https://doi.org/10.11144/Javeriana.iyu23-1.pplb

Privacy perception in location-based services for mobile devices in the university community of the north coast of Colombia[1]

Percepción de privacidad en servicios basados en localización para dispositivos móviles en la comunidad universitaria de la costa norte de Colombia[2]

Margarita Gamarra Acosta[3]

Inés Meriño Fuentes[4]

Juan Calabria Sarmiento[5]

Omar Gutierrez Acosta[6]

Mauricio Barrios Barrios[7]

Nallig Leal Narvaez[8]

Pedro Wightman Rojas[9]

How to cite this article:
M. Gamarra, I. Meriño, J. Calabria, O. Gutierrez, M. Barrios, N. Leal, P. Wightman "Privacy perception in location-based services for mobile devices in the university community of the north coast of Colombia" Ing. Univ. vol. 23, no. 1, 2019 [Online]. doi: 10.11144/Javeriana.iyu23-1.pplb

---

[1] Submitted on: August 6th, 2018. Accepted on: December 3rd, 2018.
[2] Fecha de recepción: 6 de agosto de 2018. Fecha de aceptación: 3 de diciembre de 2018.
[3] Electronic engineer, Master in electronic engineering, Universidad del Norte. PhD student, Universidad del Norte. Professor, Universidad Autónoma del Caribe. Barranquilla, Colombia. E-mail: margarita.gamarra@uautonoma.edu.co. http://orcid.org/ 0000-0003-1834-2984
[4] Systems Engineer, Universidad del Magdalena. Master of Systems and Computing Engineering, Universidad Simón Bolívar. PhD student, Universidad del Norte. Professor, Universidad del Magdalena. Santa Marta, Colombia. E-mail: imerino@unimagdalena.edu.co/uninorte.edu.co. https://orcid.org/0000-0002-6859-3303
[5] Systems engineer, Universidad Autónoma del Caribe. Master in systems engineering, Universidad del Norte. PhD student, Universidad del Norte. Professor, Universidad Simón Bolivar. Barranquilla, Colombia. E-mail: jcalabria@unisimonbolivar.edu.co/calabriaj@uninorte.edu.co. https://orcid.org/0000-0003-1004-5280
[6] Mechanical engineer, Universidad del Atlántico. Systems Engineer, Universidad Autónoma del Caribe. Master in government of computer technology, Universidad del Norte. PhD student, Universidad del Norte. Barranquilla, Colombia. E-mail: omargutierrez@uninorte.edu.co https://orcid.org/0000-0003-0439-8450
[7] Electronic engineer, Universidad Autónoma del Caribe. Biomedical engineering, Universidad Autónoma Metropolitana. PhD student, Universidad del Norte. Professor, Universidad Autónoma del Caribe. Barranquilla, Colombia. E-mail: mbarrios@uautonoma.edu.co. https://orcid.org/0000-0002-1933-8496
[8] Systems engineer, Master in engineering, Universidad de Antioquia. Associate Professor, Universidad Autónoma del Caribe. Barranquilla, Colombia. E-mail: nleal@uac.edu.co. https://orcid.org/0000-0002-4913-8540
[9] Systems engineer, Universidad del Norte. Master of Science in Computer Science, University of South Florida. Phd in Computer Science and Engineering, University of South Florida. Associate Professor, Universidad del Norte. Barranquilla, Colombia. E-mail: pwightman@uninorte.edu.co. https://orcid.org/0000-0002-7641-2090

Abstract

Introduction: The use of mobile applications has increased in the last years. Most of them require the knowledge of the user location, either for their core service or for marketing purposes. Location-based services (LBS) offer context-based assistance to users based on their location. Although these applications ask the user for permission to use their location and even explain in detail how this information will be used in its terms and conditions, most users are not aware or even interested in the fact that their location information is stored in databases and monetized by selling it to third-party companies. Regarding this situation, we developed a study with the aim to assess perception, concerns and awareness from users about their location information. *Methods:* This work is based on an exploratory survey applied to the university community, mainly from the North Coast of Colombia, to measure the perception of location privacy of users with mobile devices. The questionnaire was applied using Google Forms. The survey has nineteen questions organized in three sections: personal information, identification of privacy and privacy management. These questions were designed to know the users' perceptions of privacy concerns in LBS and any actions they take to preserve it. *Results:* The results show that, in general, the respondents do not have a real concern regarding the privacy of their geolocation data, and the majority is not willing to pay to protect their privacy. *Conclusions:* This type of surveys can generate awareness among participants about the use of their private information. The results expose in this paper can be used to create government policies and regulations by technology companies about the privacy management.

Keywords: Location privacy, Location-based services, Privacy perception.

Resumen

Introducción: El uso de aplicaciones móviles se ha incrementado en los últimos años. La mayoría de ellas requiere conocer la ubicación del usuario, ya sea para su servicio principal o para fines de marketing. Los servicios basados en localización (SBL) ofrecen asistencia contextual para los usuarios según su ubicación. Aunque estas aplicaciones le piden permiso al usuario para usar su ubicación e incluso explican en detalle cómo se usará esta información en sus términos y condiciones, la mayoría de los usuarios no están conscientes ni incluso interesados en el hecho de que la información de su ubicación se almacene en bases de datos y se monetice, vendiéndolo a terceros. Con respecto a esta situación, desarrollamos un estudio con el objetivo de evaluar la percepción, las preocupaciones y el conocimiento de los usuarios sobre la información de su ubicación. *Métodos:* este trabajo se basa en una encuesta exploratoria aplicada a la comunidad universitaria, principalmente de la costa norte de Colombia, para medir la percepción de la privacidad de ubicación de los usuarios con dispositivos móviles. El cuestionario se aplicó utilizando los formularios de Google. La encuesta tiene diecinueve preguntas organizadas en tres secciones: información personal, identificación de privacidad y gestión de la privacidad. Estas preguntas fueron diseñadas para conocer las percepciones de los usuarios sobre las preocupaciones de privacidad en SBL y cualquier acción que tomen para preservarla. *Resultados:* los resultados muestran que, en general, los encuestados no tienen una preocupación real con respecto a la privacidad de sus datos de geolocalización, y la mayoría no está dispuesta a pagar para proteger su privacidad. *Conclusiones:* este tipo de encuestas puede generar conciencia entre los participantes sobre el uso de su información privada. Los resultados expuestos en este documento se pueden utilizar para crear políticas y regulaciones gubernamentales por parte de las compañías de tecnología sobre la administración de la privacidad.

Palabras clave: Privacidad en la localización, Servicios basados en localización, Percepción de privacidad.

1. Introduction

Mobile technologies have increased recently and along with them, the flow of information. The access to knowledge and use of these data concerns many users. It has opened the debate about what kind of data should be public or private. In the study presented in [1], when Americans are asked what comes to mind when they hear the word "privacy," they give important weight to the idea that privacy applies to their "rights". According to this study, the item *details of physical location over time* is fifth out of sixteen on the level of sensitivity of personal information. Location-based information systems (LBISs) are defined as "applications that provide users with information based on their geographical position, which could be obtained from the mobile device they are accessing the service, or using a manually defined location" [2]. For LBSs to provide the requested information properly, sensitive data about the subject's location is required [3]. Location information privacy is an important topic in the context of expanding mobile technologies and applications.

The perception of privacy is a subjective concept that has changed with the advance in technology; for instance, from mail to e-mail or from telephones to cellphones. This variety of concepts hinders its measurement and the setting of privacy options in the mobile applications that use LBS, so it is more suitable to have a multidimensional concept of privacy. For example, in [4], the authors distinguish four dimensions of privacy and defining it as ''the ability to control and limit physical, interactional, psychological and informational access to the self or one's group''. Likewise, the work in [5] defines privacy "as the claim of individuals, groups or institutions to determine for themselves when, how, and what information about them is communicated to others", while in [6], "the privacy involves the policies, procedures, and other controls that determine which personal information is collected, how it is used, with whom it is shared, and how individuals who are the subject of that information are informed and involved in this process".

The concept of privacy and its implications is of vital importance, and for this reason, the UN Human Rights Council defends the right to privacy in the digital age and recognizes the global and open nature of the Internet and the rapid advancement in information and communication technologies as a driving force in accelerating progress towards development in its various forms. It also affirms that the same rights that people have offline must also be protected online, including the right to privacy [7]. In addition to these definitions, location awareness involves privacy issues that differ from others. For example, when users download some mobile applications, they are not aware that they are also giving the application permission for this information (usually because the majority of user do not read the terms and conditions). On the other hand, users are concerned with whether their location is stored and whether this information is sold to third parties, but they are willing to sacrifice their information in order to have access to the service.

