A conceptualization of the privacy concerns of cloud users

Dijana Peras and Renata Mekovec
Department of Information Systems Development, Faculty of Organisation and Informatics Varaždin, University of Zagreb, Varazdin, Croatia

Received 8 November 2021
Revised 1 February 2022
Accepted 14 March 2022

Abstract

Purpose – The purpose of this paper is to improve the understanding of cloud service users' privacy concerns, which are anticipated to considerably hinder cloud service market growth. The researchers have explored privacy concerns from dimensions that were identified as relevant in the cloud context.

Design/methodology/approach – Content analysis was used to identify privacy problems that were most often raised in previous cloud research. Multidimensional developmental theory (MDT) was used to build a conceptual model of cloud privacy concerns. Literature review was made to identify the privacy-related constructs used to measure privacy concerns in previous cloud research.

Findings – The paper provides systematization of recent cloud privacy research, proposal of a conceptual model of cloud privacy concerns, identification of measuring instruments that were used to measure privacy concerns in previous cloud research and identification of categories of problems that need to be addressed in future cloud research.

Originality/value – This paper has identified the categories of privacy problems and dimensions that have not yet been measured in the cloud context, to the best of the authors' knowledge. Their simultaneous examination could clarify the effects of different dimensions on the privacy concerns of cloud users. The conceptual model of cloud privacy concerns will allow cloud service providers to focus on key cloud problems affecting users' privacy concerns and use the most appropriate privacy protection communication and preservation approaches.

Keywords Cloud privacy concerns, Cloud services, Privacy dimensions, Privacy problems

Paper type Research paper

1. Introduction

Cloud computing is a model for enabling convenient, on-demand access to a shared pool of configurable computer resources that can be rapidly provisioned and released with minimal management effort or service provider interaction (Cloud Computing Basics, 2022). Building upon this definition, literature identifies three service models for cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The most commonly used model of cloud service is SaaS, which is popular because of its simple and straightforward nature (Al-Madhagy, 2018). However, because of the collection and processing of a large amount of data, SaaS is often considered the biggest threat to user privacy. This paper tackles the privacy issues arising from the use of SaaS services (e.g. Google Drive, Dropbox, OneDrive, etc.)

Although all major cloud service providers have implemented certain privacy protection mechanisms, privacy remains one of the most prominent concerns. Moreover, privacy

Information & Computer Security
Vol. 30 No. 5, 2022
pp. 653-671
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-11-2021-0182

problems are frequently discussed as a major barrier to using cloud services (Fox, 2021). According to the Privacy Survey (CISCO, 2019), 84% of cloud users care about privacy and want more control over their data, and 48% already switched providers because of their data policies or data-sharing practices. Privacy concerns in cloud services are closely related to the main attributes of cloud environments: outsourcing (delegating the responsibility for performing data storage and processing to a third party), multi-tenancy (sharing the infrastructure with multiple users) and massive data (storing a large volume of dynamic data). Transparency is much lower, and the data are open to more vulnerabilities. Data are often transferred beyond international borders, requiring consideration of legal requirements in different jurisdictions and complicating the user's ability to manage data flows and preserve privacy (Fox, 2021). Users' privacy concerns and related behaviors are expected to differ from other contexts because of complex data collection and storage methods, new ways of using data, and the possibility of interlinking data. These problems are anticipated to considerably hinder cloud service market growth (*Personal Cloud Market*, 2020). However, little is known about cloud service users' privacy concerns and consequent attitudes, as most privacy research in the cloud domain focuses on technical solutions (Nikkhah *et al.*, 2018). Therefore, it is important to explore which dimensions of privacy concerns are relevant in the cloud context.

The objectives of this paper are to identify the key cloud privacy problems, to group cloud privacy problems into meaningful categories, to propose a conceptual model of cloud privacy concerns and to identify the categories of problems that need to be addressed in future cloud research.

The remainder of this paper proceeds as follows:

The theoretical and methodological frameworks are defined in Sections 2 and 3. The results of the research are then presented within four subsections in Section 4. First, the search results based on search strings are presented. Second, key cloud privacy problems were extracted, and similar problems were grouped into the same category. Third, a conceptual model of cloud privacy concerns is proposed. Fourth, the privacy-related constructs used to measure privacy concerns in previous cloud research were presented, and the categories of problems that need to be addressed in future cloud research were identified. Afterward, a discussion was offered in Section 5 to describe the scientific contribution of the research, followed by a conclusion designed to summarize the research results in Section 6. Finally, the research implications and recommendations for future work are presented.

2. Theoretical framework

Privacy involves different dimensions whose importance changes according to the research context. Because of the inability to measure privacy itself, privacy research relies on the measurement of privacy-related constructs (e.g. privacy risk, privacy concerns, privacy perception, etc.).

While previous studies have reached a consensus on the effects of privacy-related constructs on the use of technology, there is limited consensus about the dimensionality of cloud users' privacy concerns. Different dimensions of privacy have not been separated, and users' beliefs related to various privacy antecedents remain unexplained. Previous studies have mostly focused on generic factors, such as general security and privacy (Alkhater *et al.*, 2018; Arpaci, 2016; Arpaci *et al.*, 2015; Asadi *et al.*, 2020; Lim *et al.*, 2015; Moryson and Moeser, 2015) and information privacy concerns (Ali *et al.*, 2019; Nakayama and Chen, 2019), while a minority have focused on context-specific factors, such as privacy protection risks (Yang, 2015) and privacy concerns in cloud computing services (Asadullah *et al.*, 2015). Although both types of findings are correct and useful, they need to be integrated into a unified framework. To do so, *Multidimensional developmental theory* (*MDT*) (Laufer and

Wolfe, 1977) will be used. Compared with theories built on the privacy calculus idea, *MDT* provides a broader understanding of the antecedents of privacy concerns. The theory argues that privacy concerns are a result of self-ego, environmental and interpersonal impacts. In the cloud context, the self-ego dimension can be interpreted as the impact of a user's individual characteristics (e.g. personality, experience and computer literacy) on their concept of privacy in the cloud. The environmental dimension can be interpreted as the impact of external factors (e.g. government legislation and privacy regulations) on users' ability to perceive and exercise their privacy rights. Interpersonal dimension can be interpreted as the impact of the relationship between a user and a cloud service provider (e.g. transparency, collection and use practices of cloud service providers) on users' beliefs regarding the protection of data entrusted to cloud service providers.

