Perceived Security and Privacy of Cloud Computing Applications Used in Educational Ecosystem

Tihomir Orehovački *, Darko Etinger * and Snježana Babić **
*Juraj Dobrila University of Pula, Department of Information and Communication Technologies, Pula, Croatia
{tihomir.orehovacki, darko.etinger}@unipu.hr
** Polytechnic of Rijeka, Department of Business, Rijeka, Croatia
snjezana.babic@veleri.hr

Abstract – When employed in educational settings, cloud computing applications enable users to create, store, organize, and share divergent artefacts with their peers. As an outcome, they have a large number of users worldwide which makes them vulnerable to a variety of security and privacy related threats. With an aim to examine the extent of the perceived security and privacy in the context of cloud computing applications that are most commonly used for educational purposes, an empirical study was carried out. Participants in the study were students from two Croatian higher education institutions. Data was gathered by means of the post-use questionnaire. Study findings uncovered pros and cons of examined cloud computing applications with respect to the manner they are addressing security and privacy concerns of their users.

I. INTRODUCTION

The introduction of Cloud Computing technologies in higher education institutions improves the efficiency of existing resources usage, as well as the reliability and scalability of software tools and applications, enabling users to create, store, organize, and share divergent artefacts with their peers.

According to the National Institute of Standards and Technology (NIST) definition, "the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction" [1]. The cloud computing follows simple "pay as you go" (PAYG) model, where you pay for the services you've used [2].

Cloud computing is an emerging new computing environment for delivering computing services which can be categorized regarding its basic components, deployment models and service delivery models. An overview of Cloud computing components is presented in Figure 1. [3].

The demand for cloud computing applications in educational ecosystem builds on the promises of free to low-cost alternatives to expensive tools. Cloud computing applications are especially suitable for educational institutions lacking technical expertise [4] to support their own IT infrastructure. According to [5] and [6], students and higher education institutions benefited from the advantages and effectiveness that cloud computing applications provided them.

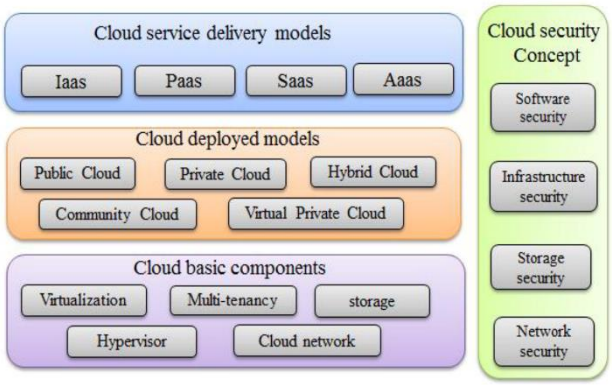

Figure 1. Cloud Computing Framework [3]

While cloud computing applications present a great opportunity for educational institutions, its usage raises concern about a variety of security and privacy threats, by placing a very large amount of student, teacher and institution data into the hands of a third-party service providers [7].

The objective of this paper is to examine the degree of perceived security and perceived privacy of cloud computing applications commonly used in educational settings.

The remainder of the paper is structured as follows. Brief theoretical foundation of our study is provided in next section. Findings of an empirical study are presented and discussed in third section. Concluding remarks, study limitations, and future work plans are offered in last section.

II. BACKGROUND TO THE RESEARCH

Most cloud computing applications used in the educational ecosystem today are SaaS cloud services that operate in the "public" cloud. These applications include productivity suites like Microsoft Office 365 and Google Apps along with data storage services such as Microsoft OneDrive and Google Drive.

One of the most significant barriers to cloud computing adoption are security and privacy [8], that relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security.

Among the main privacy challenges for cloud computing are complexity of risk assessment in a cloud environment, emergence of new business models and their implications for consumer privacy and achieving regulatory compliance.

The key elements and attributes of security issues are categorized by authors such as [9], [10], [11], [3] and they include availability (certify information is available when needed), integrity (sanctuary information integrity) and confidentiality (prevent unauthorized disclosure). They further elaborate and identify security apprehensions that a cloud computing user should discourse with cloud computing providers before approving: regulatory compliance, user access, data segregation and location, disaster recovery and long-term viability.