In a previous study, privacy has been evaluated in different contexts: management of data in the Internet [8], email, phone conversations and clinical history. However, to the best of the knowledge of the authors, there has not been a previous study that measures privacy perception in location-based services in Colombia. This work tries to cover two dimensions for privacy in LBS: privacy awareness and privacy management. The results analyzed from the survey offer a general view on the areas of privacy in location, and useful insights to understand the user preferences. The main percentage of the surveyed population is the university communities in the North Caribbean region, with a small number of participants from other communities.

2. Related Work

New modes of communication have created many concerns about user security and privacy: identity, location, routine, and opinions are mostly public information via social networks. The question of "who knows this information" has arisen within mobile technologies. This is a real concern because there are reported cases where a government used LBIS to determine political views of individuals based on the presence of keywords or expressions against official positions, turning these people into targets of exhaustive tracking. However, this is not the only risk. In [9], the authors also include other risks:

- Being tracked by an operator to determine where a particular user's phone is located.
- Listing all devices that are deployed in a certain area at a certain time.
- Wi-Fi and Bluetooth tracking through the MAC address of the mobile device, even if this is not actively connected to a network.
- Illegal malware installed on mobile devices that track the user's location and their conversations.

The above risks have also been analyzed in a study by [10] at MIT, where it was demonstrated that in a dataset of 1.5 million people where the location of an individual is specified hourly and with a spatial resolution equal to that given by the carrier's antennas, only four space-temporal points are required to uniquely identify 95% of the individuals.

Privacy in other context has been analyzed by many other studies. For example, the work done by [11] proposes a categorization of factors that should be included when examining Internet user's privacy perception. The results of the performed analyses indicate that respondents who were more concerned about information collected during their online activity were also more concerned about their online privacy. In addition, respondents with a higher level of dissatisfaction with the current privacy protection reported a higher level of online privacy concerns.

Furthermore, other recent studies show that users are becoming more aware of the security risks associated with their location, finding that 19% of cellphone owners have turned off the location tracking feature on their devices because they were concerned that other individuals or companies could access that information [12].

Regarding location privacy, some techniques based on obfuscation have been developed. In [3], the authors present a compendium of techniques to protect the location privacy of the users. In [13], the authors propose an approach based on entity resolution which enables users to disclose their mobility information without compromising their privacy, even the data are linked with external publicly available information (social networks). In this field of study, there are other proposed methods to conceal the location of a user [14] [15] [16] [17].

There are few existing studies regarding privacy perception surveys. in [18], results show that users have a variety of motivations for participating in location-based surveys and that these motivations depend on the type of the survey in question. This study concluded that users concerned with privacy are less likely to be motivated by a monetary benefit but by the importance of the topic and that the intrinsic motivators that drive the users concerned with privacy differ from those that drive unconcerned users.

In 2011, the National Institute of Information Technologies (INTECO) of Spain developed a series of investigations supporting privacy with mobile devices [19]. The purpose of the study was to "perform a diagnostic of the use that the evolutionary netizens made in the mobile devices and smartphones, as well as the safety measures used and the impact suffered". Other study based on perception was developed by the University of Madeira, using the basis of location from social networks. It stated "that location is an idiosyncratic property of people's social networking profiles, and sharing it does not conform to existing social network practices and norms, particularly when the sharing is done in real-time and through mobile devices that the user permanently carries around" [20].

In Colombia, the Groupe Speciale Mobile Association (GSMA) published the "Study of GSMA on attitudes related to the privacy of the mobile users" [21], The aim was to understand the privacy concerns that users of mobile device have and to help the development of public policies. Although data management involves the concept of privacy, there are not many studies about this topic, especially regarding LBS. This work is a first step to evaluate privacy perception in LBS in Colombia, as mentioned in the introduction.

3. Methodology

This study is based on an exploratory survey to measure the perception of location privacy of users with mobile devices. The questionnaire was applied using Google Forms, an application that is a part of the Google Drive suite, in which basic surveys can be designed and distributed electronically. We, with the help of external experts, used consensus techniques [22] and indications to generate and select the questions as it is suggested in [23].

Finally, the form of the survey instrument was designed to identify the perceptions of privacy concerns in LBS.

The link to the form was distributed by the academic programs in participating universities to all the enrolled students and faculty. In addition, other mechanisms, such as social networks and email mailing lists were used in order to increase the outreach of the survey. Once all the answers were received, a filtering process was performed in order to eliminate incomplete or corrupt information. Next, the final dataset was used for statistical analysis: the qualitative variables were used as categorical variables to perform multiple correspondence analysis (see the section 4.4) and several descriptive graphics were used to interpret the results

3.1. Materials

The survey has nineteen questions organized in three sections: personal information, identification of privacy and privacy management. These questions were designed to know the users' perceptions of privacy concerns in LBS and any actions they take to preserve it. The criteria used by the authors to generate the questions were determined by the following suggestions given by [23]:

- Questions should be clear, simple, short and motivating.
- To avoid ambiguities, the questions should include a single logical statement.
- The questions should be grouped by subject.

The responses for the multiple choice questions were selected by consensus with the purpose of trying to cover the most important possibilities and according to other similar studies such as [24], [25].

For the demographic and socioeconomic data categories, the following variables were included: age, gender, city of residence, level of study, economic sector and monthly income.

In the categories of privacy awareness about location, the questions were made to ascertain the level of knowledge that the users of mobile devices have about the privacy of their location. The following questions were asked:

1. *Do you know if you have applications on your mobile phone that have access to your geographical location? (Options: Yes/No)*
2. *How do you rate the fact that applications on your mobile can know and store your geographical location with or without your consent? (Options: scale 1-bad, 5-Good)*
3. *Which entities would you allow to have access to your geographical location? (Options, multiple responses: Relatives and friends, Advertising and marketing*

companies, Social networks, Coworkers, Financial Institutions or Insurers, Government, Telecommunications companies and None)

4. *Do you use on your mobile device applications that store your geographical location or that of your family? (Options: Yes/No)*
5. *Do you know if a relative or a friend has had an incident in security or privacy associated with the knowledge of the geographical location by third parties? (Options: Yes/No)*
6. *Do you agree with creating laws that protect the location of people? (Options: Yes/No)*
7. *Would you be willing to pay to protect access to your location? (Options: Yes/No)*
8. *What is the reason you share your location? (Options, multiple responses: Safety, Work. Business and Other)*

Finally, the last category presented questions to analyze the level of supervision and control of the users on the management of the privacy of their location. The questions asked are as follows:

1. *Which of the following situations do you consider an invasion of the privacy of your location? (Options, multiple responses: Selling my location data to third parties, Give my location to use an App, Sending advertising using my location and not being informed about using my location.)*
2. *How often would you prefer Apps to ask you about access to your location? (Options: Every time you use the application, only when you install the application and do not ask about permission to access your location.)*
3. *Which of the following cases do you think the location could be accessed without the user's permission? (Options, multiple responses: Know the location of your children, Know the location of your employees, In case of emergency, Sending advertising targeting your interests, Never and Other)*

3.2. Participants

The survey was sent to a total of 5800 people, of whom 670 responded, a response rate of 11.5%. Responses were analyzed, cleaned and standardized in terms of age and city origin, because these questions were open-ended.

The mean age of the sample was 23 years, and the range was 13-63. The majority of the respondents could be classified as young adults. The respondents were from Colombia, especially from the Colombian Caribbean Region. In addition, 50.1% of the population surveyed had a professional career, and 64.9% were students.

4. Results

In the survey, all the questions were the same and mandatory. However if the response to the question about occupation was "*work*", then the respondent was redirected to the section "*economic area*", which had 2 questions about salary and about specific area.

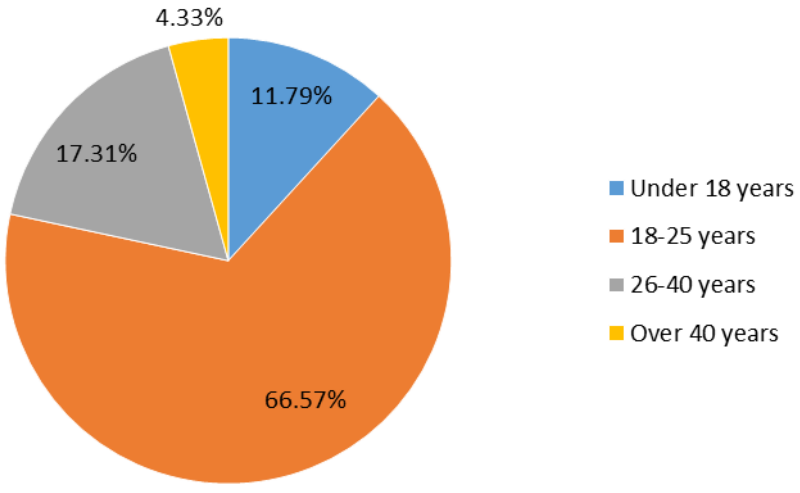
After the answers were submitted, a cleaning process was performed, removing unrelated and inappropriate responses. Then, each question was entered into the statistical analysis software IBM-SPSS. Closed responses and multiple choice questions were quantified by assigning a value for the label.

