Granting consent in mobile applications
A case study on the consent-granting-mechanisms and the Privacy Policy documents of Facebook, Google Search, Google Maps, Foursquare and WhatsApp mobile applications in Android and iOS

Kalliopi-Kyriaki Dilaveraki

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES
A thesis submitted for the degree of
LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law

February 2016
Thessaloniki – Greece
Student Name: Kalliopi-Kyriaki Dilaveraki

SID: 1104140012
Supervisor: Prof. Dr. Eleni Kosta

I hereby declare that the work submitted is mine and that where I have made use of another’s work, I have attributed the source(s) according to the Regulations set in the Student’s Handbook.

February 2016
Thessaloniki - Greece
Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law at the International Hellenic University.

Acknowledging the dangers for individuals’ privacy hidden in the widespread use of mobile applications, the dissertation studies the current practices of five of the top famous mobile applications; Facebook, Google Search, Google Maps, Foursquare and WhatsApp in Android and iOS are examined with regard to the installation procedure and the Privacy Policy documents provided to users. How applications access and process users’ information stored on the device? For what purposes? What information do they provide to them about this process? How and what are the users asked to agree to? From a legal point of view, do the Data Protection and ePrivacy Directives protect users in the European Union territory when the aforementioned applications process their personal data? When yes, do the current practices regarding the installation procedure and Privacy Policy documents reconcile with the prerequisites of these Directives concerning the acquisition of valid consent for the processing of personal data? With particular focus on the examination of the consent related issues, the dissertation elaborates on all the above questions and attempts to provide responses. Acknowledgments
Acknowledgements

This work was encouraged and supported by some people that I would like to acknowledge. First and foremost, this dissertation could not be written without the active support of Pr. Dr. Eleni Kosta, who assisted me as a supervisor. I wish to wholeheartedly thank her not only for the valuable scientific feedback and guidance, but mostly for literally being a teacher, interested in and offering care for the overall progress of her students.

My devotion to the present research, would not be possible without the multifarious support of my family, and especially my parents, to whom I am immensely grateful.

I would like to say a deep and great thank you to all the staff members of Tilburg Institute for Law Technology and Society (TILT) for introducing me to the world of academic legal research and motivating me with their energy and enthusiasm. Special thanks to my dear colleagues István Böröcz and Kiril Kalev for being there to answer all my questions. Moreover, I couldn’t have reached this knowledge and experience without the support of the staff members of the International Hellenic University and of Dr. Komnios Komninos in particular.

Understanding the technical aspects of the research would be impossible without the precious helping hand of my friends Fotis Dimanidis and Kostas Romanidis as well as of my cousin Michalis Kalaitzakis.

Effy Tsapaki, my beloved friend, has my heartfelt thanks for taking the time to read my dissertation and give me valuable insights.
Finally, this research was supported by Nikos Pavlou and Danny Hoekzema who let me explore their mobile devices. Any errors are the author's alone.

Keywords: privacy concerns on mobile applications
personal data in mobile applications
consent in mobile applications
Privacy Policy documents
applicability of the Data Protection Directive
applicability of the ePrivacy Directive

Kalliopi-Kyriaki Dilaveraki
30/01/2016
Chapter 1-Introduction

1.1 Mobile applications posing a threat on the protection of users’ personal information; description and significance of the problem.

The overwhelmed everyday life of individuals nowadays demands quick, smooth and, preferably, cheap or free solutions that can satisfy their needs. Those solutions are at a great extent already provided and are still blossoming and improving. Where? In our mobile devices. Simply by connecting those to the internet and by clicking some buttons and basic, everyday needs are covered. May sound magical or alien, but is it true and real. Mobile application developers entered the forefront of innovation and have been “drawing” applications for, almost, every human need. Although there is no doubt that mobile devices together with mobile applications have revolutionized peoples’ reality, it seems that the saying “everything comes at a cost” or at least “…at a risk” is being proven, again.