While the popular instruments for measuring privacy concerns (Malhotra *et al.*, 2004; Smith *et al.*, 2011), are commonly used in other contexts, the majority of cloud privacy studies do not use them (Fox, 2021). Privacy concerns in the cloud have mostly been conceptualized as a single first-order factor. The authors argue that cloud privacy concerns are a particular case of a general privacy concern, whose dimensions have yet to be determined. The existing research was therefore used to identify the specific privacy issues associated with cloud services (i.e. lack of visibility, control and transparency, vulnerabilities related to the nature of the cloud and the difficulty of achieving regulatory compliance, confidentiality and accountability), while the contribution of the paper lies in the categorization of identified problems and proposal of a conceptual model representing cloud privacy concerns. In this paper, the term *cloud privacy concerns (CPC)* is defined as users' negative beliefs regarding the protection of data entrusted to cloud service providers.

3. Methodology

The review of the literature was made to identify the key privacy problems that were most often raised in previous cloud research, categorize cloud privacy problems and propose dimensions of cloud privacy problems and identify the privacy-related constructs that were used to measure privacy concerns in previous cloud research. The following search string was used:

> TITLE-ABS-KEY [("privacy issue*" OR "privacy problem*" OR "privacy challenge*" OR "data protection issue*") AND (cloud service*)], with a time limit from 2015 until 2021 and a subject area limited to computer science. Only papers published in English were included, and only peer-reviewed articles and conference papers were considered. The main idea was to identify the cloud related problems and build conceptual model using bottom-up approach. The word "privacy concern" was excluded from the search string because the papers returned as a result used primarily standard instruments for measuring general privacy concern. The limitation in years was set to include only current cloud problems and exclude those that are outdated or handled. The literature search consisted of two phases. In the first phase, the search was made in Scopus and WoS, as they have the biggest coverage of computer science content, provide a respectable number of papers, allow the use of the same search string and are accessible to the authors of the paper. In the second phase, the search was made in ScienceDirect to check if any further relevant papers would emerge and to assess whether additional databases should be included in research. The databases providing technical literature (e.g. IEEE) were excluded from the search.

For a paper to be considered, it had to satisfy at least one of the following criteria:

(1) provide a review of cloud privacy problems;

(2) develop a conceptual model or framework to explain cloud users' privacy perceptions; or

(3) explore the privacy perceptions of cloud users through various means (questionnaires, experiments, etc.).

Cloud privacy problems addressed in previous research served as an input for a new conceptual model. Previous conceptual models and frameworks were used to explore different approaches and study the dimensionality of cloud privacy concern. Methods of exploring privacy perceptions were analyzed to determine the constructs used within existing privacy-related measuring instruments and to recognize the research gap.

The selection of papers was conducted in two stages:

(1) a document title and abstract screening was conducted, which segregated the papers as included or excluded; and

(2) a full-text screening of available papers was conducted, and the data were extracted.

The next step of the research was to consider the dimensionality of users' privacy concerns when using cloud services. *Content analysis* (Erlingsson and Brysiewicz, 2017) was used to identify privacy problems that were most often raised in previous cloud research. Although the research frequency may not ideally match users' privacy perceptions, this approach has been successfully used in previous research with related topic (Earp *et al.*, 2005; Smith *et al.*, 2011). The objective was to transform privacy problems into organized and compact categories. After gaining a general understanding of privacy problems in the cloud environment, each paper was divided into meaning units. The code for each meaning unit was formulated to make it easier to identify the connections between the measuring units. The codes were then compared and assessed to determine which seemed to belong together, thereby forming a category. Each category consists of privacy problems that appear to present the same concept. The preparation and initial proposal of categories was done by one author. The other author made a thorough review of the proposed categorization and suggested a few minor modifications.

MDT (Hong and Thong, 2013; Laufer and Wolfe, 1977) was used to build a conceptual model of cloud privacy concerns. This theory provides a broad description of the different dimensions that affect users' privacy perceptions. According to *MDT*, users' privacy concerns are defined by users' individual characteristics, their interactions with others and environmental factors, while control/choice is a mediating variable that influences and is influenced by the situation.

Finally, a review of all items used in instruments that were measuring privacy concerns in cloud services was conducted. The aim of this step was to identify the categories and dimensions of privacy problems that were addressed in previous research, to compare them with the ones identified in this paper and to recognize the research gap.

4. Results

4.1 Presenting the search results

The first phase of search resulted in 423 papers in Scopus, and 373 papers in WoS, of which 260 were duplicates. The second stage of a search resulted in 14 papers in ScienceDirect, of which 12 were duplicates, confirming the adequate coverage of the topic. Therefore, no additional databases were included in research. After removing the duplicates, 538 papers remained (423 in Scopus, 113 in WoS and 2 in ScienceDirect), and they were reviewed based on the document title and abstract. Only 88 papers that met the inclusion criteria were included in the next stage of selection. Papers dealing solely with technical issues (encryption, algorithms, protocols, etc.) as well as papers related to IoT, fog computing, 5 G networks, blockchain and similar technologies were excluded from research. The full-text screening of 88 papers resulted in the final set of 51 studies (42 in Scopus and 9 in WoS), which were included in the subsequent analysis.

4.2 Extracting and categorizing privacy problems arising from the use of cloud services

During the content analysis of the papers that matched the first inclusion criteria (i.e. provided a review of cloud privacy issues), each paper was broken into smaller units. The extraction of cloud privacy problems resulted in a comprehensive list of 58 codes. The comparison and evaluation of the codes resulted in their further categorization into 13 categories of privacy problems. The codes and categories are presented in Table 1. Such categorization enables further processing of results and classification of the identified categories of privacy problems into one of the dimensions of cloud privacy concerns.

Descriptions of the most relevant cloud privacy problems identified in each category of privacy problems in the cloud are provided in Table 2. The descriptions were composed based on a synthesis of the problems proposed by several authors. The synthesis consisted of thorough processing of each research paper and the extraction of plausible descriptions. These descriptions are based on the most discussed privacy problems relevant to the cloud context.

