Baalous, R., Poet, R. and Storer, T. (2018) Analyzing Privacy Policies of Zero Knowledge Cloud Storage Applications on Mobile Devices. In: 2018 IEEE International Conference on Cloud Engineering (IC2E), Orlando, Florida, USA, 17-20 April 2018, pp. 218-224. ISBN 9781538650097 (doi:10.1109/IC2E.2018.00047)

Analyzing Privacy Policies of Zero Knowledge Cloud Storage Applications on Mobile Devices

Rawan Baalous
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
r.baalous.1@research.gla.ac.uk

Ronald Poet
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
ron.poet@glasgow.ac.uk

Timothy Storer
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
timothy.storer@glasgow.ac.uk

***Abstract*— With the rapid growth of mobile applications and the increase number of mobile users, many cloud storage services started to design stand-alone mobile applications that can be used to access files remotely from mobile and share them. In this paper, an in-depth analysis has been performed on the privacy policies of zero knowledge cloud storage applications on mobile. The analysis includes the type of information collected, collection mechanisms, purpose for collection, sharing of information, user controls and information retention period. The results showed that most privacy policies addressed important areas of information collection, purposes of collection, information sharing and users' controls. On the other hand, many policies lacked detailed information of the data retention period.**

Keywords—privacy policy; cloud storage; apps; mobile

I. Introduction

Cloud storage services are growing in their popularity and usage in the last years. They are used to back up files remotely so that files can be accessed from any PC, smartphone and tablet. They allow files to be shared between users and synchronized across all devices. They also provide mechanisms for disaster recovery and prevention. Sensitive files can be encrypted on the client device as well as in transit and on cloud storage servers.

The number of mobile cloud storage apps has also grown. While the improvements in the mobile environment might enhance the usability of mobile cloud storage apps, it also could affect personal privacy. The combination of mobile and privacy is problematic and may increase privacy challenges. Extra information will be exchanged between the cloud and mobile devices as much more mobile functionalities are transitioned now to the cloud. Hence, mobile phone users may be surprised by the amount of data that no longer remains localized to their phones. In addition, the new mechanisms to collect, analyze, share, and preserve this data have raised new concerns about personal privacy [1,2].

Privacy as a concept, from a broad perspective, has been defined by a number of scholars. According to Warren and Brandeis, privacy is "the right to be let alone" [3]. Altman has declared that privacy as "the selective control of access to the self" [4]. Indeed, privacy has several dimensions with various meanings [5]. It includes control over personal information and freedom from surveillance, among other things [6].

People have different concerns about privacy. These concerns may differ according to the situation or circumstances [7]. Several surveys have been conducted to study users' privacy concerns. Professor Alan Westin, for example, conducted over 30 privacy-related surveys that covered various privacy-related areas. The results showed how users concerns change over time [8]. Ackerman et al. reported high level of users' concerns about privacy, especially on the Internet [9].

Many corporations are still reluctant to migrate to the cloud due to privacy concerns [10]. In fact, these concerns have been reinforced by the vast quantity of data that is available now for analysis as well as the technological advances in data analytics mechanisms that are applied to the data. In 2012, Reno highlighted the effect of the increases in data collection capacity and improvements in analytical tools on correlating user activities and drawing conclusions [11]. Data mining can be used to sometimes derive private information that appeared to raise no, or only manageable, privacy issues when they were collected [2].

Consumers' privacy concerns and the increased demands for protecting sensitive data led some cloud storage providers to claim zero knowledge by encrypting files locally on the user device by the user's own key before uploading to the cloud. Tresorit, BoxCryptor and Cubby are examples of such cloud storage services which use a client-side encryption approach. The privacy practices of these cloud storage services can be found in their privacy policies. According to Karjoth and Schunter, the privacy policy document generally describes the data that is collected, the purposes for what they will be used, if access to data is permitted by the company, with whom the company will share the data, the data retention period, and who will be informed in what cases [12].

The purpose of this work is to assess the availability and content of privacy policies of cloud storage mobile applications which claim zero knowledge. As illustrated by [13], while using new technology might provide clear advantages, the privacy behind it still needs to be investigated. Users are not also entirely aware of the privacy practices of these applications and the information they collect, store and transmit [14]. Hence, this paper reviews the posted privacy policy of each zero knowledge cloud storage mobile application and examines the type of information collected, collection mechanisms, purpose for collection, sharing of information, user controls and information retention period.