Smart mobile devices and mobile applications are highly interdependent. The hardware and software of smart mobile devices (hereinafter “mobile devices”) is especially manufactured to be online, detect the location of the device and interact with the mobile applications. A mobile application (hereinafter “app”) is a software, small and specific, especially designed to run on smart mobile devices.1

The functionalities of mobile devices and apps are dependent on information stored in the mobile device. This information is usually closely connected to the user of the device. Address book, photos, videos, personal and professional mails can be some examples.2

---

2 Ibid.
Thanks to these interactions, apps and mobile devices have been an indispensable everyday tool.³

By downloading apps we reveal information about ourselves in various ways. Initially, the choice of a specific application together with our activities and communications on the apps’ environment provides evidence on our needs and preferences. Additionally, applications ask permissions to access the information stored in our mobile devices and mobile identifiers have been developed to facilitate the tracking of the users’ activities, raising serious privacy concerns.⁴ Moreover, technology crammed into the mobile devices enables the constant monitoring of the location of the user. It is possible that this monitoring is taking place semi-secretively, when users are not well informed on either that the location services of the device are on or on how location data is collected and used. It is also possible that the monitoring takes place secretly, without any information having been provided to users.⁵ Last but not least, it has been proven by researches that mobile applications share information about users to third parties, without, often, notifying them.⁶ The pieces of information unveiled, or an aggregation of them, are not left unexploited.

The majority of the mobile applications are offered for free or at a low cost. More often than not, mobile app developers cover the essential needs for surviving their activities through collaborating with advertising companies. The latter provide app developers with the financial means they need in return for accessing information on app users profiles and activities. This access can be direct, when advertising companies access

⁵ ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 13/2011 on geolocation services on smart mobile devices, WP 185" (2011) 7
⁶http://techscience.org/a/2015103001/(accessed on 19/12/2015).
information through, for instance, tracking facilities offered in the mobile landscape, or indirect, when app developers share the information they collect with the advertising company. These information is used for tailored advertising and methods that are widely known as "online advertising". 

While online advertising, as being the basic source of income for app developers, plays an essential role on the growth of internet economy and consists a motive generating social and economic progress, it also raises major privacy and data protection concerns.

Advertisers need extensive information about their audience in order to present them advertisements that fall into the sphere of their interest (hereinafter “behavioural advertising”). 

Besides, the current technological innovations, such as big data analytics, facilitate the creation of profiles of internet users and thereupon offers tools of power and control over their life and preferences to companies offering online behavioural advertising services. As it is masterfully remarked by the Article 29 Data Protection Working Party (hereinafter “Article 29 Working Party”)11, “such practice must not be carried out at the expense of individual’s rights to privacy and data protection”. 

---

8 Ibid.
9 PRIVACY COMMISSION OF BELGIUM, “Recommendation no. 04/2015 of 13 May 2015” relating to 1)Facebook, 2)Internet and/or Facebook users, as well as 3) users and providers of Facebook services, particularly plug-ins” (2015). Facebook provided to the Privacy Commission the following information with regard to its business model "Facebook's underlying business model is based on advertising. … Equally, advertisers prefer to present adverts that are relevant to their audience, because users respond more positively to relevant adverts, and there is less waste in their marketing efforts. To do this we use a variety of information about our users use of Facebook services in order to gauge which adverts will be of relevance."
11 The Article 29 Data Protection Working Party is an advisory body on the protection of persons with regard to the processing their personal data, set up by the Article 29 of the Data Protection Directive. It issues Opinions, Recommendations and Working documents that, despite not being legally binding, they are of high importance to the interpretation of the current legal framework connected to the processing of personal data.
Federal Trade’s Commission’s Staff Report of February 2014 on Mobile Privacy
Disclosures and Transparency aptly points that, “When people use their mobile devices,
they are sharing information about their daily lives with a multitude of players”.13
Indeed, in the terrain of mobile applications, there are a lot of players involved; device
and OS manufacturers, app developers/owners, app stores, third parties, such as
advertising companies, and the end user.