Out of 184 mentions of identified privacy problems, most were categorized as confidentiality, integrity and availability problems. These three categories of problems had more than 20 mentions in the reviewed set of papers. On the other hand, the least mentioned problems, with fewer than 10 mentions in the reviewed set of papers, were related to transparency, collection, and storage limitation practices of cloud service providers. The frequency of occurrence of privacy problems assigned to each category was identified by quantitative analysis (Table 3).

4.3 Building the conceptual model of cloud privacy concerns

After the main categories of cloud privacy problems were identified, the final set of papers (51 papers) was reviewed to identify the proposed privacy dimensions. The literature review found little consensus regarding the conceptualization of cloud privacy concerns. Some authors have conceptualized cloud privacy concerns as a second-order factor; few have conceptualized them as a combination of second-order and first-order factors, while most

Category	Code
Accountability	Data provenance, right for investigating abnormal or illegal activities investigative support, compliance, enforcement, liability, dynamic provision, non-repudiation
Authentication and authorization	Identity security, denial of service, data recovery
Availability	Data-long-term viability, unexpected incidents, data backup and redundancy, data leakage, data sanitization, data protection, data encryption, well-secured data
Confidentiality	Abuse of cloud services, data access, data breach, unauthorized access, unnecessary access
Control	Data location, insecurity, access, individual participation, consent/choice
Collection	Limitation of collection, purpose detailing, data ownership, data duplication
Data sharing	Transborder data flow, multitenancy
Integrity	Modified or harmed data, data manipulation
Regulatory compliance	Laws and regulations, policy issues, compliance and legal issues, different laws/jurisdictions, laws of data protection, governance and legal issues, privacy policy governance, data locality issue, data segregation
Reliability	Data loss, appropriate human resources, misuse, unwanted advertising
Secondary use	Fraud, theft, unauthorized use, use limitation, privacy, notice
Transparency	Awareness, openness

Table 1. Categorization of cloud privacy problems

Problem	Description of the problem
Accountability	Multiple parties can be involved in providing the service. It is difficult to ensure that privacy policies and practices are followed by all parties and to determine who is responsible for the certain action
Authentication and authorization	The use of different identity tokens and identity negotiation protocols can result in interoperability drawbacks
Availability	It is difficult to provide on-demand service of different levels in the event of an incident or change in the terms of service
Confidentiality	It is difficult to keep data confidential and protected when relying on external providers
Control	Because of the lack of visibility, it is difficult to ensure that the user has control over their data. Customers are not comfortable storing their data on systems that reside outside of their physical range
Collection	The processing and storing of various data in cloud services (personal data, documents, metadata, keywords, etc.) create the possibility of large-scale privacy intrusions
Data sharing	It is difficult to ascertain which specific storage device will be used for data transfer and to track the transfer of data acquired by service providers to third parties
Integrity	The integrity of the encrypted data in cloud services is endangered due to the dynamic nature of the cloud. It is difficult to protect the data from unauthorized deletion, modification or use
Regulatory compliance	It is difficult to harmonize different legal and regulatory frameworks in multiple states. There is a concern about potential data misuse during the transfer to another country
Reliability	The use of multiple systems increases reliability but raises severe privacy issues
Secondary use	It is common for cloud service providers to find new uses for data (i.e. data analysis, text mining)
Storage limitation	The number of copies is difficult to trace, and it is difficult to ensure that all of them will be properly destroyed at the user's request
Transparency	It is difficult to determine where the provider's responsibilities end. There is a lack of information about the actions that they perform

Table 2.
Description of privacy problems in the cloud

authors did not recognize them as a multidimensional (higher-order) construct or did not discuss their conceptualization at all. More precisely, nine authors have conceptualized cloud privacy concern as a second-order factor, two authors have conceptualized it as a combination of second-order and first-order factors, 18 authors have conceptualized it as a mix of various first-order factors and 22 authors did not discuss its conceptualization.

A review of the proposed factor structures analyzed from the papers that matched the second criteria (i.e. developed a conceptual model or framework to explain cloud users' privacy perceptions) is presented in Table 4. As the definitions and descriptions of dimensions have varied considerably across studies, *MDT* was used to build a conceptual model for cloud privacy concerns. Interaction and information management were identified as important for research on cloud users' privacy concerns, while none of the identified categories seemed to be part of the self-ego (e.g. personality, previous experience, computer literacy) dimension.

Furthermore, although *MDT* proposes control/choice as an additional component of privacy concerns, previous research identifies it as part of interaction management. Namely, control/choice has been a strong predictor in explaining the variance of privacy concerns (Dinev and Hart, 2004; Earp *et al.*, 2005; Hong and Thong, 2013; Malhotra *et al.*, 2004; Sheehan and Hoy, 2000). Therefore, the authors propose a conceptual model of cloud privacy concerns that consists of three dimensions:

Table 3.
Categories of privacy problems in the cloud

Source	Accountability	Authentication and authorization	Availability	Confidentiality	Control	Collection	Data sharing	Integrity	Regulatory compliance	Reliability	Secondary use	Storage limitation	Transparency
Abdul Alsahib *et al.* (2015)			✓	✓	✓			✓					
Al Ladan (2016)	✓	✓	✓	✓			✓		✓	✓	✓		
Al-Omary (2019)		✓			✓				✓				
Anand *et al.* (2015)			✓	✓	✓			✓		✓	✓		
Arjun and Vinay (2016)			✓	✓			✓	✓			✓		
Asadullah *et al.* (2015)	✓		✓		✓				✓				
Cook *et al.* (2018)	✓	✓					✓		✓				
Coss and Dhillon (2019)	✓		✓	✓	✓			✓		✓	✓		✓
Dhingra and Rai (2016)	✓	✓							✓				
El Makkaoui *et al.* (2016)				✓	✓			✓	✓				
Gantner *et al.* (2015)		✓	✓	✓	✓	✓	✓	✓		✓		✓	
Ghorbel *et al.* (2017)	✓				✓	✓		✓		✓			✓
Islam *et al.* (2015)			✓	✓				✓					
Islam *et al.* (2016)	✓	✓	✓	✓			✓	✓	✓		✓		
Jena and Mohanty (2017)	✓			✓	✓				✓				✓
Kaaniche and Laurent (2017)			✓	✓				✓		✓	✓		
Kalia *et al.* (2019)	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓
Kaur and Kaur (2015)				✓				✓		✓			
Kavakli *et al.* (2015)					✓				✓		✓		
Kumar and Goyal (2019)	✓	✓		✓				✓			✓		
Mollah *et al.* (2017)			✓		✓	✓			✓		✓	✓	

(*continued*)

Table 3.