According to the kind of question (privacy awareness or privacy management), two different analyses were performed: a discriminant analysis for nominal variables, as in the case of privacy awareness [26], and for the section privacy management, a cross-tabulation analysis was performed for each variable.

4.1. Demographic and socioeconomic data

As mentioned in the Methodology section, the survey was conducted among 670 participants, of whom 59.6% were male and 40.4% female. Most participants were in the age range of 18 to 25 years old, 66.62%, followed by the age range of 26 to 40, 17.29%. These ages coincided with the answers given for the activities reported by the participants, as shown in Fig. 1 and Fig. 3.

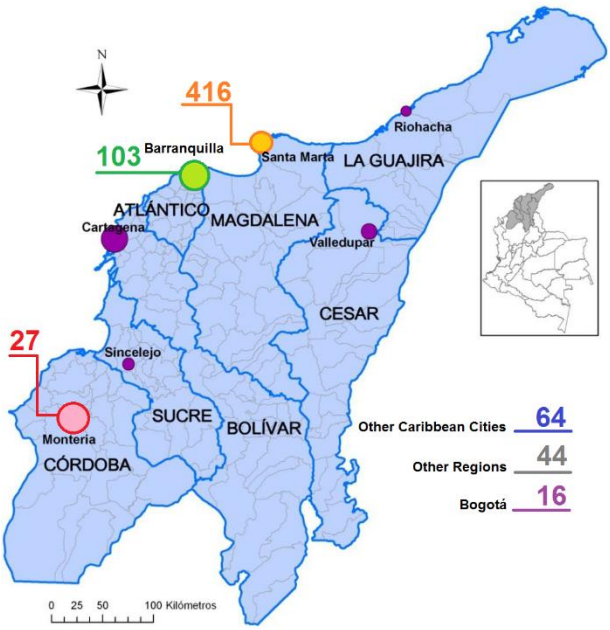
Fig. 1. Percentage of age of participants



Source: Authors' own creation

The main cities of residence of the participants were Santa Marta, Barranquilla and Monteria. The geographical distribution of the cities and the numbers of participants are shown in Fig. 2.

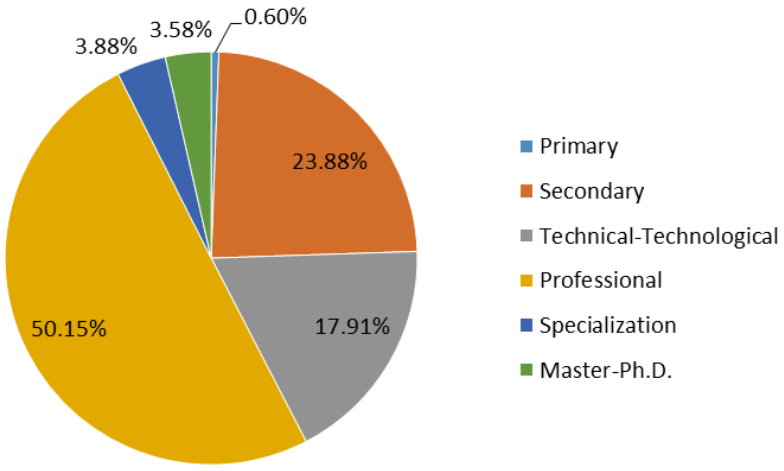
Fig. 2. Geographical distribution of the cities and amount of participants (based on [27])



Source: [27]

The level of education of the participants was mostly those who have obtained a professional degree, 50.15%; followed by secondary education, 23.88%; and third, those with technical and technological training, 17.91%, as shown in Fig. 3.

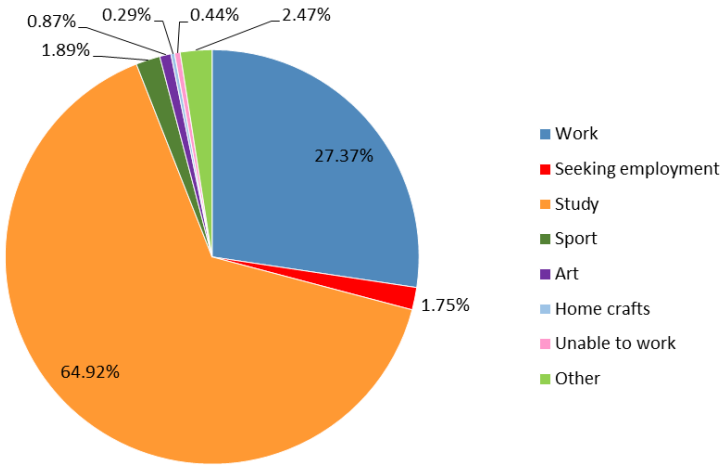
Fig. 3. Level of education of the participants



Source: Authors' own creation

With regards to the activities of the people who participated in this study, 64.92% are students, while 27.37% are either dependent or independent employees, as shown in Fig. 4.

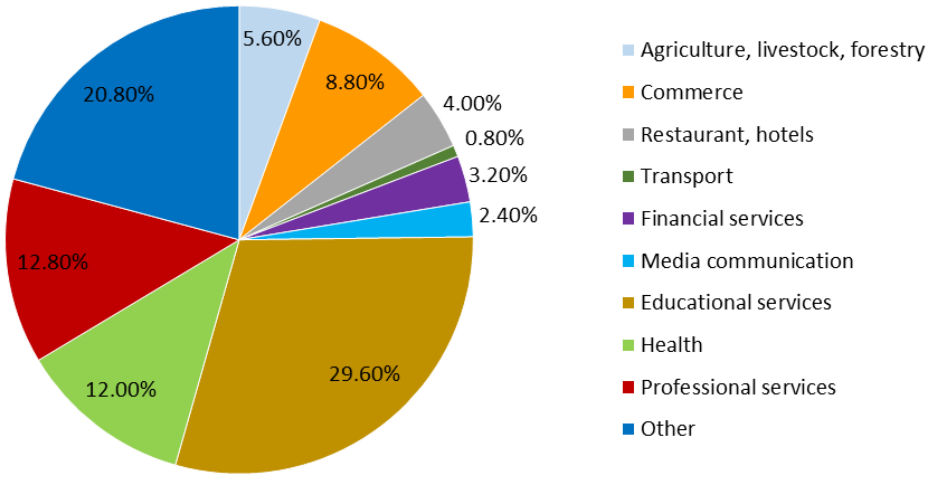
Fig. 4. Activities of the participants



Source: Authors' own creation

Of those who are working, the majority work in the education sector, 29.6%; professional services, 12.80%; and health, 12.00%, as shown in Fig. 5.

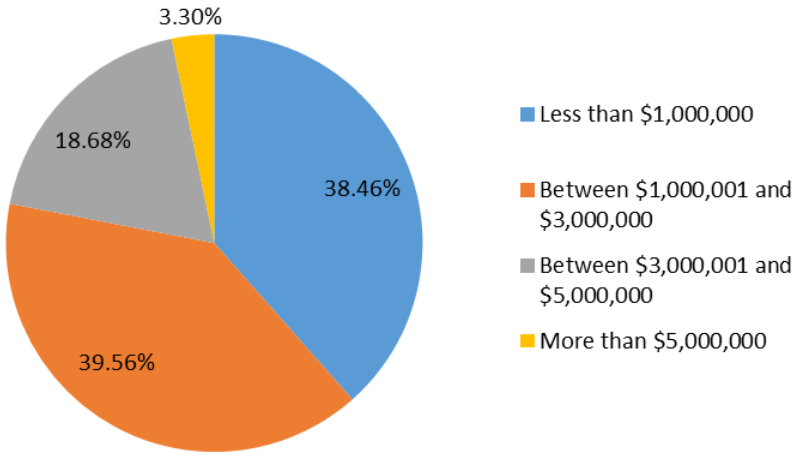
Fig. 5. Working sector of the participants



Source: Authors' own creation

The participants' monthly income is between COL$ 1,000,001 and COL$ 3,000,000 in 39.56% of the cases, and it is less than COL$ 1,000,000 in 38.46% of the cases, as shown in Fig. 6.

