2015

Overcoming Privacy Challenges In Mobile-Cloud Computing

Jordan Shropshire
University of South Alabama, jshropshire@southalabama.edu

Matt Campbell
University of South Alabama, mattcampbell@southalabama.edu

Bob Sweeney
University of South Alabama, bsweeney@southalabama.edu

OVERCOMING PRIVACY CHALLENGES IN MOBILE-CLOUD COMPUTING

Dr. Jordan Shropshire, Ph.D.
Associate Professor of CIS
School of Computing
University of South Alabama
Mobile, AL, USA
jshropshire@southalabama.edu

Dr. Matt Campbell, Ph.D.
Assistant Professor of CIS
School of Computing
University of South Alabama
Mobile, AL, USA
mattcampbell@southalabama.edu

Dr. Bob Sweeney, Ph.D.
Associate Professor of CIS
School of Computing
University of South Alabama
Mobile, AL, USA
bsweeney@southalabama.edu

ABSTRACT

The integration of mobile devices with cloud computing systems results in a platform which is well-suited for the aggregation of customer behavior. Many organizations are capitalizing on this opportunity to harvest user data. They offer free software, content, and services in order to observe customer behavior. However, users have grown wary of increasingly comprehensive and granular profiling. The public's rejection of certain applications show there is growing resistance to this business practice. The present study overcomes these concerns by proposing four alternative privacy models. The viability of these privacy models is assessed using a broad public survey. The results suggest that organizations can alleviate consumers' privacy concerns by incorporating elements of the proposed alternative privacy models into their businesses.

Keywords

mobile-cloud, privacy, big data, business model

INTRODUCTION

The development trajectories of cloud and mobile technologies have converged to create a unified environment called cloud-mobile computing. This platform overcomes previous technical limitations and delivers advanced computational resources to mobile users. Mobile-cloud applications reduce processing, memory, and storage requirements for mobile devices (Fernando et al. 2013). The computational work is offloaded to clouds to conserve battery, minimize processing load, and reduce storage requirements (Dinh et al. 2013). Unconstrained by previous limitations, application developers are able to design software with enhanced user interfaces and richer content. These benefits are achieved by leveraging the physical presence of the mobile device, the increased bandwidth of wireless networks, and elastic backend computing capabilities (Bahl et al. 2012). Many cloud-mobile applications, services, and media are offered to consumers at no cost. Organizations develop and release cloud-mobile offerings because they provide an opportunity to observe and record user behavior (Bughin et al. 2010). Because the framework offers an onboard observation point and centralized storage of user content, data can be collected on a micro level of granularity. This information is quite valuable. It can be used to guide future product/service development, improve business practices, and provide tailored advertising (Chen et al. 2012).

Despite their zeal for new mobile-cloud offerings, users are beginning to vocalize their privacy concerns (Huang et al. 2011). In some cases, public outcry has forced companies to withdraw certain applications. For instance, Facebook recently modified its messenger application because a significant portion of the user base refused to grant it unconstrained system access (Goel 2014). Consumer privacy concerns appear to have grown in response to a number of events in recent years. Reports of collusion between internet companies and government agencies are driving consumers to question their privacy rights (Robison 2009). Further, the concept of big data has been negatively portrayed in recent news stories. Glimpses into the data brokerage industry have made consumers recoil (Ramirez et al. 2014). As a result, big data now has unpopular connotations among many user groups. Finally, a succession of massive data breaches has fanned customer fears regarding the

security of their personal information. Collectively, these factors are making users wary of data collection practices in the mobile-cloud environment.

If unchecked, consumer privacy concerns could have negative implications. For instance, they could lead to calls for increased government regulations. Some countries are already implementing tougher privacy laws. For instance, the European Union has adopted a complex series of data protection regulations which govern many aspects of individuals' personal information (Pearson 2009). An unfortunate byproduct of complex regulatory measures is that they increase the difficulty in starting technology business ventures. Escalating privacy fears have potential downside for both organizations and individuals.

This study holds that mobile-cloud developers and providers can avoid consumer backlash by incorporating alternative privacy models into their strategies. It further predicts that a growing user demographic will place a premium on privacy and will gravitate to companies which accommodate this value. This article proposes four strategies for overcoming users' privacy concerns while generating sustainable revenue streams. These alternative models could lead to revenue growth by capturing a previously-untapped user segment and enjoy positive public image by appearing to be sensitive to growing privacy concerns.