In its opinion 02/2013 on apps on smart devices, the Article 29 Working Party underlines
the following as the main data protection risks related to mobile applications:

a. The large quantities of data accessible by apps, thanks to their close interaction
with the operating system (see Chapter 2: Actors’ technologies and findings on
current practices).
b. The high risk arising from “the degree of fragmentation between the many
players in the app development landscape” (see 2.1 Actors and their
technologies).
c. The lack of transparency with regard to the data that are actually collected by
the applications and an apparent trend towards data maximization.
d. Poor security measures that may lead to unauthorized processing of personal
data.14

Furthermore, the Article 29 Working Party indicates the importance of information
concerning the location of the mobile device on “disclosing” the “geographical
component” of users’ activities and, subsequently, increasing the value of any other
information collected and facilitating the formation of targeted profiles. 15

13 FEDERAL TRADE COMMISSION “Mobile Privacy Disclosures Building Trust Trough Transparency
14 ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 2/2013 on apps on smart devices,
WP 202” (2013) 5.
15 ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 13/2011 on geolocation services
on smart mobile devices, WP 185” (2011) 3.
Therefore, it appears that mobile applications entail pivotal privacy and data protection threats. The legal community has been facing the challenge of understanding technology and drawing new lines to balance conflicting (apparently at least) interests.

1.2 Research question

The dissertation reflects on the issues related to the granting of valid consent for the processing of personal data on the mobile applications’ terrain under the European Data Protection framework and, in particular under the provisions of the Data Protection and the ePrivacy Directive. To this aim it studies the current practices related to the installation procedure of five of the most famous mobile applications (Facebook, Google Search, Google Maps, WhatsApp and Foursquare, hereinafter “the examined applications” or “the examined apps”), when downloaded and installed through the most commonly used application marketplaces (Google Play Store and App Store) on Android and iOS operating systems respectively. It additionally studies the Privacy Policy documents of these applications. It specifically evaluates the above practices and documents on the light of the provisions of the Data Protection and ePrivacy Directive for a “freely given”, “specific”, “informed” and “unambiguous” consent of the data subjects for the processing of their personal data. Finally, when doubts arise on the reconciliation of the practices with the aforementioned provisions, the dissertation reflects on the recommendations of the Article 29 Working Party and other Data Protection authorities and proposes tools for building a better compliance.

18 Article 7(a) together with Article 2(h) of the Data Protection Directive and Article 5(3) of the ePrivacy Directive.
To respond to the central research question, the dissertation addresses the following subquestions:

(a) Do the examined applications process personal data as defined in Article 2(a) of the Data Protection Directive?
(b) Are the examined applications data controllers as defined in Article 2(d) of the Data Protection Directive?
(c) Are the preconditions for the territorial applicability of the Data Protection Directive, as described in its Article 4, satisfied with regard to the examined applications?
(d) Do the examined applications fall into the territorial and substantial scope of the ePrivacy Directive, as described in its Article 3(1)?
(e) Does Article 5(3) ePrivacy Directive, in particular, apply to the examined applications?
(f) Does Article 9(3) ePrivacy Directive, in particular, apply to the processing of location data by the examined applications?

1.3 Methodology and structure

The dissertation applies the methodology of empirical legal research. It aims on providing an answer to a legal question having been arisen de facto during the practical application of law, by examining specific cases and providing specific examples. In order to draw a conclusion regarding the main question, each of the sub-questions are addressed.

The assessments made are based on the examination of the current practices, as described above, and as well as on the study of the Privacy Policy documents of each one of the examined applications.

The evaluated primary sources include the Data Protection and ePrivacy Directive, as well as EU Case Law. As far as secondary sources are concerned, given the empirical
nature and the aims of the research, the dissertation focuses on the opinions of the Article 29 Working Party. Academic legal books, articles and websites shedding light to technical aspects related to the problem are also examined and invoked.