Source	Accountability	Authentication and authorization	Availability	Confidentiality	Control	Collection	Data sharing	Integrity	Regulatory compliance	Reliability	Secondary use	Storage limitation	Transparency
Nishad and Paliwal (2016)	✓	✓	✓	✓				✓					
Rawat *et al.* (2014)		✓		✓	✓								
Tabrizchi and Rafsanjani (2020)		✓											
Sanchez-Gomez *et al.* (2016)					✓			✓					
Shabalala *et al.* (2015)	✓			✓	✓	✓		✓					✓
Shallal and Bokhari (2016)			✓	✓				✓	✓				
Shankarwar and Pawar (2015)	✓		✓	✓			✓				✓		
Shin (2015)			✓					✓					✓
Shirazi *et al.* (2017)	✓		✓	✓	✓			✓	✓	✓			
Tabrizchi and Rafsanjani (2020)			✓	✓				✓					
Takabi and GhasemiGol (2019)	✓	✓	✓	✓				✓					
Teo *et al.* (2018)			✓		✓			✓			✓		
Thangavel *et al.* (2016)			✓	✓				✓					
Thilagam *et al.* (2018)			✓	✓				✓	✓				
Tiwari and Joshi (2014)		✓	✓	✓	✓			✓	✓		✓		
Waleed and Chunlin (2016)			✓	✓	✓			✓	✓	✓	✓		
Xiao and Xiao (2013)	✓		✓	✓				✓	✓	✓			
Yang *et al.* (2015)		✓			✓				✓				
Number of mentions	16	13	25	27	20	5	6	27	18	11	14	2	6

Second-order factor	First-order factor	Source
Data and storage security	Confidentiality, integrity, availability, data sharing, accountability	Islam *et al.* (2016)
Governance	Confidentiality	
Legislation	Laws and regulations	
Data security	Secondary use, confidentiality, regulatory compliance, availability	Tiwari and Joshi (2014)
	Data integrity	
	Regulatory compliance	
	Reliability	
	Control	
Data security	Confidentiality, integrity, availability	Arjun and Vinay (2016)
Data privacy	Secondary use, data sharing	
Identity security	Authentication and authorization	Takabi and GhasemiGol (2019)
Information security	Confidentiality, integrity, availability, accountability	
Legislation	Regulatory compliance, accountability	Shirazi *et al.* (2017)
Privacy threat	Secondary use, availability	Kavakli *et al.* (2015)
Privacy vulnerability	Secondary use, control, regulatory compliance and accountability	
Privacy issues	Confidentiality, integrity, availability	Thilagam *et al.* (2018)
Legislation	Regulatory compliance, accountability	
Privacy issues	Secondary use, data sharing, accountability	Shankarwar and Pawar (2015)
Security issues	Data sharing, confidentiality, availability	
Privacy issues	Secondary use, control, regulatory compliance, reliability	Shabalala *et al.* (2015)
Security issues	Availability, confidentiality, integrity	
Privacy protection	Collection, data sharing, confidentiality, control	Gantner *et al.* (2015)
Security protection	Confidentiality, integrity, storage limitation, availability, reliability	

(*continued*)

Table 4.
A conceptualization of cloud privacy concerns

Table 4.

Second-order factor	First-order factor	Source
Security issues	Control, authentication, authorization	Yang *et al.* (2015)
	Legislation	
	Integrity, confidentiality, secondary use, availability	Teo *et al.* (2018)
	Control, regulatory compliance, reliability, availability, accountability, secondary use	Al-Omary (2019)
	Confidentiality, integrity, availability	Kaur and Kaur (2015), Shirazi *et al.* (2017), Tabrizchi and Rafsanjani (2020), Thangavel *et al.* (2016)
	Secondary use, reliability, availability, integrity, control, confidentiality	Anand *et al.* (2015)
	Transparency, collection, control, secondary use, confidentiality, integrity, accountability	Ghorbel *et al.* (2017), Kalia *et al.* (2019), Shabalala *et al.* (2015)
	Confidentiality, transparency, regulatory compliance, accountability, control	Jena and Mohanty (2017)
	Control, confidentiality, integrity, reliability	El Makkaoui *et al.* (2016)
	Control, collection, awareness, transparency, accountability	Rawat *et al.* (2014)
	Confidentiality, integrity, availability, authentication, authorization, accountability, secondary use	Kumar and Goyal (2019)
	Secondary use, data sharing, control, legislation, availability, confidentiality, reliability, accountability	Al Ladan (2016)
	Confidentiality, availability, integrity, regulatory compliance	Shallal and Bokhari (2016)
	Integrity, confidentiality, authentication, authorization, accountability, availability	Nishad and Paliwal (2016)

(1) *Interaction management*: control, collection, secondary use, data sharing, transparency and reliability.

(2) *Information management*: confidentiality, storage limitation, integrity, availability, authentication and authorization.

(3) *Legislation*: regulatory compliance and accountability.

Interaction management describes how the cloud service users perceive their interaction with the cloud service provider. It relates to the user's beliefs about the collection, control, secondary use, and data-sharing practices of the cloud service provider, as well as to the user's beliefs about the transparency and reliability of the cloud service provider. Managing privacy in the cloud is challenging because of complex collection, processing and storage practices and the transfer of information across multiple platforms and jurisdictions. The service provider is responsible for storing data, thus limiting visibility and control. There is a threat of data misuse or theft, as consumers have no control over the cloud. Transparency is therefore vital to allowing users to make informed decisions. To manage privacy in the cloud, users need to have the right to access their information and take actions to protect their privacy.

Information management describes how cloud service users perceive the management of their personal information by cloud service providers. It relates to the user's beliefs about storage limitations and the integrity, confidentiality and availability of the data, as well as to users' beliefs about authentication and authorization services. Access to sensitive information should be restricted to individuals who have specific permission to use that information. In case of data breach, it is necessary to know how far outsourced data can be used, verified or recovered by the data owners. Data can be affected temporarily or permanently, and the situation can result in partial or complete data loss. Finally, the destruction of data is challenging because replicas can be stored in different geographical locations.