The reminder of this work is organized as follows: the related work examining the privacy policies of website and mobile applications is discussed in Section II. Then, the method used to assess the privacy policies of zero knowledge mobile cloud storage applications is detailed in Section III. After that, the results are presented and discussed in Section IV and V respectively. Finally, the conclusion is highlighted in Section VI.

II. RELATED WORK

A growing body of literature has examined the privacy policies of websites and mobile apps in different fields. A number of these studies have focused on evaluating the readability of privacy policy documents and assesses the language used. More recently attention has focused on evaluating the content and transparency of privacy policies, particularly in the health industry.

In 2005, Earp et al. [15] published a paper in which they investigated whether privacy policies provide the users with the information they want. They started by identifying the top three popular websites in each industry, ending up with 24 websites. They used the privacy policy documents of these websites for exploratory coding of privacy statements into categories. After that, they chose the top 23 visited websites in the health care industry for data analysis. They also developed a survey to explore users' privacy concerns. Then, they compare the results of privacy policies analysis and users reported concerns. The results showed that the assessed privacy policies do not address the same dimensions of what users want to know and concerned with in privacy policy. The privacy policies focused more on the security of data collection and transfer, data collection mechanisms and opt-in, opt-out choices. On the other hand, the survey data demonstrated that users were most concerned about sharing of their data, being notified or made aware of company's data practices and knowing what users' data are stored in the company's database.

In 2009, Gomez et al. [16] analyzed the privacy policies of the top 50 visited websites. The authors were interested in revealing the type of information collected, uses of this information, and with whom it is shared. The information collected was computer information, contact information and demographic information among others. The majority of these websites use the information collected from users for customized advertising. Regarding information sharing, many of the accessed websites allowed third party tracking, although they stated that they don't share information with third parties. The results also showed a long list of affiliates and subsidiaries that websites share data with. Given this large number of affiliates, it has been recommended that users be given the control to choose to allow or not allow sharing their information with affiliates.

With regard to privacy policies in the mobile context, the study by Singh et al. [17] examined how readable the privacy policy documents are in mobile environments. Mobile devices have limited screen size and input facilities which are common challenges that affect readability. The top 10 popular websites were chosen to evaluate their privacy policies on mobile devices. Fifty users participated in the study. Each participant was given 2 different sample policies chosen randomly (one presented on a desktop and one presented on a mobile). The results indicated that technical documents such as privacy policies are difficult to read on mobile devices. It was found that readers' comprehension dropped with the length of privacy policy in both desktop and mobile environments. Display screen as well as scrolling were major concerns reported by participants in the mobile environment.

Three years later, Sunyaev et al. [18] studied the availability and quality of mobile health applications' privacy policies. The authors surveyed the top 300 rated health apps. However, only 183 apps were chosen for assessment as the others don't have privacy policies. This was quite surprising considering that in the medical health industry users could be concerned about uses or sharing of their private and sensitive data. Privacy policies contents were categorized into the following: type of information collected, rationale for collection, sharing of information and user controls. The results, overall, showed that privacy practices were not transparent and comprehensive.

Similarly, Huckvale et al. [19] examined 79 NHS health applications' privacy policies. They used the UK Information Commissioner's Office (ICO) concerning data protection principles, in order to develop a coding schema to assess the privacy policies. A variety of privacy practices were noticed in the assessed apps. Over half of privacy policies transfer personal or health-related information or both to online services. The majority of privacy policies clarify how users' information will be used. On the other hand, detailing how long data will be held by the organization was only covered by a few privacy policies, 17%.

III. METHODOLOGY

There are a number of cloud storage applications that use the zero knowledge policy and do local encryption for all files on the client device before uploading them to the cloud server. To come up with this list, the following search terms have been written in Google: "client side encryption cloud storage", "zero knowledge cloud storage" and "end to end encrypted cloud storage". Then, all the cloud storage mobile applications that do client-side encryption and are available for Android, the most popular mobile operating system, have been listed. One cloud storage application, Cloudfogger, has been excluded as it announced that it is shutting down. Cloud storage services which provide local encryption and synchronization to files that are already stored in well-known cloud storage services were also included. The final list of zero knowledge cloud storage Android apps with their characteristics in September 2016 is presented in the following table.