The concept of trust is elaborated by [11], with numerous trust objects and measures that can operationalize the impact of trust on the adoption of technological innovations. They identified the following items as appropriate for the operationalization of the security & trust factor in the context of cloud computing: data security, trustfulness of the cloud service provider, contractual agreements and geographical location where data is stored and processed. According to [11], security is viewed as a composite notion, namely "the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information".

A mapping of cloud service and security requirements was carried out by [12], while [13] composed a list and description of cloud computing threats, compromised attributes and related studies.

Topic areas in information privacy research include among others, information privacy concerns, information privacy attitudes, trust and information privacy and information privacy practices [13].

Examining the individuals' security and privacy concerns with their intention to use mobile applications, [14] developed a research model from the principal tenets of the theory of planned behaviour (TPB) and protection motivation theory (PMT). The study by [15] has provided early empirical support for a model that explains the formation of privacy concerns from the CPM theory perspective. The authors state that the globalization of economies and information technology and the ubiquitous distributed storage and sharing of data puts the issue of privacy on the forefront of social policies and practices. Drawing on the CPM theory, [15] developed a model suggesting that privacy concerns form because of an individual's disposition to value privacy, or situational cues that enable one person to assess the consequences of information disclosure.

III. EMPIRICAL STUDY

A. Procedure

The study was conducted during the winter semester of the academic year 2016. /17. in controlled lab conditions and was composed of two main parts: (1) scenario-based interaction with two cloud computing application for managing artefacts and (2) evaluation of their perceived security and privacy by means of the post-use questionnaire. Upon arriving to the lab, the participants were welcomed and briefly acquainted with the study. At the beginning of the scenario performance session, each participant received the form containing a list of 12 representative steps of interaction. Participants were asked to carry out all scenario steps twice – first with Google Drive and thereafter by means of Microsoft OneDrive (both shown in Figure 2). Upon finishing all the scenario steps with both cloud based applications, the participants were asked to complete the post-use questionnaire. At the end of the study, respondents were debriefed, and thanked for their participation. The duration of the study was 40 minutes.

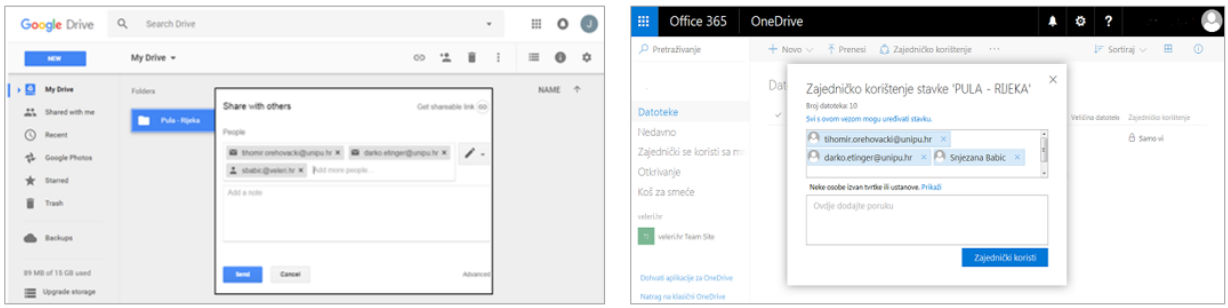

Figure 2. Examples of screenshots that indicate which level particular student reached within predefined time interval (left: Google Drive, right: Microsoft OneDrive)

B. Apparatus

The post-use questionnaire was administrated online by means of the KwikSurveys questionnaire builder. The questionnaire comprised 16 items related to participants' demography and 35 items meant for measuring facets of perceived security and privacy. Items on perceived security and perceived privacy were adopted from Cheung and Lee [16], Flavián and Guinalíu [17], Janda et al. [18], O'Cass and Fenech [19], and Ranganathan and Ganapathy [20]. Responses to the post-use questionnaire items were modulated on a five point Likert scale (1- strongly agree, 5 – strongly disagree). The psychometric features of the

measuring instrument were examined with respect to the construct validity and reliability [21]. Convergent and discriminant validity, as indicators of construct validity, were explored by means of a principal component analysis (PCA) with equamax rotation and Keiser normalization. With an aim to verify that the requirements for factor extraction were met, the Kaiser-Meyer-Olkin test of sampling adequacy and Bartlett's test of sphericity were evaluated. As a criterion for identifying the number of factors, an eigenvalue greater than one was employed. Only items with loadings above .40 and cross-loadings below .40 were retained [22]. Reliability in terms of the internal consistency of extracted factors was measured with Cronbach's Alpha coefficient.