A broad national survey of US consumers was undertaken to assess consumer privacy concerns and gauge the viability of the proposed alternative privacy models. The results indicate that there is growing concern for personal privacy.

CONTEMPORARY BUSINESS PRACTICES

Within the mobile-cloud computing space, there are two dominant business practices: Businesses that sell software or services to consumers or other organizations and businesses which grant software or service usage in order to collect user information. These are depicted in Figure 1, below. The first business practice is rooted in the traditional approach to enterprise revenue generation in that it is based on the sales of products or services to clients. The product or service being marketed could be a mobile app, mobile cloud computing in the form of Backend-as-a-Service (BaaS), or a complete solution which is acquired on a contractual basis. The second business practice is unique in that it does not seek revenues from users but from the sales of user data. This approach is akin to the advertising networks which offer free content in order to sell advertising. It represents a small but growing segment of mobile-cloud business ventures.

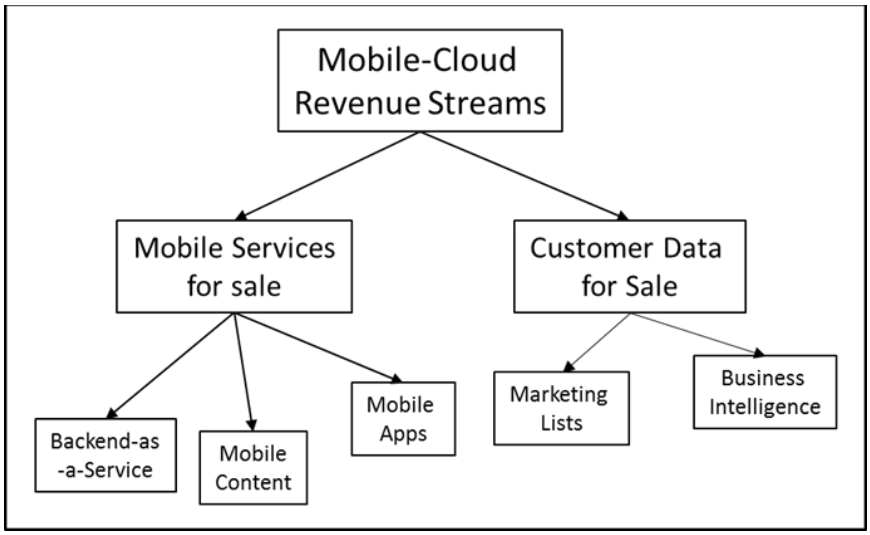


Figure 1. Taxonomy of Mobile-Cloud Business Practices

Because the mobile-cloud computing space is occupied by a variety of organizations with different goals, a variety of data types are collected. From the mobile device, collected data could include inbound and outbound phone calls, SMS messages, photos, video, application events, calendar entries, contacts, location points, unique cell towers, sensor data, Bluetooth activity, unique Bluetooth devices, WIFI activity, and audio samples [33]. This data is transmitted to a cloud where it is stored for later analysis. From within the cloud, backend application processing would result in user data such as search logs, customer transaction records, customer generated content, and network content [5]. The data can be used for recommender systems, social media analysis, crowd-sourcing, social and virtual games, customer discovery, human health applications, proximity-based maps, and incident monitoring.

ALTERNATIVE PRIVACY MODELS

In response to growing user privacy concerns, this research proposes four privacy models: pay-for-usage, fee-for-deletion, specified-collection and specified-usage (see Table 1). These models were conceived as revenue-generating alternatives for

users who are sensitive to corporate data collection practices. The first privacy model, pay-for-usage, allows user to opt out of data collection in exchange for payments approximately equal to the loss of the data sales opportunity. Although some organizations statutorily allow users to opt-out of data collection, the process is notoriously difficult. This is because organizations have a financial incentive to prevent users from opting out. To create a win-win situation for both individuals and organizations, it is proposed firms develop the capability to allow opt-outs on a subscription basis. Those concerned for their own privacy would be able to use a mobile-cloud service or software while being excluded from data collections. Companies would be able to calculate the value of their data aggregations and adjust prices as necessary.