Regulatory compliance and accountability are part of the environmental dimension, which was classified as *legislation* because both categories relate to users' beliefs about laws that impact their privacy and no other categories (i.e. cultural, sociophysical or life cycle elements) that compose the environmental dimension have been identified as cloud privacy problems. Different countries have defined similar principles to identify the framework on which privacy protection is based. Currently, the *General Data Protection Regulation (GDPR)* is one of the most important data protection laws that apply to both EU and non-special case-EU organizations. Cloud providers must ensure that privacy policies and practices are followed. In addition, rules enabling cloud users to exercise their rights should be made to meet privacy obligations.

The conceptual model of cloud privacy concerns is presented in Figure 1.

4.4 Measuring privacy in the cloud

After identifying the categories and dimensions of privacy problems related to cloud services, the final set of papers was analyzed to detect the instruments that were used to measure privacy concerns in cloud services. Only 10 publications met the third inclusion criterion (measuring privacy perceptions of cloud users). The items used in measuring instruments used in those papers were examined. The aim was to identify relevant cloud privacy problems that were tackled by previous research, compare them with the categories of privacy problems proposed by the authors and determine which of them are insufficiently explored in the cloud context. The following section describes the privacy-related constructs used in previous research on cloud services. These constructs are listed in Table 5, where

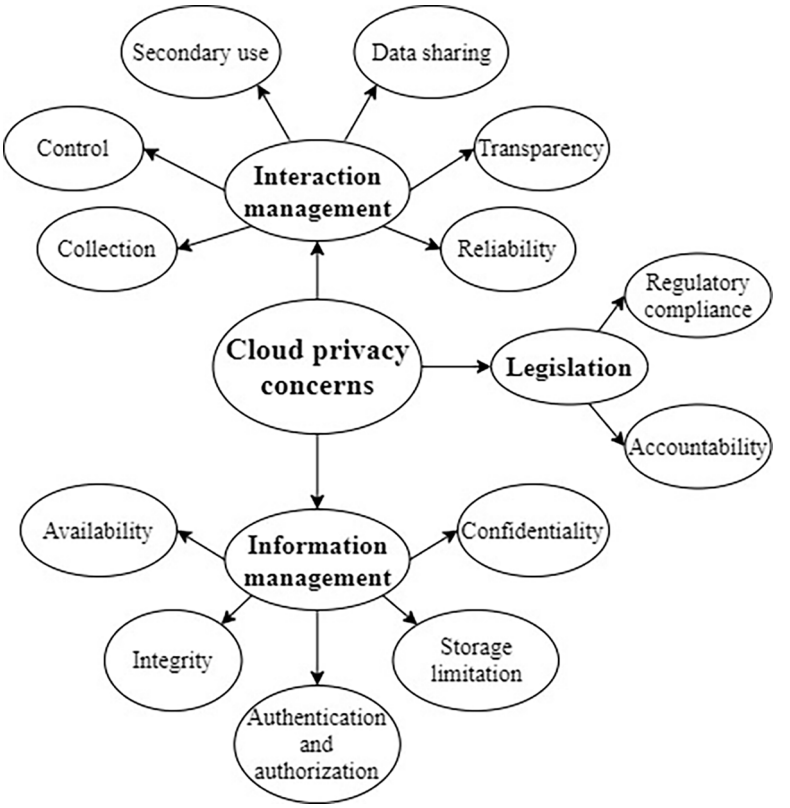

Figure 1.
A conceptual model of cloud privacy concerns

Table 5.
Privacy-related constructs mapped on authors' conceptual model of cloud privacy concerns

Constructs	Categories	References
Security-Privacy	General	Asadi *et al.* (2020)
Perceived internet privacy risk, cloud information privacy concern	Secondary use, data sharing	Ali *et al.* (2019)
Privacy	Control, Secondary use	Alkhater *et al.* (2018)
Perceived privacy	General	Arpaci (2016)
Privacy protection risk, lack of privacy-policy risk	Secondary use, Regulatory compliance	Yang (2015)
Perceived security risk	General	Moryson and Moeser (2015)
Security-Privacy	General	Arpaci *et al.* (2015)
Perceived obstacles	General	Lim *et al.* (2015)
Privacy concerns	Secondary use	Nakayama and Chen (2019)
Privacy risk, Privacy concern	Secondary use, Data sharing,	Asadullah *et al.* (2015)
Privacy control and regulatory compliance	Control, Regulatory compliance	

they are matched with the corresponding categories of privacy problems identified by the authors.

The constructs *security-privacy, perceived privacy, perceived security risk* and *perceived obstacles* were used to measure users' beliefs related to sending data to the cloud (*general privacy concern*). These constructs contained a mix of questions concerning users' trust in cloud services and beliefs related to providers' management practices. The constructs *cloud information privacy concern* and *privacy concern* were used to measure users' beliefs that their data in the cloud would be improperly accessed or disclosed (*data sharing*). The constructs *perceived internet privacy risk, privacy protection risk, privacy concerns* and *privacy risk* were used to measure users' concerns that their data would be used in an inappropriate manner (*secondary use*). The construct *privacy* was used to measure users' concern for theft or misuse of their personal data (*control* and *secondary use*). The construct *privacy control* was used to measure users' beliefs about control over processing and access to personal data in the cloud (*control*). Finally, the constructs *lack of privacy-policy risk* and *regulatory compliance* were used to measure users' beliefs about being protected by privacy regulations (*regulatory compliance*).

It is important to note that only a few papers have used some kind of instrument for measuring privacy-related constructs. The rest of the papers focused on providing technical solutions to cloud privacy problems (i.e. encryption). Most of the instruments were based on items that had been used in previous research on Internet privacy concerns. Furthermore, not only were all measuring instruments unidimensional but they were also intended to measure only one, or in the best case, a limited number of categories of cloud privacy problems. Therefore, they were unable to explain users concerns related to different privacy problems. Problems concerning *collection, transparency, reliability, storage limitation, integrity, availability, accountability, authentication and authorization* were not measured explicitly. Although some authors mentioned the collection and data-sharing practices of cloud service providers when measuring general privacy concerns, the summary of results does not explain users' particular concerns. Therefore, the constructs used with existing privacy-related measuring instruments need to be complemented with the new cloud-specific constructs identified in this research.