To start with, in Chapter 2, the dissertation notes down the procedure for downloading and installing the examined applications in each one of the OS and application marketplaces. The existing differences are examined with focus on what users are asked to agree to, what permissions are asked, what information is provided to users and at which point of the procedure. The scrutiny of the Privacy Policy and related documents follows, on the light of pointing out what data are collected, for what purposes, whether information is shared with third parties and whether opt-in and opt out techniques are provided. The overall structure of the documents and the information provided are discussed. The dissertation has adopted the terminology of the Article 29 Working Party on its opinion 02/2013 on apps on smart devices, with regard to the actors involved in the mobile applications terrain.\(^\text{19}\) Although this may be relevant for Facebook, Foursquare and WhatsApp, privacy issues related to the posts and status messages users share on these applications fall outside of the scope of the present research.

Focus shifts in Chapter 3 on the presentation of the legal framework provided by the Data Protection and ePrivacy Directive. Not all the provisions of the aforementioned Directives are examined, but only those needed to answer the research question and subquestions. The legal findings will be supported by Case Law and investigations by national data protection authorities, where necessary.

In Chapter 4 the dissertation assesses the findings of Chapter 2 under the legal provisions elaborated in Chapter 3 and, in particular, under the requirements stipulated on the Data Protection and ePrivacy Directive with regard to a “freely given”, “specific”, “informed” and “unambiguous” consent of the data subjects for the processing of their personal data. When doubts arise on the conformity of the practices with the aforementioned provisions, the dissertation presents the recommendations of

---

the Article 29 Working Party and other Data Protection authorities, and proposes tools for building a better compliance.

Finally, Chapter 5 entails the conclusions of the research.
Chapter 2: Actors’ technologies and findings on current practices

Players in the mobile applications terrain, accordingly to their technologies, adopt various practices on providing users with information on what data the applications access and for what purposes. Chapter 2 presents the technical aspects and the findings of the research.

2.1 Actors and their technologies

Device and operating system manufacturers, applications marketplaces, application developers and third parties are the four building blocks in the arena of mobile applications. They are intertwined and the practices of each one of them may affect the others.

2.1.1 The device and OS manufacturers

Mobile devices need an operating system in order to be functional. The operating system (hereinafter "OS") is a software, compatible with the hardware, which triggers the facilities of the device. One of the greatest functionalities of the OS is the administration of the applications running on the device. Applications need to “communicate” with the operating system in order to function and this becomes possible through the application programming interfaces (APIs). APIs are inherent in mobile devices and enable apps to access data stored in the device or generated by it, as well as sensors crammed into the device. These sensors (gyroscope, digital compass, accelerometer, front and rear cameras etc) enable the detection of the location of the
user. In this way, app developers are able to read the devices and apps’ history, users’ identity, detect their location, take pictures and much more.

At the time being there are a lot of companies manufacturing smart mobile devices (iOS, Samsung, Nokia, Sony etc) and four basic mobile operating systems; Android, iOS, Windows Phone and Blackberry OS. The majority of the device manufacturers implement Android OS, while iPhones and iPads share the same owner with iOS, Apple, and are always designed to operate under it.

Applications in Android and iOS run in a sandbox, an isolated area of the system that does not have access to the rest of the resources, unless access permissions are explicitly granted by the user. Application developers decide on the permissions to be asked by the user and the OS together with the application marketplace are basically responsible for the way information on the permissions asked is provided to end users.

Additionally, the hardware together with the OS are responsible for creating the privacy settings of the device and enable users to control whether and what categories of their personal data are accessed and processed by the apps.

### 2.1.2 Application marketplaces

Application marketplaces are the distributors of the applications. Upon request by the user, they offer the software of the application that is subsequently installed in the mobile device. The most broadly used operating systems are very closely connected to a particular app store. Google Play store is the primary and official application store, pre-installed on most Android devices, and App Store is the unique pre-installed marketplace platform for iOS mobiles and tablets.

---

As explained above, application marketplaces are involved in the permissions requesting system and as the Article 29 Working Party has aptly observed, “App stores are in an important position to enable app developers to deliver adequate information about the app, including the types of data the app is able to process and for what purposes.” Therefore, application marketplaces, are, without a doubt a key actor linked to the privacy concerns in the mobile applications terrain.