Fig. 6. Income of the working participants



Source: Authors' own creation

4.2. Respondents' privacy awareness

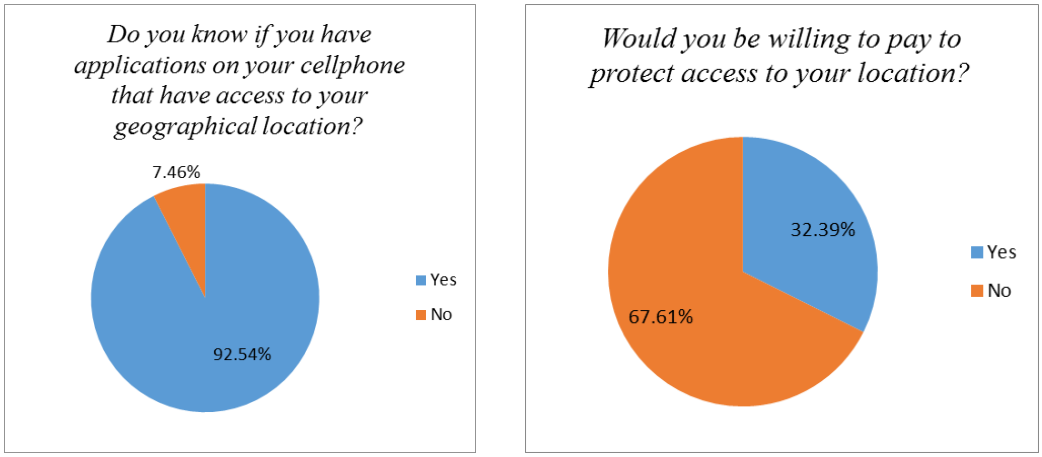
This section describes the percentage of respondents who know about apps that use their location. It considers the respondents reported age, gender, education level and occupation. Statistical tests are conducted to determine whether any differences observed are statistically significant.

4.2.1. Do you know if you have applications on your cellphone that have access to your geographical location?

The majority of respondents (92.54%) stated that they know about apps that have access to their geolocation (see Fig. 7.a.). This behavior was common in all cases (age, gender, education level and occupation). A first discriminant analysis showed that the relationship between this question and age, education level and occupation of respondent was not statistically significant. Nevertheless, gender has a p-value<0.05 in the test of equal means of groups. Then, a second analysis was performed, comparing the gender with the other variables.

In the case of gender and age range, it can be seen that the knowledge about location differed on the predictor variable gender. This result was obtained using ANOVA. A single discriminant function was calculated. The value of this function was significantly different for knowledge and nonknowledge (χ^2=8.740, df=2, p-value<0.05). The correlations between the predictor variables and the discriminant function suggested that gender was the best predictor for this question, since gender was positively correlated with discriminant function value. This means that gender can affect the answer to this question.

Fig. 7. Percentage of participants questioned about privacy awareness



a) b)

Source: Authors' own creation

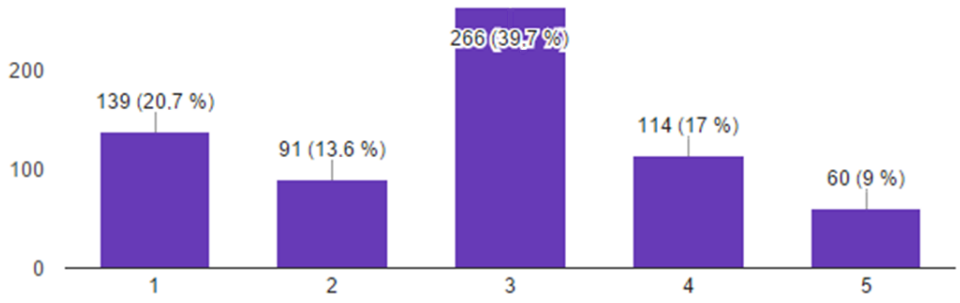
4.2.2. Would you be willing to pay to protect access to your location?

The majority of respondents (67.61%) stated that they would not pay to protect access to their location (see Fig. 7b.). This behavior was common in all cases (age, gender, education level and occupation). A discriminant analysis showed that the relationship between this question and gender, age, education level and occupation of respondents was not statistically significant.

4.2.3. Other questions related with privacy awareness

The respondents were also questioned about the entities that could have access to their location, and the majority (83.3%) agreed that family members could access the geolocation. Regarding the reason to share the location, 75.2% of respondents selected *to be in touch with relatives*, of which 49% selected *for safety*. In Fig. 8, the respondents rated the access to the location of the mobile applications, being 1-bad and 5-good.

Fig. 8. How do you rate the fact that your mobile applications can know and store your geographical location with or without your agreement?



Source: Authors' own creation

Taking into account these results, the main reasons for respondents to share their location is to keep in touch with relatives or safety reasons. Additionally, more than a third of them have an indifferent position regarding other entities having access to their location, and a third of the surveyed individuals consider that it tends to be bad.

4.2.4. Respondents privacy management

This section describes the percentage of respondents who would take action facing the privacy management. It considers the respondents' reported age, gender, education level and occupation. A cross-tabulation is created in order to analyze the relationship between the independent variables and the response options.

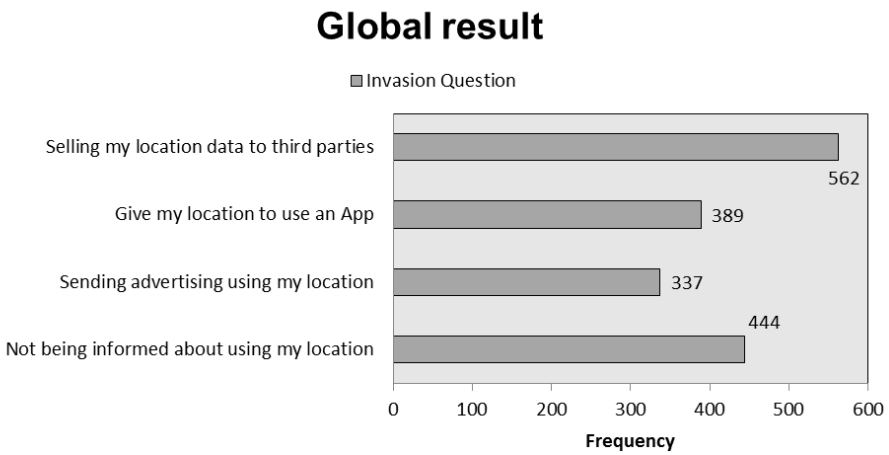
Respondents were split into four groups of their reported age (18 years or younger; 19–25 years; 26–40 years; 40 years or older), corresponding to levels 1, 2, 3 and 4, respectively. The gender was codified with 1 for female and 2 for male; the education level was codified 1-specialization, 2-master or Ph.D., 3-primary school, 4-professional, 5-high school, 6-technique; the occupation was codified 1- art, 2-looking for a job, 3-sport, 4-studing, 5-chores, 6-internship and 7-working.

4.2.5. Which of the following situations do you consider an invasion of the privacy of your location?

In this question, the respondents had four options for responses available: 1) Selling my location data to third parties, 2) Give my location to use an App, 3) Sending advertising using my location and 4) Not being informed about using my location.

In Fig. 9, it can be seen that the majority of respondents consider an invasion of the privacy in location *selling the location data to third parties* and a large percentage (66.3%) also consider *not being informed about using the location* an invasion.

Fig. 9. Which of the following situations do you consider an invasion of the privacy of your location?

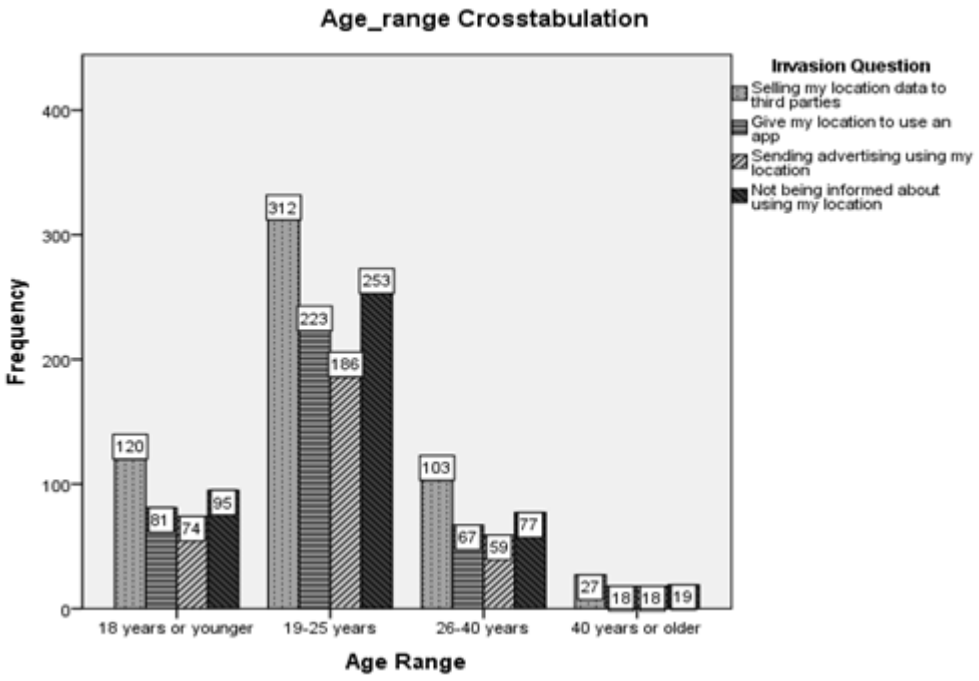


Source: Authors' own creation

A crosstabulation was performed for each independent variable (age, gender, education level and occupation). Fig. 10 shows the analysis between the age range and the four options of the question. Figures 11, 12 and 13 show the crosstabulation between the four options of the question and gender, education level and occupation, respectively.