5. Discussion

This section discusses the significance of the research results compared to what is already known about cloud privacy concerns.

Previous research has been inconsistent with the terminology regarding cloud privacy problems. The same problems were often labeled and defined in a different manner across studies, while different problems were defined using the same concept. This research provides systematized and concise categories for privacy problems and their descriptions and definitions.

Previous research has proposed various dimensions of privacy concerns, some of which overlap, and some of which comprise completely different categories of privacy problems. However, most authors did not recognize the multidimensional structure of privacy concerns, because they were focused on explaining privacy problems from a technical perspective. This research identifies three dimensions that form the basis for the conceptualization of cloud privacy concerns. By using *MDT* as a theoretical framework, the identified categories of privacy problems were grouped into three key dimensions: interaction management, information management and legislation. A similar approach was used by Hong and Thong (2013) in their study on internet privacy concerns.

As only a few reviewed papers have focused on measuring the privacy concerns of cloud users, a wide range of privacy problems has remained insufficiently explored. The impact of these problems on user's cloud privacy perception is yet to be determined, and the theoretical framework provided in this paper is intended to serve as the stepping stone into future research. Furthermore, as the measuring instruments used in previous research were unidimensional, there is a gap in the knowledge about users' perceptions of the core cloud privacy problems highlighted in this research. It should be noted that users probably do not care equally about all the categories of privacy problems proposed within the paper. Nevertheless, their perceptions regarding various categories of privacy problems should be considered to better understand their needs. The categories of privacy problems presented within the paper will provide a higher degree of abstraction and facilitate the exploration of the relationships between them.

6. Conclusion

The use of cloud services depends greatly on perceived privacy. However, our research shows that cloud privacy concerns are a complex and comprehensive issue that needs to be further studied. Namely, research conducted to understand privacy problems in the cloud lacks an understanding of current privacy issues. Without an understanding of users' privacy concerns, privacy protection cannot be successfully communicated to users, and actions aimed at encouraging the use of cloud services can easily fail. Although the use of cloud services is higher than ever before, the number of users is still relatively low. Only 35% of the total EU population (16–74 years old) uses cloud services (Individuals - use of cloud services, 2020). Therefore, it is important to explore how to address cloud users' privacy perceptions.

To maximize the potential of cloud services and to better understand behaviors related to users' privacy concerns when using cloud services, users' beliefs regarding specific privacy dimensions should be considered. To get closer to achieve that goal, this paper provided the following outcomes:

- systematization of recent cloud privacy research;
- categorization of cloud privacy problems and proposal of a conceptual model of cloud privacy concerns;
- identification of measuring instruments that were used to measure privacy concerns in previous cloud research; and
- identification of the categories of problems that need to be addressed in future cloud research.

6.1 Research implications

The findings of this research are useful for researchers and cloud service providers. First, researchers were provided with an overall review and categorization of cloud privacy problems. As the findings of previous research were inconsistent, it would be beneficial to jointly study the various possible antecedents of cloud privacy concerns. The simultaneous examination of the identified categories of problems should clarify the effects of different dimensions on the privacy concerns of cloud users. Second, the conceptual model of cloud privacy concerns will allow cloud service providers to focus on key problems affecting users' privacy concerns. This will help them use the most appropriate privacy protection communication and preservation approaches. Furthermore, proposed model can be used when implementing the principles of data

protection in the cloud. Finally, a gap in the knowledge about users' perceptions of the core cloud privacy problems was detected. The measuring instruments used in previous research were unidimensional and unable to explain users concerns related to different privacy problems. Most cloud privacy problems were not measured explicitly. This research has provided new cloud-specific constructs that were needed to tackle this problem.

6.2 Limitations and future work

This paper has a few limitations that could be explored in future work. First, although the databases used to search the relevant literature are the most widely used for bibliometric analyses and provide the most exhaustive coverage, future work may be expanded by including more databases [e.g. *the IEEE/IET Electronic Library, Inspec and The Directory of Open Access Journals (DOAJ)*]. Second, it relies solely on the work of other authors. As a result, it gives a clear categorization of cloud-related privacy problems, but does not provide any insight into user's perceptions of these problems. This exclusive reliance on previous work can be handled in future work by discussing the proposed dimensions with cloud users. Third, the proposed conceptual model was not validated. The paper's main focus was on summarizing and conceptualizing cloud privacy issues. As a result, a theoretical framework on the dimensionality of cloud user's privacy perceptions was provided and new context-specific dimensions were presented. The relationships between the constructs should be estimated in future research to check the predictive capabilities of the proposed conceptual model. Fourth, none of the identified categories of cloud privacy problems were part of the self-ego (e.g. personality, previous experience, computer literacy) dimension. However, this dimension should not be neglected in future research; rather, it should be treated as having a moderating effect on the relationships between the other three dimensions and cloud privacy concerns. Fifth, only the privacy-related constructs identified in the papers that met all the inclusion criteria were presented. Although this list provides valuable insight into the practices of measuring privacy in the cloud and supports claims from previous papers, further research is advised to identify existing measuring instruments that could be relevant to the context of cloud services. Finally, future research should focus on the development and validation of instruments that will measure the more specific concerns of cloud users. As it is likely that users do not perceive all cloud issues as equally concerning, future research should compare the importance of the proposed constructs.

References

Abdul Alsahib, S., Aldeen, Y., Salleh, M. and Abdur Razzaque, M. (2015), "A survey paper on privacy issue in cloud computing", *Research Journal of Applied Sciences, Engineering and Technology*, Vol. 10 No. 3, pp. 328-337.

Al Ladan, M.I.A. (2016), "A review and a classifications of mobile cloud computing security issues", *International Conference on Cyber Warfare and Security*, p. 10.

Ali, U., Mehmood, A., Muhammad, F.M., Muhammad, S., Khan, M.K., Song, H. and Malik, K.M. (2019), "Innovative citizen's services through public cloud in Pakistan: user's privacy concerns and impacts on adoption", *Mobile Networks and Applications*, Vol. 24 No. 1, pp. 47-68.