2.1.3 Application developers/owners

As described above, applications are software designed by app developers who work independently or as part of a company. The dissertation has adopted the terminology of the Article 29 Working party and it is necessary to clarify that the use of the term “app developers” refers to the programmers and technical developers of mobile applications as well as the companies and organizations who request the development of an application and “determine its purposes”.

2.1.4 Third parties

Undertakings or natural persons that have access to data through the application that the user has downloaded, or with whom the app developers share personal information of the users are called third parties.

---

23Ibid.
Third parties may be advertising networks, intermediaries, other entities providing the app developers with analytics and communication services, or entities processing data and offering services on behalf of the data controller.24

2.2 Method of approach-research strategy

The research is conducted on Nexus 7 mobile device with Android OS version 6.0.1 and on iPhone 5 with iOS 9.2 version (see Figure 2 Nexus 7 mobile device on which the research was conducted and Figure 3 iPhone 5 on which the research was conducted on Appendix).

First and foremost, two different operating systems are chosen with the aim of indicating how possible differences with regard to the practices adopted may reflect on the legal assessment. Android and iOS are selected as ranked first in popularity.25 The same goes with the examined applications. Different practices may lead to different legal assessment. Facebook, Google Search, Google Maps, Foursquare and WhatsApp are examined and the selection is a result of their popularity and as well as of the particular characteristics of each one of them. Privacy concerns surfaced on some of them also affected the final selection.26

Facebook is the most famous social networking service. More than one billion users have downloaded the Facebook application through the Google Play Store27. Serious privacy issues have been raised around the huge quantity of users’ information that the service has access to and the way it has been processing it. Google Search is the most widely

25In 2015, Android dominated the smartphone market share with a percentage of 82.8% followed by iOS with a percentage of 13.9%. Samsung has been the leader in the worldwide smartphone market reaching a 21, 4% share in 2015, followed by Apple (13,9% of the market share). Based on data of the International Data Corporation, "Smartphone OS Market Share, 2015 Q2", http://www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed 25/11/2015).
26For more information on Facebook privacy concerns among others see MARK WEINSTEIN, "Is privacy dead?", http://www.huffingtonpost.com/mark-weinstein/internet-privacy_b_3140457.html, accessed on 06/01/2016)
27Based on the information provided on the Facebook’s page on Google Play store
used web search engine on the World Wide Web28 and it is owned by Google Inc. that also owns Google Maps. Google Maps belongs among the most popular location based services.29 Its mobile application version uses the location tracking facilities of the mobile device to provide navigation, traffic report and other relevant services. Foursquare mobile application offers a location based service as well, providing recommendations for worth visiting places around the current location of the user, based on the preferences that the user has shared with the application. WhatsApp is an instant messaging mobile application. The app has been “one of the world’s top five best-selling apps” according to the Dutch Data Protection Authority that, in collaboration with the Office of Privacy Commissioner of Canada, investigated WhatsApp for issues relating to (among other) access by the application to the address book of the users.30

The dissertation focuses on the examination and assessment of the consent related issues. To this view, particular emphasis is paid on the practices of the apps’ marketplaces and the examined apps; however, the architecture of the mobile devices, as described above, and the interrelationship between device, OS, apps marketplace and apps requires that light is also shed on the practices of the rest of the actors, and the issues arising are approached spherically. The research is carried out as follows; all five applications are downloaded both form Google Play Store and App Store. The permissions that each app requests from users in order to access data stored in the device are noted down. The differences between the two OS and application marketplaces are observed with regard to the information provided to users, as well as

29 COLLETE CUIJPERS AND BERT-JAAP KOOPS, “How fragmentation in European law undermines consumer protection: the case of location-bases services” (2008) 33 European Law Review 886. According to the authors, location based services “are services based on location information (....) can be delivered by means of wireless systems and unique identification of communication devices, combined with location data(....) use different types of techniques that process location data in various ways.”
to the privacy settings each operating system has developed. Where appropriate, references are provided to the Appendix of the dissertation, where screenshots (Figures) from the research are presented. Following, the Privacy Policy and related documents of each application are scrutinized to puzzle out what data each application collects, whether location data are collected, for what purposes and if it is shared with third parties. These practices are assessed in Chapter 3 under the light of the Data Protection and ePrivacy Directive and the guidelines given by the Article 29 Working Party and other data protection authorities to the players on mobile applications’ arena.