TABLE I. CHARACTERISTICS OF ZERO KNOWLEDGE CLOUD STORAGE ANDROID APPS

Android cloud storage apps	**Offered by**	**Rating**	**Number of downloads**
BoxCryptor	Secomba GmbH	4.3	100,000 - 500,000
CrashPlan	Code 42 Software	3.5	50,000 - 100,000
Cubby	LogMeIn, Inc	4.3	100,000 - 500,000
IDrive Online Backup	IDrive Inc	4.2	1,000,000 - 5,000,000
MEGA	Mega Ltd	4.0	10,000,000 - 50,000,000
Mozy	Mozy, Inc	3.9	10,000 - 50,000
nCryptedCloud	nCrypted Cloud	3.9	1,000 - 5,000
pCloud: Free Cloud Storage	PCloud LTD	4.3	500,000 - 1,000,000
Seafile	Seafile Ltd	4.2	50,000 - 100,000
SOS Online Backup	SOS Online Backup	3.9	10,000 - 50,000
SpiderOak ONE	SpiderOak, Inc	3.7	100,000 - 500,000
Sync.com - sync secure storage	Sync.com Inc	4.2	10,000 - 50,000
TeamDrive 4	TeamDrive Systems	3.8	1,000 - 5,000
Tresorit	Tresorit	4.3	100,000 - 500,000
Viivo	PKWARE, Inc	4.1	10,000 - 50,000

Privacy policies were evaluated in September and October 2016. The assessment method relied on manual testing and review. To assess the availability of the privacy policy, the privacy policy document needs to be located. To do so, for each app, the app store page has been checked for a privacy policy link. If not found, the cloud storage website has been checked. Finally, Google was searched by typing the cloud storage application name with the phrase “privacy policy” and the top 100 results were reviewed. If the privacy policy was not discovered by all the three methods, it has been concluded that it is not available.

After locating the privacy policy, the content has been examined based on the following [9][15][16][20][21][22]:

A. *Type of information collected and collection mechanisms*

There are different types of information that cloud storage services can collect. To begin with, when a user registers with the service, personal data will be collected. First and last name, email address, postal address and credit card number are examples of such personal data. Many companies ask for this data to provide the requested service. Furthermore, some cloud providers may collect metadata about uploaded files such as the type of the file and its size.

When the user navigates through the website, certain usage and log data are collected, such as IP address, browser version, Internet Service Provider, operating system type, software ID and accessed page. Several mechanisms are used for collecting all or part of this information. A cookie is an example of such mechanisms in which a small text file is installed on the user's device to keep track of him. HTML5 local storage is another mechanism that stores the collected data locally within the user's browser. This is different from cookies, data is never transferred to the server [23]. Web bugs, web beacons and gif files are other methods of tracking which use an embedded image in the page to determine, for example, if this page has been opened. Finally, Google analytics which is provided by the Google third party service is another mechanism that is used for tracking and web analytics.

B. *Purpose for collection*

Cloud storage services may use collected information for several purposes. They may use them for improving and developing their services as a whole. This includes understanding users' needs and personalizing their experience. The collected information will also be used for functional reasons, such as helping in administration and operation of the website and services, providing technical support and maintaining the website. More importantly, providing the user with the requested service which can be processing his payment or creating his account, for example. Some companies may collect specific information for statistical purposes to know the number of visitors to their website and the duration of each visit, for instance. Others may collect personal information for security reasons in order to make identification possible when conducting illegal activities. In addition, the collected information can be used for marketing and advertising purposes, such as sending newsletters and promotional materials. Moreover, the cloud service provider may use the customer email to communicate with him in general, not necessary for marketing purposes. This communication can be used to notify the user of a software update or to respond to his query.

C. *Sharing of information*

Information sharing is a big concern for many users. While some companies explicitly mention that they don't sell or rent the submitted information, others say that they do. More often, companies contract with third parties to provide them with certain facilities that are considered necessary for their service operation. Database storage and management, payment processing, hosting, support and maintenance are examples of these facilities. In such cases, they contract with different entities to assist them in conducting their business and improve their services. This implies that users' personal data or cookies and usage data or both will be shared with these entities. These entities may adhere to the same privacy policy followed by the cloud storage provider or even have their own privacy practices.

Context for sharing is a fundamental aspect that has been looked for in the privacy policy document. Information could be shared in response to a legal request. Other drives may include fulfilling users' orders, protecting the property of the cloud provider, stopping illegal activities such as fraud and in connection with a sale or merger of the cloud service.