Alkhater, N., Walters, R. and Wills, G. (2018), "An empirical study of factors influencing cloud adoption among private sector organisations", *Telematics and Informatics*, Vol. 35 No. 1, pp. 38-54.

Al-Madhagy, T.H.G. (2018), *Acceptance Model of SaaS Cloud Computing at Northern Malaysian Main Campus Public Universities*, Universiti Utara Malaysia, Kedah.

Al-Omary, A. (2019), "A secure framework for mobile cloud computing", *Presented at the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 1-6.

Anand, P., Ryoo, J. and Kim, H. (2015), "Addressing security challenges in cloud computing – a pattern-based approach", *Presented at the 2015 1st International Conference on Software Security and Assurance (ICSSA)*, pp. 13-18.

Arjun, U. and Vinay, S. (2016), "A short review on data security and privacy issues in cloud computing", *Presented at the 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, pp. 1-5.

Arpaci, I. (2016), "Understanding and predicting students' intention to use mobile cloud storage services", *Computers in Human Behavior*, Vol. 58, pp. 150-157.

Arpaci, I., Kilicer, K. and Bardakci, S. (2015), "Effects of security and privacy concerns on educational use of cloud services", *Computers in Human Behavior*, Vol. 45, pp. 93-98.

Asadi, Z., Abdekhoda, M. and Nadrian, H. (2020), "Cloud computing services adoption among higher education faculties: development of a standardized questionnaire", *Education and Information Technologies*, Vol. 25 No. 1, pp. 175-191.

Asadullah, A., Oyefolahan, I.O., Bawazir, M.A. and Hosseini, S.E. (2015), "Factors influencing users' willingness to use cloud computing services: an empirical study", in *Recent Advances in Information and Communication Technology*, Springer International Publishing, Cham, pp. 227-236.

CISCO (2019), Consumer Privacy Survey.

Cloud Computing Basics (2022), "Federal office for information security", available at: www.bsi.bund.de/EN/Topics/CloudComputing/Basics

Cook, A., Robinson, M., Ferrag, M.A., Maglaras, L.A., He, Y., Jones, K. and Janicke, H. (2018), "Internet of cloud: security and privacy issues", in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, Springer, New York, NY, pp. 271-301.

Coss, D.L. and Dhillon, G. (2019), "Cloud privacy objectives a value based approach", *Information and Computer Security*, Vol. 27 No. 2.

Dhingra, A.K. and Rai, D. (2016), "Evaluating risks in cloud computing: security perspective", *Presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 533-536.

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents – measurement validity and a regression model", *Behaviour and Information Technology*, Vol. 23 No. 6, pp. 413-422.

Earp, J.B., Anton, A.I., Aiman-Smith, L. and Stufflebeam, W.H. (2005), "Examining internet privacy policies within the context of user privacy values", *IEEE Transactions on Engineering Management*, Vol. 52 No. 2, pp. 227-237.

El Makkaoui, K., Ezzati, A., Beni-Hssane, A. and Motamed, C. (2016), "Cloud security and privacy model for providing secure cloud services", *2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, IEEE, pp. 81-86.

Erlingsson, C. and Brysiewicz, P. (2017), "A hands-on guide to doing content analysis", *African Journal of Emergency Medicine*, Vol. 7 No. 3, pp. 93-99.

Fox, G. (2021), "Understanding and enhancing consumer privacy perceptions in the cloud, in", Lynn, T., Mooney, J.G, van der Werff, L. and Fox, G. (Eds), *Data Privacy and Trust in Cloud Computing*, Springer International Publishing, Cham, pp. 59-78.

Gantner, J., Demetz, L. and Maier, R. (2015), "All you need is trust – an analysis of trust measures communicated by cloud providers", in Debruyne, C., Panetto, H., Meersman, R., Dillon, T.,

Weichhart, G., An, Y. and Ardagna, C.A. (Eds), *On the Move to Meaningful Internet Systems: OTM 2015 Conferences*, Springer International Publishing, Cham, pp. 557-574.

Ghorbel, A., Ghorbel, M. and Jmaiel, M. (2017), "Privacy in cloud computing environments: a survey and research challenges", *The Journal of Supercomputing*, Vol. 73 No. 6, pp. 2763-2800.

Hong, W. and Thong, J.Y.L. (2013), "Internet privacy concerns: an integrated conceptualization and four empirical studies", *Mis Quarterly*, Vol. 37 No. 1, pp. 275-298.

Individuals – use of cloud services (2020), "Eurostat", available at: https://ec.europa.eu/eurostat/web/products-datasets

Islam, T., Manivannan, D. and Zeadally, S. (2016), "A classification and characterization of security threats in cloud computing", *International Journal of Next-Generation Computing*, Vol. 7.

Islam, S., Ouedraogo, M., Kalloniatis, C., Mouratidis, H. and Gritzalis, S. (2015), "Assurance of security and privacy requirements for cloud deployment models", *IEEE Transactions on Cloud Computing*, Vol. 6 No. 2, pp. 387-400.

Jena, T. and Mohanty, J.R. (2017), "Cloud security and jurisdiction: need of the hour", in Satapathy, S.C., Bhateja, V., Udgata, S.K. and Pattnaik, P.K. (Eds), *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Springer, Singapore, pp. 425-433.

Kaaniche, N. and Laurent, M. (2017), "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms", *Computer Communications*, Vol. 111, pp. 120-141.

Kalia, P., Sofat, S. and Bansal, D. (2019), "Analyzing privacy issues in cloud computing using trust model", *Proceedings of 2nd International Conference on Communication, Computing and Networking*. Springer, New York, NY, pp. 1041-1052.

Kaur, R. and Kaur, J. (2015), "Cloud computing security issues and its solution: a review", *2nd International Conference on Computing for Sustainable Global Development (INDIACom). Presented at the 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1198-1200.

Kavakli, E., Kalloniatis, C., Mouratidis, H. and Gritzalis, S. (2015), "Privacy as an integral part of the implementation of cloud solutions", *The Computer Journal*, Vol. 58 No. 10, pp. 2213-2224.

Kumar, R. and Goyal, R. (2019), "On cloud security requirements, threats, vulnerabilities and countermeasures: a survey", *Computer Science Review*, Vol. 33, pp. 1-48.

Laufer, R.S. and Wolfe, M. (1977), "Privacy as a concept and a social issue: a multidimensional developmental theory", *Journal of Social Issues*, Vol. 33 No. 3, pp. 22-42.