2.3 Current Practices

2.3.1 Giving permissions

As explained above, the majority of the applications need access to personal data stored in the device in order to function or share it for advertising purposes; however this access is not possible unless the user gives permission (see 2.1.1 The device and OS manufacturers). Both Android and iOS have been criticized for their permissions granting systems and the sufficiency of the information provided in the application stores and during the installation procedure\(^3\). The latest versions, Android Marshmallow 6.0 and iOS 9 present the following characteristics:

<table>
<thead>
<tr>
<th></th>
<th>Android Marshmallow 6.0</th>
<th>iOS 9 versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links to legal documents presented to users before installation.</td>
<td>• Link to the Privacy Policy of the application developer.</td>
<td>• Link to the Privacy Policy of the application developer.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Time when permissions are asked</th>
<th>When the app actually needs to use the specific feature or information (see an example on Figure 4 New permissions’ system on Android Marshmallow 6.0.1 and Figure 5 Facebook mobile app asking for permissions on Android Marshmallow 6.0.1 on Appendix).</th>
<th>When the app actually needs to use the specific feature or information (see an example on Figure 6 Facebook mobile app asking for permissions on iOS 9.2 and Figure 7 Facebook mobile app asking access to location services on iOS 9.2 on Appendix).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information given about the reason why each permission is asked</td>
<td>It is usually not presented. It depends on the information that the app developer has provided to the permissions granting.</td>
<td>It is presented when each permission is asked. (see an example on the same Figures as above).</td>
</tr>
</tbody>
</table>
Enabling users’ control

Through the Settings users can control which applications have access to which category of data and can change their choices whenever they decide to (see Figure 10 Location permissions on Android Marshmallow 6.0.1 and Figure 11 Google Maps Application permissions on Android Marshmallow 6.0.1 on Appendix).

Through the Settings users can control which applications have access to which category of data and can change their choices whenever they decide to (see Figure 8 Privacy Settings of iOS 9.2 and Figure 9 Settings of iOS 9.2 on Appendix).

<table>
<thead>
<tr>
<th>Table 1 Installation procedure-Permissions-Information asked</th>
</tr>
</thead>
</table>
| Android Marshmallow 6.0 launched a significant change to the permissions granting system compared to the previous versions (see Figure 4 New permissions’ system on Android Marshmallow 6.0.1 on Appendix). The “all or nothing system”, where users were asked, before installing the application, to grant all permissions that the application were asking for otherwise they could not download it, has been abandoned and presently, users can grant only the specific permissions they want, similarly to iOS. Additionally, unlike the previous versions, Android Marshmallow 6.0 enable users to control which applications have access to each specific category of data and change the settings whenever they decide to again similarly to iOS (see examples on Figure 8 Privacy Settings of iOS 9.2 and Figure 10 Location permissions on Android Marshmallow 6.0.1 and Figure 11 Google Maps).

---

32 This information is provided by the app developers and not by the app store; therefore it is possible that some applications do not explain the reason why they ask for each permission.
Application permissions on Android Marshmallow 6.0.1 on Appendix. iOS latest versions have included links to the Privacy Policy documents of the app developers.