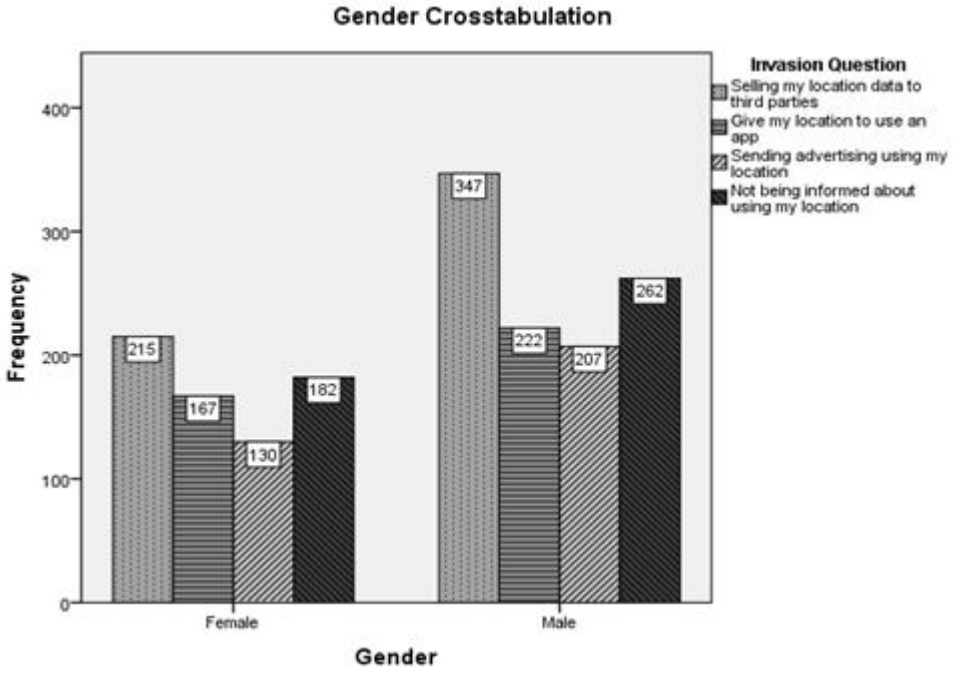
In this case, the majority of respondents in the group comprising 19-25 years, male gender, bachelors and students considered an invasion of the privacy in the categories of *selling the location data to third parties* and *not being informed about using the location*. This shows that not knowing what using the location information may be a concern for the user.

Fig. 10. Crosstabulation for age_range and invasion question



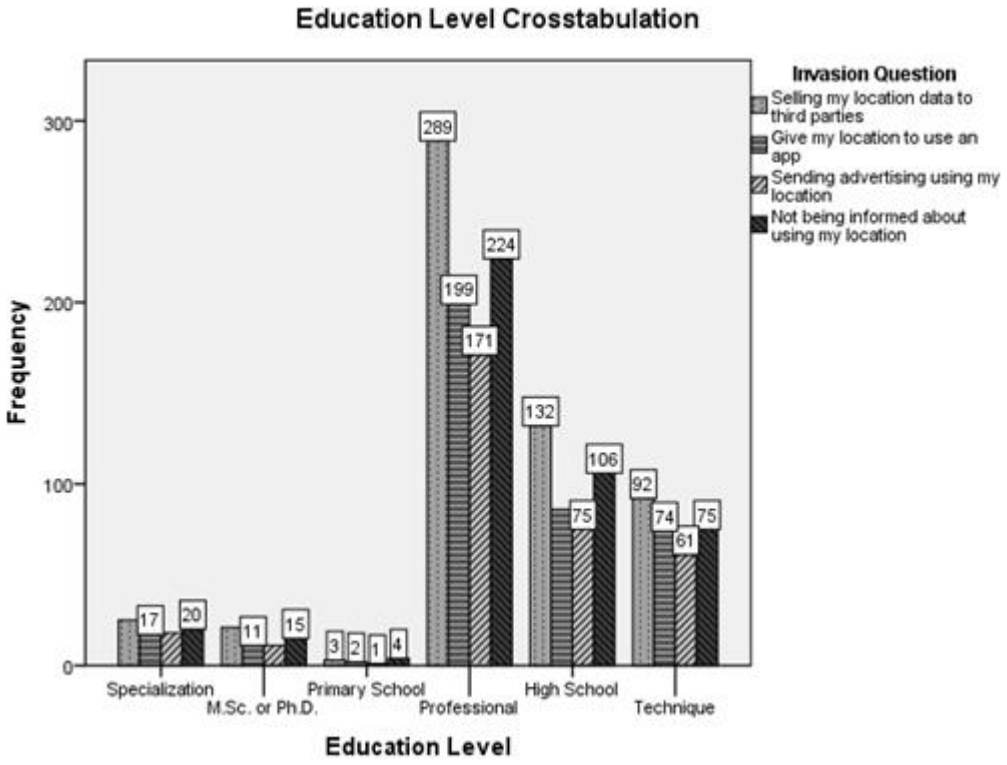
Source: Authors' own creation

Fig. 11. Crosstabulation for gender and invasion question



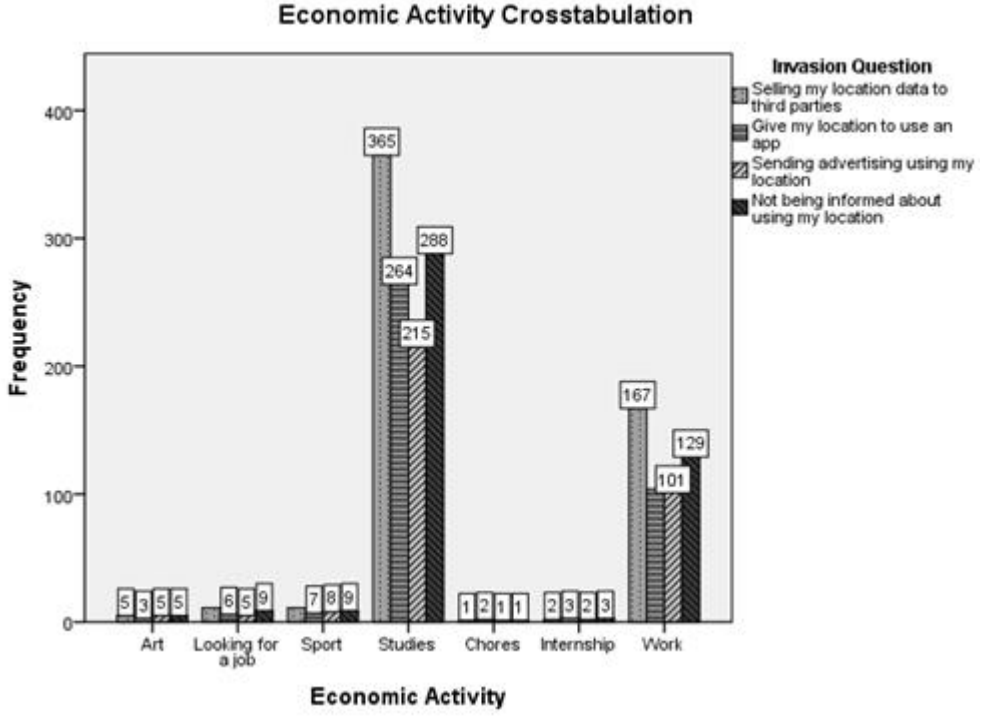
Source: Authors' own creation

Fig. 12. Crosstabulation for education level and invasion question



Source: Authors' own creation

Fig. 13. Crosstabulation for occupation and invasion question



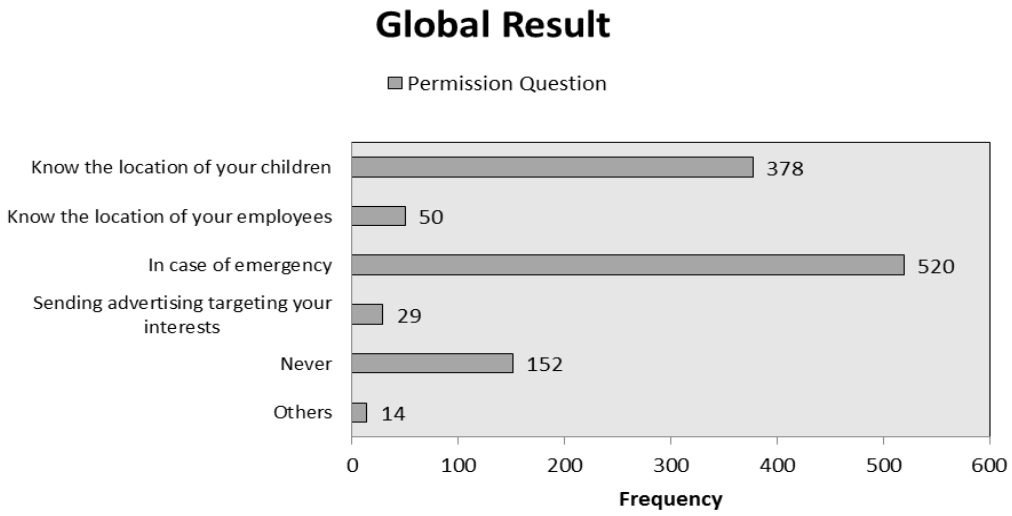
Source: Authors' own creation

4.2.6. Which of the following cases do you think the location could be accessed without the user's permission?

In this question, the respondents had five options, with multiple responses available: 1) know the location of your children, 2) know the location of your employees, 3) in case of emergency, 4) sending advertising targeting your interests, 5) never and 6) other.