The second privacy model, fee-for-deletion, gives privacy conscious users the opportunity to have all of their personal information deleted from company holdings. In contrast with the pay-for-usage option, this privacy model requires a one-time fee. If a concerned individual wishes to have his or her records purged again at a later date, another fee would need to be remitted. This solution is relatively simple to implement and provides a clear outcome to users. The third privacy model, specified-collection, would allow users to pick and choose which pieces of personal information (e.g. name, physical location, contact information, web browsing history, recent purchases, social media contacts, phone contacts, SMS & call log, and pictures, video, or music) they are willing to share and at what times they are willing to share them. App creators would assign a unique value to each piece of personal data or to specific data-time combinations that would reflect the value of that specific data to the app creator. The value of the data that the user agrees to supply could then be used to offset the retail price of the software. The more data the user is willing to supply, the less the user would pay for the software. The fourth privacy model, specified-usage, allows users to decide in what form they are willing to let their information be used: individual or aggregate. Being able to collect user-specific data on a specific individual over time is very valuable to the app creator. Alternatively, users who allow the app creator to utilize their data only in aggregate provide relatively low value to the app creator. The more individualized the data that the user is willing to let the app creator maintain, the less the user would pay for the software.

We anticipate that both the specified-collection and specified-usage models would require that users generate a minimum number of data points or observations. This stipulation would remedy a shortcoming of the current data-collection supported freeware model; the installation of apps on devices that generate little to no usable user data. This situation can occur when an app is installed on a device that does not have regular internet access, an enabled GPS, or cell phone service.

Type	Description	Revenue Type	Privacy Obtained	Billing Frequency
Pay-for-Usage	Excludes users from data collection during subscription period	Subscription expense	Nothing recorded during subscription period	Recurring
Fee-for-deletion	Deletes all data associated with a user profile	Deletion Fee	Everything up to the present is deleted	Single Instance
Specified-Collection	Allows users to specify which data elements will be collected and when	Mixed	Only approved data elements are collected	Recurring
Specified-Usage	Allows users to specify in what format their data will be used (individual or aggregate)	Mixed	Personal data can only be used as specified	Recurring

TABLE 1: ALTERNATIVE PRIVACY MODELS

RESEARCH METHODS

The purpose of this section is to evaluate mobile-cloud users' privacy concerns and gauge their interest in the proposed privacy models. A U.S. national survey was recently conducted. This section describes the survey sample, questions, and procedure.

Sample

To provide a representative sampling of mobile-cloud users, a nation-wide survey is currently underway. The sample is restricted to users in the United States because regulations and individual perceptions may differ between countries. For this study, participants are recruited online through a major web portal. Those included in the study must be US residents, at least 18 years of age, own a mobile device, and have used at least one mobile-cloud application or service. In total, 103 respondents have completed the survey. These persons form an inclusive sample of the United States: all major geographic regions are represented, ages ranged from 18 to 62, all genders are included, and multiple ethnicities are represented.

Questionnaire

Besides demographic questions, the questionnaire covers five topics: respondents' demographic information, understanding of mobile-cloud computing, mobile device usage habits, use of mobile-cloud applications or services, mobile-cloud privacy concerns, and interest in alternative privacy models. In total, the survey has 21 questions developed specifically for this study. The questions are a mix of multiple-choice, choose all that apply, and short answer.

Procedure

Subjects were recruited from a popular web portal and directed to a web-based survey hosted by Amazon Mechanical Turk. After answering some basic screening questions, subjects were given the opportunity to complete the survey. This survey used a combination of descriptions, illustrations, and mobile app logos to help subjects understand questions and recall certain details regarding their mobile computing habits. Those who completed the survey were awarded five dollars. This data was analyzed using the SPSS statistical package.

RESULTS

Some 103 respondents completed the survey. Their demographic information is depicted in Table 2 (below). As illustrated, survey participants were of all age generations and genders. Multiple ethnicities and U.S. geographic regions were represented. Table 3 (Below) depicts respondents' economic status. This information is important because it portrays the sample's purchasing power. The amount of disposable income has implications on the ability to make non-essential purchases such as - additional privacy consideration. As shown, the majority of respondents could be categorized as lower or upper middle class. This group has assets and resources which ostensibly require more protection. Therefore, security would be more important. Further, the survey shows variation in employment status. Respondents are a mix of full and part-time workers, unemployed, retired, and currently in school. In sum, the sample provides a highly representative sample of the United States, giving additional weight to survey findings.