For Android OS, applications have to be developed in a language that has complete access to Android APIs. Respectively, for iOS, applications have to be developed with Apple’s iOS SDK. Google Play Store and App Store has created several groups of permissions that an application can ask from the user. Each permissions group includes several information that the application is granted to access and some actions that the application is granted to perform. Those permission groups are more on Android. Explanations on what each group of permissions entails are provided by Google in its Help Centre, but not by Apple. In its description for some groups of permissions Google Play Store warns users of potential harmful consequences from the use of a malicious application. Permission groups may be modified or reclassified over time. Unlike Google Play Store, App Store asks users to enter their Apple ID and password in order to download and install an application; however users can change this setting. Automatic updates are usually by default turned on for both OS and stores; nonetheless, users can opt to turn them off.

Unfortunately, not all apps available on the Google Play Store are designed for the new operating system of Android and have not implemented the new permissions system yet. As a result, for those applications users still need to follow the “all or nothing system”.

In order to be launched on Google Play Store and App store apps must follow their policies. The reason behind that is security. Application marketplaces need to protect their customers from malware and applications “hiding” illegal activities, like promotion of violence and bullying. Applications that are infringing these policies are removed.


Google Help Centre states that if the update of the application needs access to permissions that are part of a permission group that the user has already accepted, he/she will receive no notification asking for approval for the new permission. It is considered as already approved. If the permission needed is part a permissions group that the user has not given its approval for, he/she will be asked to accept the update, despite of the fact that automatic updates are turned on. https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1 (accessed on 01/02/2016).
Location based services such as Google Maps and Foursquare cannot (fully) run if the location services of the mobile device are off. When needed, the apps ask permission for turning on the location services. For Android, on the poping-up window, asking for permission, the user can click on the option “Learn more” and the Help Centre provide information on how Android OS and Google Play Store have developed location settings and permissions.

Google Search and Google Maps apps are usually preinstalled on Android OS devices and permissions are granted automatically by the OS to them. Users have several options, including forcing them to stop, uninstall updates (but not the application) and disable them. Users can always enable them again and use them only by filling in a box that they agree with the Terms and Conditions and Privacy Policy document of the app, without having been asked to give any permission.

2.3.2 Privacy Policies and related documents

Privacy Policies are part of the legal documents accompanying a mobile application. They have been developed on the line of compliance with legal obligations protecting privacy online, part of which is the obligation of the entities collecting data online to provide the data subject with some information about the data processing. Most of the times, Privacy Policies consist part of the Terms of Use of the application. Their contractual nature has been disputed and it is still a grey area.

Following, the table presents the information collected by each one of the five mobile applications that the dissertation examines. All the information provided on the tables is based on the Privacy Policy and related documents of each of the applications. Different names can be given to Privacy Policy documents. For instance, Facebook names the relevant legal document as “Data Policy” while WhatsApp names it “Privacy Notice”.

---

38 Different names can be given to Privacy Policy documents. For instance, Facebook names the relevant legal document as “Data Policy” while WhatsApp names it “Privacy Notice”.
40 Data Policy of Facebook, available at https://www.facebook.com/privacy/explanation (accessed on 31/01/2016)
data collected have been categorized by the author and it is possible that some of the particular examples included in each category does not refer to all the applications that access the general category. Emphasis has been put on the information that the author considered as collectable though the mobile applications and not through the “on browser” versions of the services. Given that Google Search and Google Maps share the same Privacy Policy document, they are examined in a unified category named as “Google Services”.

<table>
<thead>
<tr>
<th>Information collected</th>
<th>Facebook</th>
<th>Google Services</th>
<th>Foursquare</th>
<th>WhatsApp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity of the data subject, e-mail, telephone number, credit card and payment data, photos (Those data are generally named by the examined apps as “information provided by the user in order to use the services”)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√ (only telephone number)</td>
</tr>
<tr>
<td>Date and duration of accessing the apps, browsing history, interaction with advertisements, information</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>communicated with others, address book</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Those data are generally named by the examined apps as “Information collected when the user uses the application”)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about the device and operating system, unique mobile identifiers, language, time zone, IP address.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Location information, like GPS signals</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Information on or about the content the user provides, such as the location of a photo, or the date a file was created and information about the user provided by other users</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about users and their activities on and off the application.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Information generated through cookies or similar technologies that applications use to identify the device.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Table 2 Information collected by the applications based on their Privacy Policy documents

In their privacy policies, the application developers also enunciate the purposes of the processing of personal data. Based on the findings all five apps collect data for the purposes of:

(a) providing, improving and developing services,
(b) communicating with the user about the services, terms and policies and sending them marketing communications,
(c) verifying accounts and activity, promoting safety and security,
(d) showing relevant ads and measuring their effectiveness (except WhatsApp).