The Fig. 14 shows that the majority of respondents consider that the location could be accessed without permission in case of emergency (76.6%) and the 56.1% consider they can access to the location of their children, even without their permission.

Fig. 14. Which of the following cases do you think the location could be accessed without the user's permission?

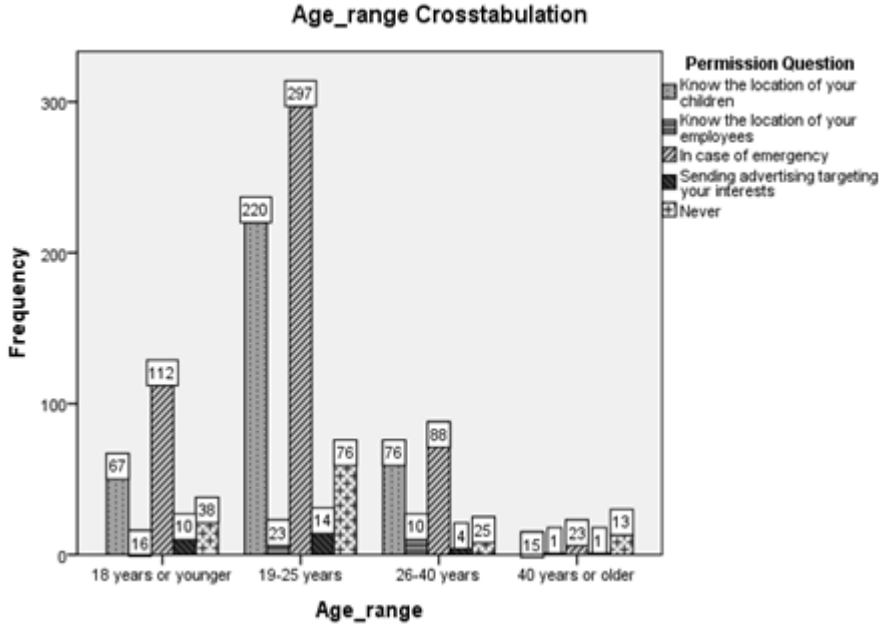


Source: Authors' own creation

A crosstabulation was performed for each independent variable (age, gender, education level and occupation). Additionally, a crosstabulation for location variable was done, with the aim to compare their results in different regions of Colombia. Fig. 15 shows the analysis between the age range and the five options of the question. Figures 16, 17 and 18 show the analyses between the five options of the question and gender, education level and occupation, respectively. Option 6) Other was omitted in the graphics because of the low percentage of respondents.

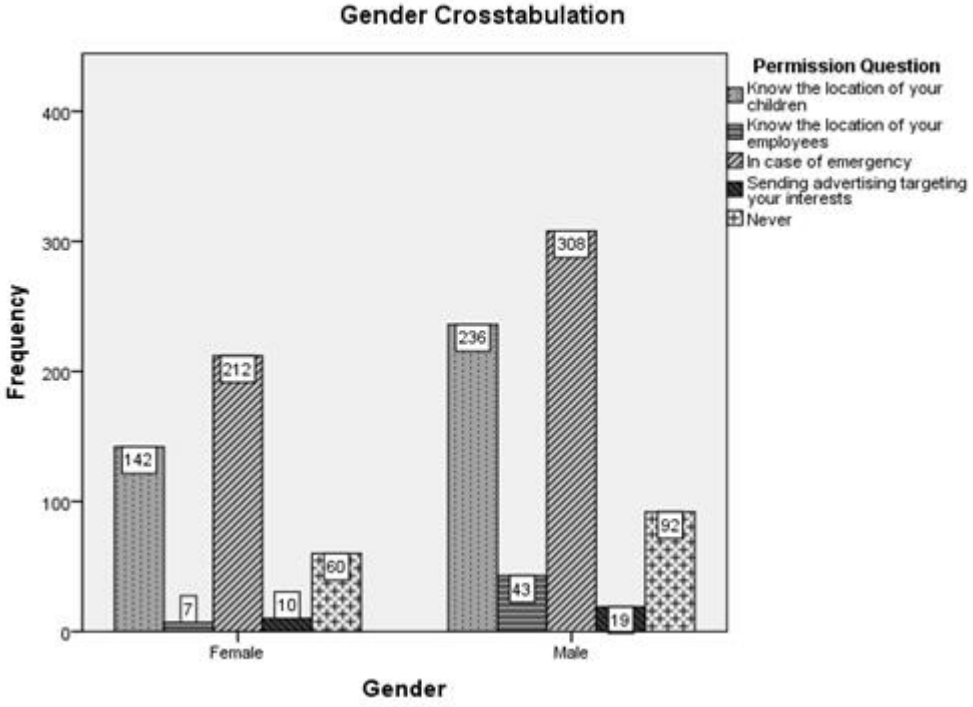
In this case, the majority of respondents in the group 19-25 years, male gender, bachelors and students consider that the location could be accessed without permission *in case of emergency and they can access to the location of their children*, even without their permission.