C. Participants

A total of 318 subjects took part in the study. They ranged in age from 18 to 48 years (M = 21.03, SD = 4.197). The sample was composed of 67.30% male and 32.70% female students. At the time study took place, majority of them (50.31%) were students at Juraj Dobrila University of Pula, Department of Information and Communication Technologies while remaining 49.69% studied at Polytechnic of Rijeka. Most of the study participants (80.50%) were full-time students. When the computer literacy is considered, respondents are proficient users of both computers and the Internet. More specifically, they have between 2 and 29 years (M = 11.82, SD = 3.559) of experience in employing computers and between 2 and 20 years (M = 9.76, SD = 3.092) of experience in using the Internet. In addition, 74.21% and 82.08% of participants believe that their computer skills and Internet skills, respectively, are at least very good. When the frequency of using the Internet for different purposes is taken into account, 69.50% of respondents is employing it for communication at least 11 hours per week, 60.06% of students is using the Internet for educational purposes between 4 and 20 hours per week, 71.07% of participants is using the Internet for fun more than 11 hours per week, and 41.82% of students is using the Internet for business purposes at least one hour per week. Study participants had also been loyal users of popular social Web applications. Namely, 65.55% respondents have been socializing on Facebook for more than 6 years, 52.86% of them have been podcasting on YouTube for more than 7 years, whereas 67.96% of students have been sharing their moments with a community for less than 2 years. Regarding the length of using Google Drive and Microsoft OneDrive, 49.16% of participants have been using them for more than one year, while 12.04% have not used aforementioned cloud computing applications prior to this study.

D. Findings

The Kaiser-Meyer-Olkin measure of sampling adequacy (KMO = .936, KMO = .944) and Bartlett's test of sphericity ($\chi2$ = 7638.851, p = .000; $\chi2$ = 8026.838, p = .000) confirmed that the data in the case of both Google Drive and Microsoft OneDrive, respectively, have met the requirements for conducting the principal component analysis (PCA). During the purification procedure, eight items (SCR6, SCR7, SCR8, SCR11, SCR14, SCR15, PRV10, and PRV11) were dropped. As presented in Table 1 and Table 2 (see Appendix), the final iteration of PCA uncovered two dimensions of perceived security and four dimensions of perceived privacy, respectively. They accounted for 69.137% and 66.021% of the sample variance in the case of Google Drive and Microsoft OneDrive, respectively. Values of the Cronbach's Alpha coefficient were in range from .787 (in the case of measuring the Confidentiality of Google Drive) to .934 (in the context of evaluating Integrity of Microsoft OneDrive) thus indicating that reliability of scales was deemed adequate. Items marked with asterisk are reverse coded.

Results of data analysis indicate that 66.67% and 57.55% of study subjects believe that Google Drive and Microsoft OneDrive, respectively, have built-in high-quality mechanisms that protect users' artefacts from unauthorized use (SCR1). It was also found that 63.84% and 58.49% of students reported that Google Drive and Microsoft OneDrive, respectively, have integrated good security measures that protect their personal information (SCR2). In addition, 61.64% and 53.77% of study participants stated that Google Drive and Microsoft OneDrive, respectively, protect the security of all activities carried out by their employment (SCR3). The collected data also imply that 61.01% and 53.14% of students perceive that Google Drive and Microsoft OneDrive, respectively, have good protection mechanisms that prevent the theft of their identity by a third party (SCR4). Moreover, it was discovered that only 38.99% and 34.91% of respondents believe that Google Drive and Microsoft OneDrive, respectively, are protected to the extent that no third party cannot falsely introduce oneself to their users (SCR5).

Results of data analysis also indicate that 69.50% and 62.58% of subjects believe that Google Drive and Microsoft OneDrive, respectively, have built-in mechanisms that prevent unauthorized changes to information about the user (SCR9). Furthermore, 68.24% and 61.95% of students agree that Google Drive and Microsoft OneDrive, respectively, have built-in mechanisms that prevent unauthorized modification of stored documents (SCR10). Similarly, 75.47% and 71.70% of subjects is convinced that Google Drive and Microsoft OneDrive, respectively, verify user's identity before granting access to personal data and documents (SCR12).