The survey includes several basic questions to gauge respondents' familiarity with mobile-cloud computing. Not surprisingly, roughly half of the sample had either never heard of mobile-cloud computing or weren't sure what it is. As depicted in Table 4, some 42 subjects had at least a basic grasp of mobile-clouds. This information is not surprising because the end user does not need to be aware of an app's computing architecture in order to use it. As presented in the following tables, many respondents were using mobile-cloud applications even though they weren't familiar with the concept. When familiarity with mobile-cloud was cross-referenced against respondent age, it was found that those in the Millennial and Gen X generations were most knowledgeable. To assess user adoption of mobile-cloud apps, subjects were presented with a list of mobile-cloud applications and asked if they had previously used. The results are rank-ordered in Table 5 (below). For context, subjects were asked to give the capacity in which these apps were used. It turned out that most used mobile-cloud apps solely for work (41%). Some 10% used these apps for personal use only, while 20% used their mobile-cloud apps for business and pleasure. This information is important because user privacy may be influenced by organizational policies such as limitations imposed within BYOD policies.

Next, subjects' privacy concerns were elicited. As shown in Table 6, more than half of the respondents were either worried (40%) or very worried (15%) about the privacy of information entered in their mobile phone. Those most worried were in the middle and upper income brackets, and had at least two years of post-secondary education. Some 35% further believed that mobile-cloud apps were spying on them. This question is important because it measure the extent to which respondents perceive any impropriety on the part of the organization. Thus, it could be an indication of a coming consumer backlash. This table also depicts subjects' sensitivity to specific types of data. It appeared that respondents were more concerned with their location, friends, social media activity, and purchase habits being recorded than other personal data such as name and contact information. Finally, Table 7 (below) depicts subjects' interest in the proposed privacy models.

Geographic Region		**Age Range**		**Gender**		**Ethnicity**	
Northeast	19	iGeneration	26	Male	49	African American	27
Mid-Atlantic	14	Millennial	33	Female	52	Hispanic or Latino	17
Southeast	12	Gen X	26	Other	0	Non-Hispanic White	57
Midwest	7	Boomer	15	Prefer not to say	1	Asian American	1
Southwest	14	Greatest Generation	3			Indian American	1
West Coast	21						
Northwest	16						

TABLE 2. DEMOGRAPHICS

Employment Status		Income Level	
Employed full-time	35	Less than $23,050	25
Employed part-time	31	$23,050 - $32,500	34
Stay-home parent	1	$32,500 - $60,000	25
Student	14	$60,000 - $150,000	18
job-seeking	15	Over $150,000	1
Unable to work	2		
Retired	5		

TABLE 3. SUBJECTS' ECONOMIC STATUS

Familiar with Mobile-Cloud?	
Never heard of it	31
Heard of it but don't know what it is	29
Vaguely familiar with it	21
Understand the concept	17
Have in-depth knowledge	5

TABLE 4. PLATFORM FAMILIARITY

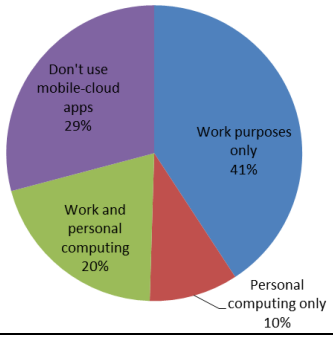
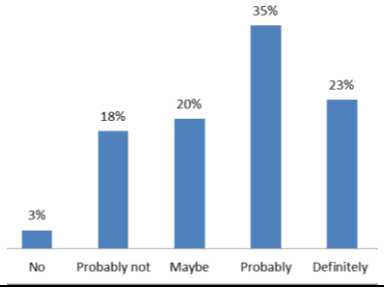
Top Mobile-Cloud Apps	Use of Mobile-Cloud Apps
1. iCloud 2. Google Drive 3. Facebook 4. SalesForce mobile 5. Google+ 6. iTunes Radio 7. eVoice 8. Netflix 9. Hopto 10. OfficeScope	

TABLE 5. MOBILE-CLOUD USAGE

Worried About Personal Privacy?	
No	17%
I'm a little concerned	28%
I'm worried	40%
I'm very worried	15%
I haven't considered it	1%

Do mobile-cloud apps spy on you?