D. User controls and rights

There are a number of principles that are related to user controls and rights, such as the ability to opt out of receiving advertising communications and the right to be notified if a breach happened. Some cloud storage services may afford such rights to their users while others may deny them or not explicitly state them. Another crucial right for the user is the ability to edit or delete his personal information from the cloud storage databases or even request access to his personal information held by the cloud. In addition, some users may want to know if the privacy policies have been changed or if changes happened to the cloud ownership, especially in the case of acquisition or merger, giving them the chance to update or delete their personal data. As many users may not be well informed or aware of their ability to refuse cookies, some cloud storage services could explicitly mention to their users that they have the right to decline cookies or being notified when the cookies are being sent by changing browser settings.

E. Information retention period

It is important to investigate if the cloud storage service discusses the information retention period in its privacy policy. Many users question if their personal information is stored indefinitely, especially after deleting their account, or if the cloud provider states a specific number of days during which the personal information will be retained. The same principle applies to the encrypted files. Users may also question if their files will be destroyed immediately after deleting their account, so that they will not be available to anyone, or if they are going to be retained.

The content of each privacy policy has been assessed based on these 5 categories as either being addressed or not mentioned. Results were categorized into groups to simplify the comparison between the privacy policies.

IV. RESULTS

A. Availability of the privacy policies

All the zero knowledge cloud storage Android apps had privacy policies. Most of them (12 out of 15) provided a link to their privacy policy through the app store page on Google Play. However, four of the apps (BoxCryptor, Cubby, nCryptedCloud and pCloud) provided misleading links. The BoxCryptor privacy policy link goes to its terms and conditions page which covers the agreement between Secomba GmbH, the German company that developed BoxCryptor, and the user concerning two of the company products: BoxCryptor and Whisply. The link to the actual privacy policy statement of BoxCryptor can be found on their website. Cubby was developed by LogMeIn Incorporation which has many products including Cubby. The link to the Cubby privacy policy in the app store goes to the LogMeIn privacy policy page, although Cubby has its own privacy policy which can be found through its website. The nCryptedCloud privacy policy link, on the other hand, goes to the master subscription agreement page which covers the use of nCryptedCloud software and services. The actual privacy policy document was then found in the website. Finally, pCloud directs the visitor to its home page, rather than privacy policy page, when clicked on the privacy policy link in the app store on Google Play. From the home page, the privacy policy link can be found.

There were three apps only which didn't provide a link to their privacy policy on the app store page (CrashPlan, IDrive and Seafile). The first two privacy policies were found through the cloud storage website. Unfortunately, the location of the last app privacy policy page, Seafile, was not clear on the website. After searching Google, the privacy policy was found in the Seafile forum.

B. Content of the privacy policies

The following table shows the addressed content of the privacy policies. The content categories and subcategorizes were identified in the methodology described previously. Then, the number of apps which addressed each type of content has been presented.

TABLE II. CONTENT OF THE PRIVACY POLICIES

Privacy policy content categories	**Privacy policy content subcategories**	**Number of apps**
Type of information collected	Personal information	15
	Usage or log data	15
	Files metadata	3
Collection mechanisms	Cookies	15
	HTML5 local storage	1
	Web beacons	3
	Google Analytics	3
Purpose for collection	Functional purposes	15
	Improving and developing purposes	14
	Contact and communication purposes	9
	Marketing purposes	11
	Statistical or analytical purposes	9
	Security purposes	3
Sharing of information	To fulfill users orders, deliver and enhance the services	15
	To comply with law enforcement or respond to legal processes	13
	To use it for marketing and advertisements	5
	To protect the rights, property, or safety of cloud provider , third parties or members of the public	8
	To stop illegal activities	6
	In connection with a sale, merger, acquisition or bankruptcy	8
User controls and rights	Can opt out of receiving marketing materials	10
	Informed about his right to disable cookies or remove HTML 5 local storage objects	13
	Can edit and/or delete personal information	11
	Can request access to personal information held by cloud storage provider	7

	Notified in case of change in ownership, merger and acquisition	5
	Notified of privacy policy changes via email or notice on website	12
	Notified in case of a breach happened	1
Information retention period	-	9

All discovered privacy policies stated that they collect personal information and usage or log data. This is almost expected as they need some form of personal data in the registration process to provide the requested service, such as credit card number to process transaction and email address to communicate with customers regarding their order or query. Users' activities and actions when using the app or visiting the website (usage data) were also considered important as they help to know users preferences, for example, and hence improve the product offered or service. A fifth (n = 3/15) of privacy policies explicitly mentioned that they collect metadata also. MEGA, for example, indicated that it records each file's metadata, such as the file size.