The data gathered from study participants revealed that 76.73% and 71.07% of them believe that Google Drive and Microsoft OneDrive, respectively, is taking care of the protection of personal data and documents that are stored on it (SCR13). In addition, results of data analysis imply that 69.81% and 60.38% of students think that Google Drive and Microsoft OneDrive, respectively, are secure cloud computing applications (SCR16). Finally, according to data presented in Table 1, 63.52% and 57.23% of study subjects believe that Google Drive and Microsoft OneDrive, respectively, have implemented all the required security mechanisms (SCR17).

Data displayed in Table 2 imply that 32.30% and 33.65% of study participants is concerned that Google Drive and Microsoft OneDrive, respectively, will use their personal data for other purposes without their permission (PRV1). Furthermore, the findings of the pilot study imply that 39.94% and 36.48% of respondents think that Google Drive and Microsoft OneDrive, respectively, collect too

much information about their users (PRV2). It was also discovered that 31.45% and 32.70% of study subjects is concerned about the privacy of their personal information. when using Google Drive and Microsoft OneDrive, respectively (PRV3). In addition, 32.08% and 31.45% of students is concerned that Google Drive and Microsoft OneDrive, respectively, will give their personal information to third parties without their permission (PRV4). The collected data also indicate that 65.09% and 58.18% of study participants think that Google Drive and Microsoft OneDrive, respectively, take care of the privacy of their users (PRV5). Moreover, it was found that 52.52% and 46.86% of respondents feel that their privacy is protected when storing their personal information and documents on the Google Drive and Microsoft OneDrive, respectively (PRV6).

According to the results of data analysis, 70.13% and 65.72% of study subjects think that Google Drive and Microsoft OneDrive, respectively, comply with the laws and regulations on the protection of users' personal data (PRV7). In addition, 48.43% and 47.80% of students agree that Google Drive and Microsoft OneDrive, respectively, collect only the information about users that is necessary for their use (PRV8). Data gathered from students revealed that 63.84% and 61.01% of them think that while collecting data about users, Google Drive and Microsoft OneDrive, respectively, respect their rights (PRV9). Students' responses are also implying that 38.68% and 37.74% of them is afraid to provide Google Drive and Microsoft OneDrive, respectively, with their personal information because they do not know what these cloud computing applications could do with them (PRV12).

Considering the results of data analysis, 43.40% and 41.51% of students think is risky to provide Google Drive and Microsoft OneDrive, respectively, with their personal information (PRV13). It was also discovered that equal number of students (25.47%) believe that if they provide Google Drive or Microsoft OneDrive with their personal information, they could be faced with unexpected problems (PRV14). Moreover, 25.47% and 23.59% of respondents think that Google Drive and Microsoft OneDrive, respectively, could use their personal information in an inappropriate fashion (PRV15). Results of the data analysis also indicate that 34.59% and 35.54% of study participants think there is a very strong correlation between the potential loss of privacy and disclosure of personal information to Google Drive and Microsoft OneDrive, respectively (PRV16). Moreover, 43.71% and 39.31% of students believe that they have control over who has the access to their personal data collected by Google Drive and Microsoft OneDrive, respectively (PRV17). Finally, as can be observed from students' responses, 40.25% and 36.48% of them think they have control over how Google Drive and Microsoft OneDrive, respectively, are using their personal information (PRV18).

IV. CONCLUSION

The aim of this paper was to examine the perceived security and perceived privacy of cloud computing applications. For that purpose, an empirical study was carried out. Based on the data collected from study participants, psychometric features of measuring instrument were evaluated. Construct validity was tested with the use of a principal component analysis whereas Cronbach's Alpha coefficient was employed for assessing the construct reliability. As an outcome, data analysis uncovered two dimensions of perceived security (Integrity and Confidentiality) and four facets of perceived privacy (Privacy Concerns, Privacy Protection, Privacy Risks, and Privacy Control).