Can this data be shared?	% no
Physical location	52%
Name	18%
Contact information	12%
Websites I visit	36%
Recent purchases	54%
Social media friends	52%
Contacts	59%
SMS messages & call log	33%
Pictures, video, or music	18%

TABLE 6. PRIVACY CONCERNS

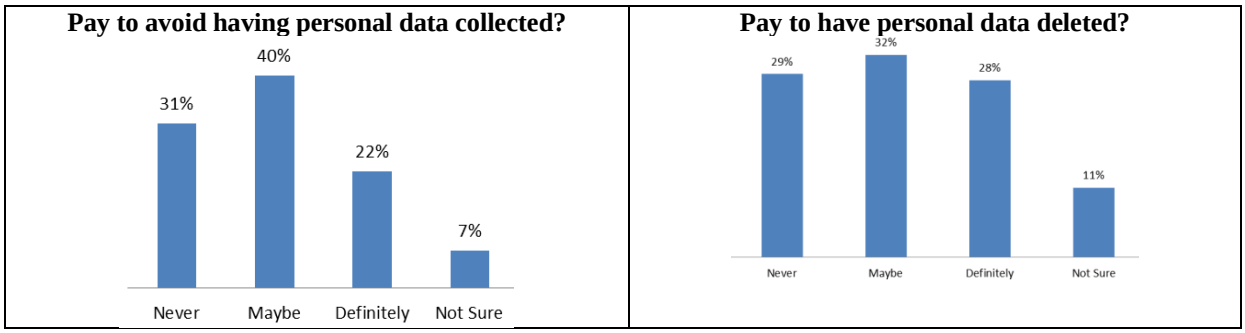


TABLE 7. PAYING FOR PRIVACY

In general, a significant portion of respondents would be willing to pay to limit data collections and/or have their personal information deleted from the database. When broken into age and income groups, a positive correlation was found between economic class and willingness to pay. This could be due to the availability of disposable income or the desire to protect more substantial assets. Further, older respondents were also more interested in paying for their privacy. Thus, it appears that despite in-depth familiarity with the mobile-cloud landscape, older Americans are more willing to pay for privacy.

CONCLUSIONS

The mobile and cloud spheres have converged to form an integrated environment for high performance computing. Mobile software, services, and content providers are rapidly developing strategies to profit off this new ecosystem. A common theme among these companies is the collection and analysis of user data. If properly mined, massive data aggregations provide lucrative revenue streams. Although this is a boon to businesses, it is interpreted as a privacy threat to a growing proportion of mobile users. This research advocates alternatives to contemporary mobile-cloud business practices. It proposes four alternative privacy models which offer increased user control while allowing organizations to maintain cash inflows. The results of our survey portray a public which is increasingly sensitive to corporate data collection practices. Forward-looking organizations should begin to incorporate alternative privacy models into their businesses.

REFERENCES

1. Bahl, P., Han, R., and Li, L. Year. "Advancing the state of mobile cloud computing," Proceedings of the third ACM workshop on Mobile cloud computing and services, Low Wood Bay, UK, 2012, pp. 21-28.
2. Bughin, J., Chui, M., and Manyika, J. 2010. "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch," *McKinsey Quarterly* (21:3), pp 2-14.
3. Chen, H., Chiang, R., and Storey, V. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), pp 1165-1188.
4. Dinh, H., Lee, C., Niyato, D., and Wang, P. 2013. "A survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," *Wiress Communications and Mobile Computing* (13:18), pp 1587-1611.
5. Fernando, N., Loke, S., and Rahayu, W. 2013. "Mobile cloud computing: A survey," *Future Generation Computer Systems* (29:1), pp 84-106.
6. Goel, V. 2014. "Facebook Requires Users to Install Separate Messaging App," April 15, 2014.
7. Huang, D., Zhou, Z., Xing, T., and Zhong, Y. Year. "Secure data processing framework for mobile cloud computing," 2011 IEEE Conference on Computer Communications Workshops, Shanghai, CN, 2011, pp. 614-618.
8. Pearson, S. Year. "Taking account of privacy when designing cloud computing services," Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, CA, 2009, pp. 44-52.
9. Ramirez, E., Brill, J., Ohlhausen, M., Wright, J., and McSweeny, T. 2014. "Data brokers: A call for transparency and Accountability," Federal Trade Commission.
10. Robison, W. 2009. "Free at what cost? Cloud computing privacy under the stored communications act," *Georgetown Law Journal* (98:4), pp 1195-1241.