The information collection mechanisms varied between the selected apps. Cookies were a popular mean of collecting usage data. However, only one app (CrashPlan), as well as third partied whom CrashPlan partners to, use HTML5 local storage objects in conjunction with cookies.

Web beacons and Google Analytics were used by a small number of applications (n=3). Viivo, for example, uses web beacons to count the number of visitors who visited some pages or to know if a promotional email has been opened and acted upon. Google Analytics were also used by three apps. Two apps from the three made it clear that the information gathered by Google are transferred and stored in a Google server in the USA. They also described when the full IP address of the user will be sent to the Google server and when it will be truncated before sending. They informed the user that he has the option to prevent this information collection by Google and provided him with the link to download a browser add-on for opting out from Google Analytics. The third app, on the other hand, just stated that such third party services do not collect personal data and that the corporation who owned the app will not sell user personal data to these third parties without user permission.

Data collection was used for several purposes across cloud storage apps. All apps use the collected information for functional reasons such as delivering the requested service and assisting in operating the app. All apps except one mentioned that they use such information for improving and development purposes. Over half of the selected apps (n=9) use collected information, more specifically the email address, to maintain the communication channels between the cloud provider and the user, to contact the customer about his order or send him product updates and revisions. Around two-thirds of privacy policies (n = 11/15) benefit from collected information to be used for marketing activities and campaigns. Statistical or analytical purposes were reported by 9 apps and security purposes were reported by 3 apps only.

Zero knowledge cloud storage apps reported a wide range of cases where information will be shared. The top case was where shared information will be needed for fulfilling users' orders, delivering and enhancing the service. This is particularly the case in which cloud storage services contract with third party service providers to help them conduct their business and work on their behalf to process payments, manage databases or provide technical support, for instance. Most apps (n = 13/15) will share users' data to comply with law and legal requests, such as court orders and search warrants. Several apps (n=5) share data with third parties marketing and advertising companies to assist them in analyzing the market and manage advertising. Sharing for protecting the rights, property, or safety of cloud provider, third parties or members of the public were addressed in 8 privacy policies. The same number was found in the case where cloud storage provider will be involved in a sale of its assets, merger or acquisition, since user data might need to be transferred as part of this decision. Finally, means for sharing to prevent fraud, stop illegal activities and misconduct were declared in 6 privacy policies.

Several controls and rights were given to users. A large proportion of privacy policies (n=10) provided the user with the option to opt out from receiving marketing communications. The majority of privacy policies (n=13) informed the user that he can disable or refuse cookies by adjusting browser settings. They also notify the user that in this case some features will be limited or not function properly. Almost three-quarters of apps (n = 11/15) give the user the ability to edit and/or delete his personal data. Moreover, approximately half of the apps (n=7) provide the user with the right to request a copy or ask to view his personal information that is held by the cloud service provider. A third of assessed privacy policies (n = 5/15) stated that they will notify the user if they are involved in a sale of their assets, merger or acquisition. Twelve apps declared that they will let the user know of their privacy policies change either by email or by a notice on their website that could be reflected by the last update date. Only one app stated that a notification email will be sent to the user if a breach occurred in which users' files become readable.

The findings also indicate that 6 of the assessed privacy policies do not focus on the information retention period. Unfortunately, even some of the 9 privacy policies which addressed the information retention period just addressed it partially. For example, it was unclear in some privacy policies how many days user personal information as well as usage data and sever logs will be retained after deleting the account. What will happen to the encrypted files after account cancelation was also ambiguous.

V. DISCUSSION

The developments in analytics methods as well as the huge increase in computing power and the capacity of data storage have expanded the scope of information available for companies. Furthermore, the growing number of devices that are now connected by networks has transformed the way data is collected, shared and accessed. Therefore, to create a balance between individual privacy and beneficial uses of data, policymakers should pay attention to some of major concepts of privacy law, which include the definition of “personally identifiable information,” and the principles of purpose limitation [24].