As with all empirical studies, some limitations which require further examination have to be acknowledged. The first one deals with the homogeneity of participants. Although students in our study are a representative sample of cloud-based applications users, perceived security and perceived privacy might vary if it would be evaluated by more heterogeneous group of users. The second limitation is that the findings cannot be generalized to all types of cloud computing applications except to the ones involved in the study. Keeping the set forth limitations in mind, study outcomes should be interpreted with caution.

Takin into account that this study is a part of an ongoing work, our future work efforts will be focused on exploring the extent to which identified aspects of perceived security and perceived privacy contribute to users' behavioural intentions regarding the employment of cloud computing applications.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.

[3] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," J. Netw. Comput. Appl., vol. 75, pp. 200–222, 2016.

[4] M. Al-zoube, "E-Learning on the Cloud," Int. Arab J. e-Technology, vol. 1, no. 2, pp. 58–64, 2009.

[5] H. Bicen, "Effects of Training on Cloud Computing Services on M-learning Perceptions and Adequacies," Procedia - Soc. Behav. Sci., vol. 116, pp. 5115–5119, 2014.

[6] T. Lis and B. Paula, "The Use of Cloud Computing by Students from Technical University – The Current State and Perspectives," Procedia Comput. Sci., vol. 65, pp. 1075–1084, 2015.

[7] S. Mutkoski, "Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide For School Administrators and Legal Counsel," John Marshall J. Inf. Technol. Priv. Law, vol. 30, no. 3, p. 3, 2014.

[8] U. J. Bora and M. Ahmed, "E-Learning using Cloud Computing," Int. J. Sci. Mod. Eng., vol. 1, no. 2, pp. 9–13, 2013.

[9] B. Hari Krishna, S. Kiran, G. Murali, and R. Pradeep Kumar Reddy, "Security Issues in Service Model of Cloud Computing Environment," Procedia Comput. Sci., vol. 87, pp. 246–251, 2016.

[10] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia Comput. Sci., vol. 48, no. Iccc, pp. 204–209, 2015.

[11] M. Stieninger, D. Nedbal, W. Wetzlinger, G. Wagner, and M. A. Erskine, "Impacts on the organizational adoption of cloud computing: A reconceptualization of influencing factors," Procedia Technol., vol. 16, pp. 85–93, 2014.

[12] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," Appl. Comput. Informatics, 2016.

[13] F. Bélanger and R. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," MIS Q., vol. 35, no. 4, pp. 1–36, 2011.

[14] G. Garrison, S. Kim, and X. Xu, "Consumer adoption and use of mobile applications: Do privacy and security concerns matter?", Issues Inf. Syst., vol. 17, no. II, pp. 56–64, 2016.

[15] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," J. Assoc. Inf. Syst., vol. 12, no. 12, pp. 798–824, 2011.

[16] C.M.K. Cheung, and M.K.O. Lee, "Trust in internet shopping: instrument development and validation through classical and modern approaches", Journal of Global Information Management, vol. 9, no. 3, pp. 23-35, 2001.

[17] C. Flavián, and M. Guinalíu, "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site", Industrial Management & Data Systems, vol. 106, no. 5, pp. 601-620, 2006.

[18] S. Janda, P. Trocchia, and K. Gwinner, "Consumer perceptions of internet retail service quality", International Journal of Service Industry Management, vol. 13, no. 5, pp. 412-431, 2002.

[19] A. O'Cass, and T. Fenech, "Web retailing adoption: exploring the nature of internet users web retailing behaviour", Journal of Retailing and Consumer Services, vol. 10, no. 2, pp. 81-94, 2003.

[20] C. Ranganathan, and S. Ganapathy, "Key dimensions of business-to-consumer web sites", Information & Management, vol. 39, no. 6, pp. 457-465, 2002.

[21] D. Straub, M. Boudreau, and D. Gefen, "Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems", vol. 13, no. 1, pp. 380–427, 2004.

[22] J.F. Hair Jr., W.C. Black, B.J. Babin, and R.E. Anderson, "Multivariate Data Analysis", 7th edn. Prentice Hall, Englewood Cliffs, 2009.