Lim, N., Grönlund, Å. and Andersson, A. (2015), "Cloud computing: the beliefs and perceptions of swedish school principals", *Computers and Education*, Vol. 84, pp. 90-100.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Mollah, M.B., Azad, Md, A.K. and Vasilakos, A. (2017), "Security and privacy challenges in mobile cloud computing: survey and way ahead", *Journal of Network and Computer Applications*, Vol. 84, pp. 38-54.

Moryson, H. and Moeser, G. (2015), "Lucky users on cloud nine? Determinants of cloud computing usage behavior in Germany", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 6, pp. 375-385.

Nakayama, M. and Chen, C.C. (2019), "Length of cloud application use on functionality expectation, usability, privacy, and security", *Pacific Asia Journal of the Association for Information Systems*, Vol. 11.

Nikkhah, H.R., Grover, V. and Sabherwal, R. (2018), "Why do users continue to use mobile cloud computing applications? A security-privacy", *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*.

Nishad, L.S. and Paliwal, J. (2016), "Security, privacy issues and challenges in cloud computing: a survey", *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, p. 7.

Personal Cloud Market (2020), "Personal cloud market (no. 5031482)", Allied Analytics LLP.

Rawat, D.B., Bista, B.B. and Yan, G. (Eds) (2014), "Security, privacy, trust, and resource management in mobile and wireless communications", *Advances in Information Security, Privacy, and Ethics*, IGI Global. New York, NY.

Sanchez-Gomez, A. Diaz, J. and Arroyo, D. (2016), "Combining usability and privacy protection in free-access public cloud storage servers: review of the main threats and challenges".

Shabalala, M.V., Tarwireyi, P. and Adigun, M.O. (2015), "Addressing privacy in cloud computing environment", in Nungu, A., Pehrson, B., Sansa-Otim, J. (Eds), *E-Infrastructure and e-Services for Developing Countries*, Springer International Publishing, Cham, pp. 144-153.

Shallal, Q. and Bokhari, M. (2016), "Security and privacy issues in cloud computing", *Transaction of the International Conference on Endodontics. International Conference on Endodontics*.

Shankarwar, M. and Pawar, D.A. (2015), "Security and privacy in cloud computing: a survey", *Advances in Intelligent Systems and Computing*, Vol. 328, pp. 1-11.

Sheehan, K.B. and Hoy, M.G. (2000), "Dimensions of privacy concern among online consumers", *Journal of Public Policy and Marketing*, Vol. 19 No. 1.

Shin, D. (2015), "Beyond user experience of cloud service: implication for value sensitive approach", *Telematics and Informatics*, Vol. 32 No. 1, pp. 33-44.

Shirazi, F., Seddighi, A. and Iqbal, A. (2017), "Cloud computing security and privacy: an empirical study", *International Conference on Human-Computer Interaction*, Springer, New York, NY, pp. 534-549.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35, p. 989.

Tabrizchi, H. and Rafsanjani, M.K. (2020), "A survey on security challenges in cloud computing: issues, threats, and solutions", *The Journal of Supercomputing*, Vol. 76 No. 12, pp. 9493-9532.

Takabi, H. and GhasemiGol, M. (2019), "Introduction to the cloud and fundamental security and privacy issues of the cloud", in Chen, L., Takabi, H., Le-Khac, N.-A. (Eds), *Security, Privacy, and Digital Forensics in the Cloud*, John Wiley and Sons Singapore Pte. Ltd., Singapore, pp. 1-22.

Teo, M., Mahdin, H., Hwee, L.J., Dicken, H.A., Hui, T.X., Ling, T.M. and Azmi, M.S. (2018), "A review on cloud computing security", *Joiv International Journal on Informatics Visualization*, Vol. 2 Nos 4/2, p. 293.

Thangavel, M., Varalakshmi, P. and Sridhar, S. (2016), "An analysis of privacy preservation schemes in cloud computing", *Presented at the 2016 IEEE International Conference on Engineering and Technology (ICETECH)*, pp. 146-151.

Thilagam, T., Arthi, K. and Amuthadevi, C. (2018), "A survey on security and privacy issues in cloud computing", *International Journal of Engineering and Technology*, Vol. 7 No. 2.4, p. 88.

Tiwari, P.K. and Joshi, S. (2014), "A review of data security and privacy issues over SaaS", *Presented at the 2014 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, IEEE, *Coimbatore*, pp. 1-6.

Waleed, A.-M. and Chunlin, L. (2016), "User privacy and security in cloud computing", *International Journal of Security and Its Applications*, Vol. 10 No. 2, pp. 341-352.

Xiao, Z. and Xiao, Y. (2013), "Security and privacy in cloud computing", *IEEE Communications Surveys and Tutorials*, Vol. 15 No. 2, pp. 843-859.

Yang, H.-L. (2015), "User continuance intention to use cloud storage service", *Computers in Human Behavior*, Vol. 52.

Yang, Y., Zhao, C. and Gao, T. (2015), "Cloud computing: security issues overview and solving techniques investigation, in", Al-Saidi, A., Fleischer, R., Maamar, Z., Rana, O.F. (Eds), *Intelligent Cloud Computing*, Springer International Publishing, Cham, pp. 152-167.

About the authors

Dijana Peras is a teaching assistant in the Faculty of Organization and Informatics, University of Zagreb, Croatia, and she is working toward her Ph.D. degree in the Department of Information Systems Development. Her research interests include privacy concerns, personal data protection and cloud services. Her educational background includes a master's degree in the field of information science in 2010 and a bachelor's degree in information systems in 2008, all at the Faculty of Organization and Informatics, University of Zagreb, Croatia. Dijana Peras is the corresponding author and can be contacted at: dijana.peras@foi.unizg.hr

Renata Mekovec is an Associate Professor in the Faculty of Organization and Informatics, University of Zagreb, Croatia. Her educational background includes a PhD in the field of information and communication science in 2011, a master's degree in the field of information science in 2006, and a bachelor's degree in information systems (informatics) in 1997, all at the University of Zagreb. Her research interests lie in the fields of privacy and personal data protection, e-service quality and evaluation of e-service quality, and e-service users' perception of privacy and e-service quality.