It was noticed that definitions were missing for some terms used throughout the privacy policy which makes it difficult to understand what the term used actually means. In many of the assessed privacy policies, there were no clear distinctions between third parties, subcontractors, business partners, service providers, affiliates and other terms that are used to specify with whom the information will be shared. For example, third parties are covered by the same privacy policy of the cloud service provider in some cases, while in others third parties have their own, different privacy policies that the cloud service provider has no control over it. A related problem was faced by Gomez et al. [16] as they examined the privacy policies of 50 websites. They reported that most of the assessed privacy policies stated or indicated that they share data with affiliates, but they did not identify who these affiliates are. The authors also described that the consumer might assume an affiliate or tracker to be a third party as well.

The purposes for collection and contexts of information sharing were clearly specified by most privacy policies. However, there were some differences between assessed privacy policies regarding detailing the context in which information will be shared or why it is collected. Some used the phrase "including but not limited to" which means that the cases listed for sharing are not complete and that there could be other cases in which the cloud storage provider will disclose the collected information. This has previously been observed by Pollach [25]. He analyzed the content and the language used by 50 online privacy policies. The linguistic analysis revealed that some companies use vague language such as "perhaps, in/at our discretion, on a limited basis, including but not limited to". He suggested representing usages of data in a more accurate way.

Another key related issue in information sharing is the degree to which user information will be shared with third parties for marketing purposes [26]. Only a third of cloud storage services explicitly stated that they shared user information with third parties to manage marketing and advertising. They differed in the type of information shared. For some, only the non-identifiable information will be disclosed. Others share personal information with third parties or let the third party companies collect personal information about customers' visits on their behalf in order to tailor advertisements to them.

The information collection and sharing can be done through different ways and using several mechanisms. Reinforcing user control in these activities is essential to maintain user's privacy. It is apparent from Table 2 that a number of controls and rights were given to cloud storage users. What is interesting is that only one cloud storage provider will notify users if a breach occurred. According to Anton et al. [20], there are a number of data breach notification laws which require businesses to notify their customers if the breach involves their personal data. Yet, breach notification laws are only in force in some states. In fact, it is not surprising that only one cloud storage service declared that it will notify customers if their encrypted content became readable to third parties. Understanding the impact of such notification on business's reputation could be the reason that prevents other cloud storage services from doing so, although hiding such event has a great impact on user's privacy.

Existing research pointed out the importance of deleting all kinds of data when they are no longer of value. In the past, companies often destroy some kinds of data after a specified periods of time. This is mainly due to the little benefit seen in keeping such data, besides the physical cost of retention. Nowadays, it has been observed that big data is able to bring economic or social value to companies. In addition, the cost of retention is decreasing exponentially particularly in the era of the cloud. Hence, there might be a tendency to keep data for longer period of time with obvious privacy implications [2]. Detailing how long each type of information (personal information, usage data and encrypted files) will be kept is a key aspect. Specifying the exact number of days as well as clearly describing all contexts in which data will remain or be deleted plays an important role in addressing users' privacy concerns after deleting their accounts.

Finally, although this work does not aim to study or further discuss usability and readability issues in privacy policies, it might be of interest to draw the attention to some noticeable issues in the assessed privacy policies in this regard. For example, the last update of a few privacy policies was written in numbers only, 7/3/2015, for instance. The interpretation of such date will differ from country to country. The date may follow the form dd/mm/yyyy or mm/dd/yyyy. In this example, it is hardly to know which is the day and month. Another noticeable issue was the large number of words in some privacy policies and the low level of coherence, which adds to the difficulty of reading and understanding the privacy policy for a normal user.

VI. CONCLUSION

Fifteen privacy policies were reviewed and analyzed based on specific criteria. The results showed the strengths and weaknesses of these privacy policies. Overall, most privacy policies addressed fundamental areas of information collection, purposes, sharing and users' controls. However, many policies lacked detailed information of data retention period. The discussion suggested providing clear definitions for terms used throughout the privacy policy and avoids vague language. Some usability and readability issues found in assessed privacy policies were also highlighted.

This privacy policy review is the first step to get a comprehensive understanding of zero knowledge cloud storage services' privacy practices. The results from this assessment provide the initial body of data for this research. Later, the policy claims can then be compared to the actual implementation to investigate to what extent zero knowledge cloud storage services adhere to what they state in their privacy policies. This contributes to the knowledge by shedding some light on points of conflicts, which will help cloud storage services to align functionality with their commitments more efficiently.

REFERENCES

[1] S. Trepte and L. Reinecke, eds. "Privacy online: Perspectives on privacy and self-disclosure in the social web", Springer Science & Business Media, 2011.

