705.

Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In T. Tryfonas, & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (pp. 436–448). Cham: Springer.

Solove, D.J. (2002). Conceptualizing privacy. *California Law Review*, *90*, 1087–1156. https://doi.org/10.15779/Z382H8Q.

Smith, W.P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy?. *Academy of Management Perspectives*, *23*(4), 33–48. https://doi.org/10.5465/amp.23.4.33.

Tome de Souza, R., & Zorzo, S.D. (2015). Privacy-preserving mechanism for monitoring sensitive data. In *Proceedings of 12th International Conference on Information Technology – New Generation* (pp. 191–196). Retrieved on 3 May 2019 from http://www.proceedings.com/26300.html.

Townsend, D., Knoefel, F., & Goubran, R. (2011). Privacy versus autonomy: A tradeoff model for smart home monitoring technologies. In *Proceedings of Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 4749–4752). Retrieved on 3 May 2019 from https://ieeexplore.ieee.org/xpl/topAccessedArticles.jsp?reload=true&punumber=6067544&topArticlesDate=August%202017.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in e-health: Requirements from the user's perspective. *Health Informatics Journal*, *18*(3), 191–201. https://doi.org/10.1177/1460458212442933.

Williams, M., & Nurse, J.R.C.(2016). Optional data disclosure and the online privacy paradox: A UK perspective. In T. Tryfonas (Ed.), *Human aspects of information security, privacy, and trust* (pp. 186–197). Cham: Springer.

Windley, P.J. (2005). *Digital identity: Unmasking identity management architecture (IMA)*. Sebastopol: O'Reilly Media.

Vitale, J., Tonkin, M., Ojha, S., Williams, M-A, Wang, X., & Judge, W. (2017). Privacy by design in machine learning data collection: A user experience experimentation. In *The AAAI 2017 Spring Symposium on Designing the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 439–442). Retrieved on 1 May 2019 from https://www.aaai.org/ocs/index.php/SSS/SSS17/paper/viewFile/15305/14583.

Xie, H., Kulik, L., & Tanin, E. (2010). Privacy-aware traffic monitoring. *IEEE Transactions on Intelligent Transportation Systems*, *11*(1), 61–70. https://doi.org/10.1109/TITS.2009.2028872.

Xu, H., Dinev, T., Smith, H.J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *ICIS 2008 Proceedings*. Retrieved on 3 May 2019 from http://aisel.aisnet.org/ icis2008/6.

Yoo, Ch.W., Ahn, H.J., & Rao, H.R. (2012). An exploration of the impact of information privacy invasion. In *Proceedings of Thirty Third International Conference on Information Systems, Orlando, AIS/ICIS* (pp. 2260–2278). Retrieved on 30 April 2018 from https://aisel.aisnet.org/icis2012/.

Zhong, S., Zhong, H., Huang, X., Yang, P., Shi, J., & Xie, L. (2019). Networking cyber-physical systems: System fundamentals of security and privacy for next-generation wireless networks. In S. Zhong, H. Zhong, X. Huang, P. Yang, J. Shi, L. Xie, & K. Wang (Eds.), *Security and privacy for next-generation wireless networks* (pp. 1–32). Cham: Springer. https://doi.org/10.1007/978-3-030-01150-5_1.