Fig. 15. Graph with crosstabulation for age_range and permission question



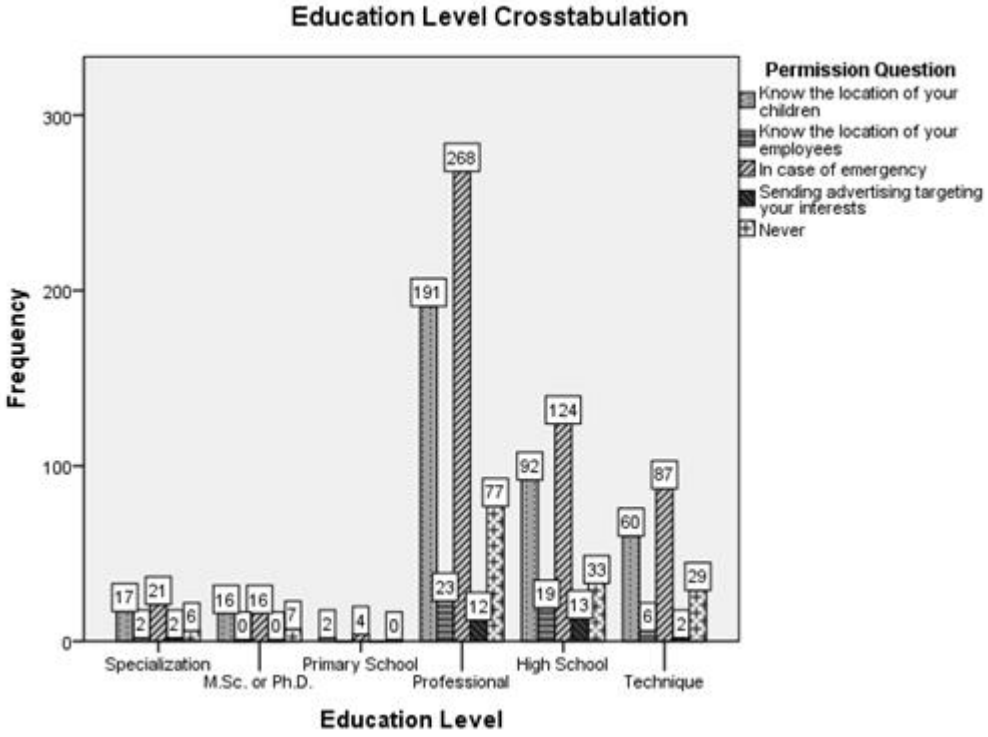
Source: Authors' own creation

Fig. 16. Crosstabulation for gender and permission question



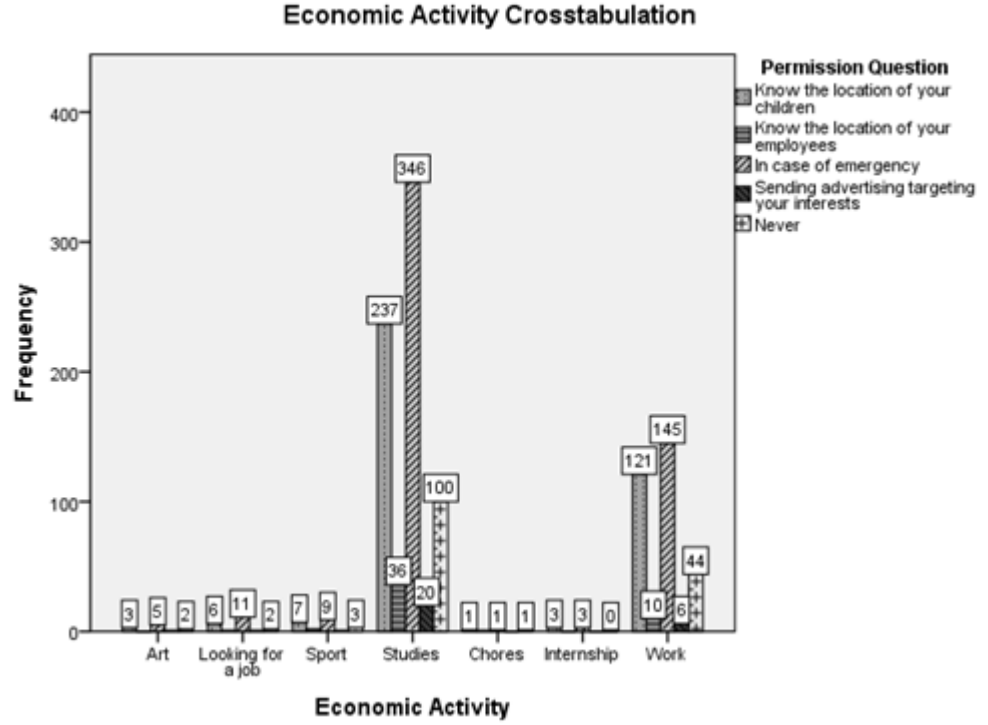
Source: Authors' own creation

Fig. 17. Crosstabulation for education level and permission question



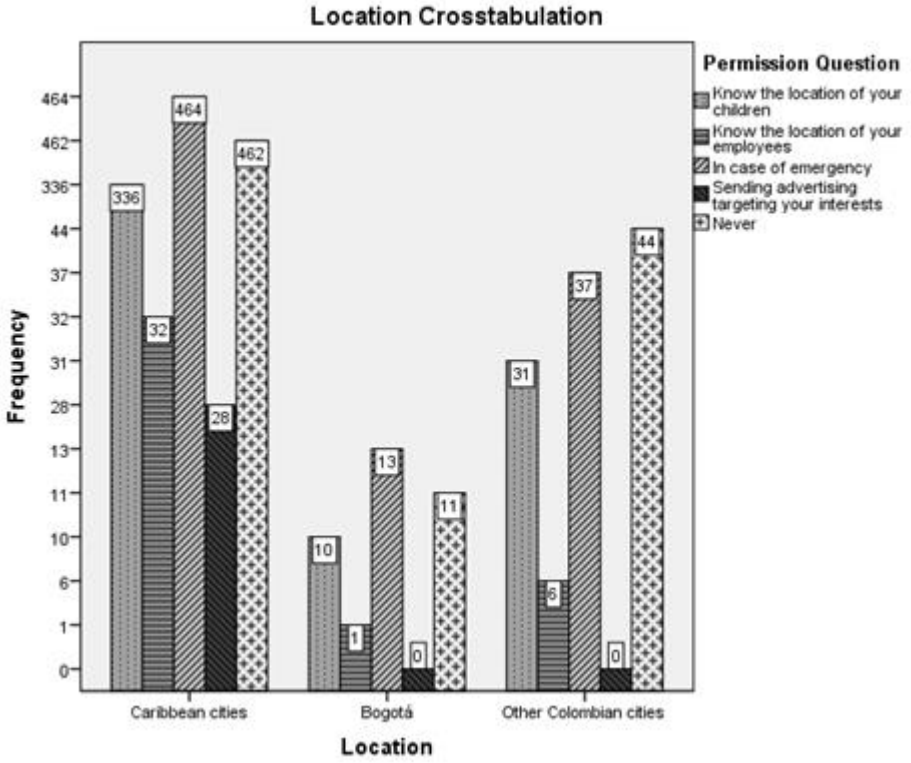
Source: Authors' own creation

Fig. 18. Crosstabulation for occupation and permission question



Source: Authors' own creation

Fig. 19. Crosstabulation for location and permission question



Source: Authors' own creation

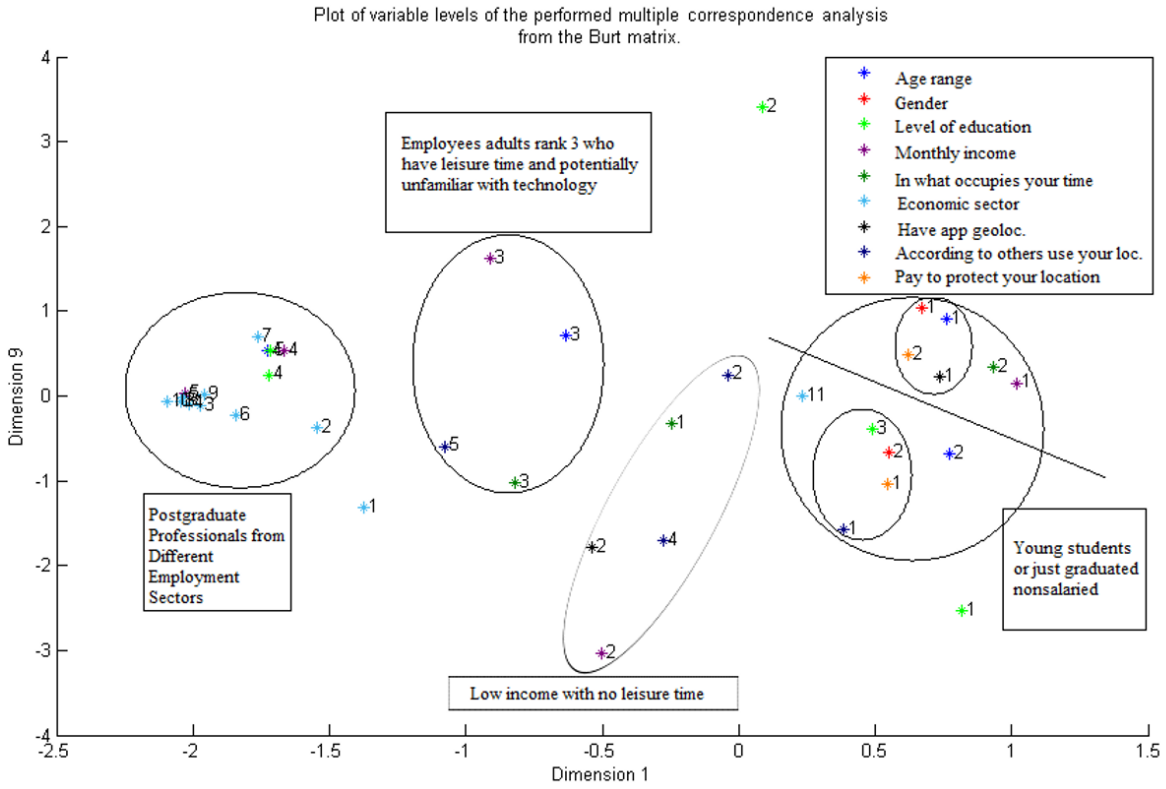
According to the comparative analysis by regions in Fig. 19, it may be observed that the percentage of respondents who agree to access the location without the user's permission *in cases of emergency and to know the location of their children* does not vary according to the region. In all cases, it tends to remain constant with 56% for the Caribbean cities and 62% for the rest of the country.

We can state that the concerns about the privacy of the location data are the same across the country and are not affected by the region of origin of the respondents. The above is also evident in the disapproval of the persons to whom its location can be *known by the employers*, a response that gets a very low percentage of acceptance: 5% in the Caribbean region and of 8.5% on average for the rest of the country. Nevertheless, it is important to highlight that the size of the sample in regions that do not belong to the Caribbean coast is very low; thus, it is desirable in future studies to expand the sample of those regions in order to get better conclusions.