APPENDIX

TABLE I. RESPONSES OF STUDY PARTICIPANTS TO QUESTIONNAIRE ITEMS RELATED TO THE PERCEIVED SECURITY

Perceived Security Items	Google Drive		Microsoft OneDrive	
	Mean	SD	Mean	SD
Integrity (Cronbach's α = .919 and .934 in the case of Google Drive and Microsoft OneDrive, respectively)				
SCR1. I believe this application has integrated high-quality mechanisms that protect my documents from unauthorized use.	2.26	.951	2.40	.980
SCR2. The application has implemented good security measures that protect my personal information.	2.33	1.015	2.47	1.025
SCR3. I think this application protects the security of all activities carried out by its use.	2.36	.982	2.48	.985
SCR4. I think this application has good protection mechanisms that prevent the theft of its identity by a third party (other organizations or individuals).	2.35	.964	2.47	.991
SCR5. I think this application is protected to the extent that no third party (individual or organization) cannot falsely introduce oneself to its users.	2.86	1.173	2.93	1.175
SCR16. I think this application is secure.	2.16	.939	2.32	.981
SCR17. I believe that the application has implemented all the required security mechanisms.	2.30	.954	2.40	.951
Confidentiality (Cronbach's α = .787 and .792 in the context of Google Drive and Microsoft OneDrive, respectively)				
SCR9. The application has built-in mechanisms that prevent unauthorized changes to information about the user.	2.19	.853	2.30	.881
SCR10. The application has built-in mechanisms that prevent unauthorized modification of stored documents.	2.20	.846	2.30	.846
SCR12. Before granting access to personal data and documents, the application verifies user's identity.	1.99	1.054	2.02	1.073
SCR13. The application is taking care of the protection of personal data and documents that are stored on it.	1.99	.870	2.08	.913

TABLE II. RESPONSES OF STUDY PARTICIPANTS TO QUESTIONNAIRE ITEMS RELATED TO THE PERCEIVED PRIVACY

Perceived Privacy Items	Google Drive		Microsoft OneDrive	
	Mean	SD	Mean	SD
Privacy Concerns (Cronbach's α = .858 and .864 in the case of Google Drive and Microsoft OneDrive, respectively)				
PRV1. I am concerned that the application will use my personal data for other purposes without my permission.*	3.10	1.167	3.04	1.142
PRV2. I think the application collects too much information about its users.*	2.78	1.109	2.85	1.038
PRV3. When using the application, I am concerned about the privacy of my personal information.*	3.14	1.126	3.06	1.107
PRV4. I am concerned that the application will give my personal information to third parties (organizations or individuals) without my permission.*	3.20	1.216	3.18	1.179
Privacy Protection (Cronbach's α = .903 and .901 in the context of Google Drive and Microsoft OneDrive, respectively)				
PRV5. I think that the application takes care of the privacy of its users.	2.29	.926	2.37	.951
PRV6. When storing personal information and documents on the application, I feel that my privacy is protected.	2.54	.977	2.64	.955
PRV7. I think that the application complies with the laws and regulations on the protection of users' personal data.	2.14	.897	2.21	.883
PRV8. I think the application collects only the information about users that is necessary for its use.	2.67	1.106	2.67	1.055
PRV9. I think that while collecting data about users, the application respects their rights.	2.31	.961	2.36	948

* reverse coded items

TABLE II. CONTINUED

Perceived Privacy Items	Google Drive		Microsoft OneDrive	
	Mean	**SD**	**Mean**	**SD**
Privacy Risks (Cronbach's α = .863 and .862 in the case of Google Drive and Microsoft OneDrive, respectively)				
PRV12. I am afraid to provide the application with all my personal information because I do not know what it could do with them.*	2.95	1.168	2.92	1.143
PRV13. I think is risky to provide the application with my personal information.*	2.84	1.154	2.84	1.153
PRV14. If I provide the application with my personal information, I could be faced with unexpected problems.*	3.14	1.051	3.11	1.029
PRV15. I think the application could use my personal information in an inappropriate fashion.*	3.22	1.067	3.25	1.068
PRV16. I think there is a very strong correlation between the potential loss of privacy and disclosure of personal information to the application.*	2.98	1.076	2.94	1.065
Privacy Control (Cronbach's α = .880 and .861 in the context of Google Drive and Microsoft OneDrive, respectively)				
PRV17. I believe that I have control over who has the access to my personal data collected by the application.	2.86	1.067	2.91	1.078
PRV18. I think that I have control over how the application is using my personal information.	2.91	1.108	2.96	1.080

* reverse coded items