[2] President's Council of Advisors on Science and Technology, "Big data and privacy: A technological perspective", Washington, DC: Executive Office of the President, 2014.

[3] S.D. Warren and L.D. Brandeis, "The right to privacy", Harvard law review, pp.193-220, 1890.

[4] I. Altman, "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding", 1975.

[5] B. Arief, K. Coopamootoo, M. Emms and A. van Moorsel, "Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse", In Proceedings of the 13th Workshop on Privacy in the Electronic Society, ACM, pp. 201–204, 2014.

[6] D.J. Solove, "Understanding privacy", 2008.

[7] J. Tsai, S. Egelman, L. Cranor and A. Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", Information Systems Research, vol. 22, no. 2, pp. 254-268, 2011.

[8] P. Kumaraguru and L.F. Cranor, "Privacy indexes: a survey of Westin's studies", 2005.Vaandrager (Eds.). Lecture Notes in Computer Science, Vol. 1494. Springer-Verlag, London, 368–394. DOI: http://dx.doi.org/10.1007/3-540-65193-429

[9] M.S. Ackerman, L.F. Cranor and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences", In Proceedings of the 1st ACM conference on Electronic commerce, ACM, pp. 1-8, 1999.

[10] M. Paul, C. Collberg and D. Bambauer, "A Possible Solution for Privacy Preserving Cloud Data Storage," IEEE International Conference on Cloud Engineering, pp. 397-403, 2015.

[11] J. Reno, "Big Data, Little Privacy", CA Technology Exchange, p.24, 2012.

[12] G. Karjoth and M. Schunter, "A privacy policy model for enterprises." In Computer Security Foundations Workshop, Proceedings. 15th IEEE, pp. 271-281. IEEE, 2002.

[13] F. Schaub, R. Balebako and L. Cranor, "Designing Effective Privacy Notices and Controls", IEEE Internet Computing, vol. 21, no. 3, pp. 70-77, 2017.

[14] M. Rowan and J. Dehlinger, "Encouraging privacy by design concepts with privacy policy auto-generation in eclipse (PAGE)", In Proceedings of the 2014 Workshop on Eclipse Technology eXchange, ACM, pp. 9–14, 2014.

[15] J. Earp, A. Anton, L. Aiman-Smith and W. Stufflebeam, "Examining Internet Privacy Policies Within the Context of User Privacy Values", IEEE Transactions on Engineering Management, vol. 52, no. 2, pp. 227-237, 2005.

[16] J. Gomez, T. Pinnickand and A. Soltani, "KnowPrivacy". School of Information, 2009.

[17] R. Singh, M. Sumeeth and J. Miller, "Evaluating the Readability of Privacy Policies in Mobile Environments", International Journal of Mobile Human Computer Interaction, vol. 3, no. 1, pp. 55-78, 2011.

[18] A. Sunyaev, T. Dehling, P. Taylor and K. Mandl, "Availability and quality of mobile health app privacy policies", Journal of the American Medical Informatics Association, 2014.

[19] K. Huckvale, J. Prieto, M. Tilney, P. Benghozi and J. Car, "Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment", BMC Medicine, vol. 13, no. 1, 2015.

[20] A. Anton, J. Earp and J. Young, "How internet users' privacy concerns have evolved since 2002", IEEE Security & Privacy Magazine, vol. 8, no. 1, pp. 21-27, 2010.

[21] B. Miller, K. Buck and J.D. Tygar, "Systematic analysis and evaluation of web privacy policies and implementations". In Internet Technology and Secured Transactions, IEEE, pp. 534-540, 2012.

[22] S. Winkler and S. Zeadally, "Privacy Policy Analysis of Popular Web Platforms", IEEE Technology and Society Magazine, vol. 35, no. 2, pp. 75-85, 2016.

[23] W3schools, (2016). "HTML5 Web Storage". [online] Available at: http://www.w3schools.com/html/html5_webstorage.asp

[24] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics", Northwestern Journal of Technology and Intellectual Property, vol. 11, no. 5, 2013

[25] I. Pollach, "What's wrong with online privacy policies?", Communications of the ACM, vol. 50, no. 9, pp. 103-108, 2007.

[26] A. Miyazaki and A. Fernandez, "Internet privacy and security: An Examination of Online Retailer Disclosures", Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 54-61, 2000.