4.3. Multiple Correspondence Analysis

A multiple correspondence analysis was performed to discern the attributes of the groups that are formed when matching the qualitative variables, discerning each one of the dimensions. All the variables were coded according to the definition in section 4.3, but the variable *Occupation* (*In what occupies your time*) was summarized in three categories: 1) work, 2) studies and 3) leisure. The results are presented in Fig. 20, where dimension 1 is the variable *Age* and dimension 9 is the variable *payment for protection in location*:

Fig. 20. Dimension 9 vs. Dimension 1 of the variables



Source: Authors' own creation

According to Fig. 20, the group "young students or just graduated nonsalaried", which corresponds to the groups adolescents and young adults, mostly students (age range: 1 under 18 years and 2, 19 to 25 years), or young just graduates who do not yet earn salaries, regardless of gender, disapprove the use of their location with or without their consent. This may be mainly because they know about technology and have some degree of knowledge about the use that the telecommunications companies can give to this information. In this group, there are a greater correspondence in levels 2 of "Gender", level 1 of the variable "According to others use your location" and level 1 of the variable "Pay to protect your location", which indicates that within this group, the men disapprove even more the use

consented or not of its location, reason why even they would be willing to pay to protect this information.

On the other hand, women in this group tend to not to pay for the protection of their location, and in fact they are more inclined to use geo-localized applications than men. The line is used to visualize the aforementioned situation of disparity in preferences between men and women in this group.

The group "Employees adults rank 3 who have leisure time and potentially unfamiliar with technology" shows the opposite correspondence to the previous group. In this case, the people in the age range of 26 to 40 years who have a job that provides a good income and have sufficient leisure time mostly approve the use of their location with or without their consent. This may be because they are people who do not have a good knowledge of technology and use it only to supply their needs in telecommunications.

A third group, "Postgraduate Professionals from Different Employment Sectors" is observed, which shows the correspondence of adults over 40 with a high level of education (Specialization, M.Sc. and Ph.D.), regardless of their work sector. In this case, there is not a well-defined correspondence related to the aspects of use of its location through its mobile phones. Furthermore, they are a potential group that would not bother sharing their location or give others access to it without their consent.

There is a remnant group, "Low income with no leisure time", which shows that low-income people, in general terms, spend all their time at work, so they may not be related to the use of geo-localized applications (because their salary level does not allow it or because they are not inclined to use them) resulting in that they are not clearly inclined by the approval or disapproval of the use consented or not of its location.

5. Conclusions

In this study, a survey was applied to assess how citizens from Colombia perceive privacy in LBS for mobile device users. A total of 670 answers were used in the analysis from 690 original answers, after the filtering process. It is worth noting the demographics of the respondents; the majority of them were university students because the contacted population was several universities of Barranquilla, Santa Marta and Monteria, mainly. This can bias the results, but the questions and the methodology can be applied to the whole country, which would build a more assorted sample.

Regarding the results, it can be stated that, in general, the respondents did not show a real concern about the privacy in their geo-location and the majority is not willing to pay to protect this privacy. However, they consider it an invasion to their geo-location privacy if location data is sold to third parties or if they are not informed about using the location. They agree

with allowing access the location without permission in order to know the location of their children and in case of emergency.

Furthermore, with the multiple correspondence analysis we find that mobile device users who would be willing to pay to protect their privacy are young men in the age range of 18 to 25 years, who also disapprove the use of their location information without consent.

Responding to this type of surveys can generate awareness among participants about the use of their private information. In addition, these results can be used to create government policies and regulations by technology companies about the privacy management.

Finally, it is worth mentioning that *Google Forms* facilitated the assessment of data, taking into account that the participants were not geographically located in the same area. Additionally, it was necessary to limit the number of questions in order to ensure that the motivation level of respondents was kept high and to avoid poor data quality [28]. The survey did not ask the identity of the respondent, ensuring anonymity of the respondents.

For future work, a new survey should be applied to a larger and more diverse population in order to capture not only university-related citizens but also other communities that may have different needs from their LBS. Additionally, it could show the impact of the number of increasing scandals related to privacy in social networks, such as the ones about Facebook and the elections in the United States. In addition, the survey may evaluate the perception of the citizens about strategies to save the privacy in LBS for mobile device users.

References

[1] M. Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center, 2014. [Online]. Available: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[2] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[3] M. Zurbaran, L. Gonzalez, P. Wightman Rojas, and M. Labrador, "A Survey on Privacy in Location-Based Services," Ing. y Desarro., vol. 32, no. 2, pp. 314–343, 2014.

[4] J. K. Burgoon, R. Parrott, B. A. Le Poire, D. L. Kelley, J. B. Walther, and D. Perry, "Maintaining and Restoring Privacy through Communication in Different Types of Relationships," J. Soc. Pers. Relat., vol. 6, no. 2, pp. 131–158, May 1989.

[5] A. F. Westin, "Washington and Lee Law Review Privacy And Freedom," Lee L. Rev, vol. 166, 1968.

[6] L. Steinfeld and K. Sutherland Archuleta, "Privacy Protection and Compliance in Higher Education: The Role of the CPO," 2006.

[7] UN High Commissioner for Human Rights, "The right to privacy in the digital age," 2014. .

[8] C. Paine, U.-D. Reips, S. Stieger, A. Joinson, and T. Buchanan, "Internet users' perceptions of 'privacy concerns' and 'privacy actions,'" Int. J. Hum. Comput. Stud., vol. 65, no. 6, pp. 526–536, 2007.

[9] EFF, "The Problem with Mobile Phones," Surveillance Self-Defense - EFF, 2015. [Online]. Available: https://ssd.eff.org/en/module/problem-mobile-phones. [Accessed: 06-Aug-2018].

[10] Y.-A. de Montjoye and C. A. Hidalgo, "Unique in the Crowd: The privacy bounds of human mobility," Sci. Rep., vol. 3, pp. 193–220, Mar. 2013.

[11] R. Mekovec and N. Vrþek, "Factors That Influence Internet Users' Privacy Perception," Int. Conf. Inf. Technol. Interfaces, 2011.
[12] J. L. Boyles, A. Smith, and M. Madden, "Privacy and Data Management on Mobile Devices | Pew Research Center," 2012.
[13] I. Boutsis and V. Kalogeraki, "A Fast and Efficient Entity Resolution Approach for Preserving Privacy in Mobile Data," in 2016 IEEE International Congress on Big Data (BigData Congress), 2016, pp. 173–180.
[14] L. Tang, S. Vrbsky, and X. Hong, "Collaborated Camouflaging Mobility for Mobile Privacy."
[15] R. Liu, J. Cao, L. Yang, and K. Zhang, "PriWe: Recommendation for Privacy Settings of Mobile Apps Based on Crowdsourced Users' Expectations," in 2015 IEEE International Conference on Mobile Services, 2015, pp. 150–157.
[16] Y. Gong, L. Wei, Y. Guo, C. Zhang, and Y. Fang, "Optimal Task Recommendation for Mobile Crowdsourcing With Privacy Control," IEEE Internet Things J., vol. 3, no. 5, pp. 745–756, Oct. 2016.
[17] F. Giselle, B. Javier, and H. Alejandro, "Location Privacy for a Monitoring System of the Quality of Access to Mobile Internet," IEEE Lat. Am. Trans., vol. 14, no. 6, pp. 2894–2896, Jun. 2016.
[18] M. Poikela, R. Schmidt, I. Wechsung, and S. Moller, "About your smartphone usage; — Privacy in location-based mobile participation," in 2015 IEEE International Symposium on Technology and Society (ISTAS), 2015, pp. 1–6.
[19] Observatorio de la Seguridad de la Información - INTECO, "Estudio sobre seguridad en dispositivos móviles y smartphones," 2011.
[20] D. Wagner et al., "Hide and seek," in Proceedings of the 12th international conference on Human computer interaction with mobile devices and services - MobileHCI '10, 2010, p. 55.
[21] GSMA, "Mobile Privacy: Consumer Research Insights and Considerations for Policymakers," 2014.
[22] A. Fink, J. Kosecoff, M. Chassin, and R. H. Brook, "Consensus methods: characteristics and guidelines for use.," Am. J. Public Health, vol. 74, no. 9, pp. 979–83, Sep. 1984.
[23] J. Casas Anguita, J. R. Repullo Labrador, and J. Donado Campos, "La encuesta como técnica de investigación.Elaboración de cuestionarios y tratamiento estadístico de los datos (I)," Aten. Primaria, vol. 31, no. 8, pp. 469–558, 2003.
[24] D. Christin, C. Buchner, and N. Leibecke, "What's the value of your privacy? Exploring factors that influence privacy-sensitive contributions to participatory sensing applications," in 38th Annual IEEE Conference on Local Computer Networks - Workshops, 2013, pp. 918–923.
[25] A. J. B. Brush, J. Krumm, and J. Scott, "Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location," in Proceedings of the 12th ACM International Conference on Ubiquitous Computing, 2010, pp. 95–104.
[26] M. Arriaza Balmón, Guía práctica de análisis de datos. Instituto de Investigación y Formación Agraria y Pesquera, 2006.
[27] L. Armando Galvis, "Geografía económica del Caribe Continental," 2009.
[28] U.-D. Reips, "Standards for Internet-Based Experimenting," Exp. Psychol., vol. 49, no. 4, pp. 243–256, 2002.