The examined apps share information that they collect with third parties that also process it, either for the provision of the service, on behalf of the application developer, or for advertising and measurement purposes.

The structure of the Privacy Policy and related documents and the way users are provided with information about the collection of their personal data is of tantamount importance to the substance of the information provided.

Google’s Privacy Policy is part of Google’s Privacy&Terms document. The document is not long. For key terms on the text, users can put the mouse on them and read examples and further explanations in a pop-up window. In case users want to learn more, they can click on the pop-up window. Apart from the Privacy Policy document, information on the data processing policies of Google are also provided in other links and pages,

both on Google’s Privacy&Terms page and other hyperlinks run by Google such as the Google Public Policy blog and the Google Blog.⁴²

Similarly to Google Services, information on data processing by Facebook can be found not only in Facebook’s Data Policy but also in other links, like Facebook’s Cookies Policy and Help Centre. At some points, the Data Policy document presents links on which the user can click and get further information.

Foursquare presents a summary of its privacy policy on “Privacy 101” page as well as a set of frequently asked questions related to privacy on a different link. WhatsApp’s Privacy Notice is brief and does not include any link to other pages.

Facebook offers the possibility to its users to opt-out from seeing on-line interest based ads.⁴³ Google also offers opting-out of interest based ads served by Google. Foursquare and WhatsApp does not offer any opt-out possibilities. Users can always opt out through initiatives like Your online Choices, an initiative of online advertising agencies that, though a website, provide information on online behavioural advertising and the opt-out possibility. ⁴⁴

---

Google Official Blog, [https://googleblog.blogspot.nl/](https://googleblog.blogspot.nl/) (accessed on 31/01/2016)
Chapter 3: The European Union’s legal arsenal

In the legal terrain, the European lawmakers, the Data Protection Authorities and generally the legal community faced the necessity of unraveling and understanding the technological mysteries and of reacting to the new challenges. How is the right to privacy understood towards the reality of smart mobile devices and mobile applications? Are the existing legal arsenal a shield against inroads in users ‘privacy? The present Chapter aspires to address these thorny issues.

3.1. The right to privacy and data protection on mobile applications terrain

Globally, the majority of the democratic societies officially recognize the right of individuals to enjoy an area of privacy.\textsuperscript{45} That area encompasses the right of individuals to keep secret parts of their lives, as well as their personal communications and information. From the wide span of the concept of the right to privacy and data protection, the dissertation presents only the lines that connect the mobile applications ecosystem with the privacy and data protection concerns.

Among the understanding of the right of a person to enjoy a private area, many parameters have been understood and conceptualized as the right to privacy. It has been shortly defined as "the right to be let alone" by Warren and Brandeis\textsuperscript{46}, while Roger Clarke writes that "Privacy is the interest that individuals have in sustaining a personal space, free from interference from other people and organizations".\textsuperscript{47}

\textsuperscript{46} Samuel D. Warren and Louis D. Brandeis, “The right to privacy” (1890) 4 HAR.L.REV. 193,220, available at \url{http://www.english.illinois.edu/-people-faculty/debaron/582/58220readings/right%20to%20privacy.pdf}
\textsuperscript{47} Roger Clarke “Introduction to Dataveillance and Information Privacy, and Definitions of terms” available at \url{http://www.english.illinois.edu/-people-faculty/debaron/582/58220readings/right%20to%20privacy.pdf}
As a part of the right to privacy, many legal orders recognize the right of individuals to control what information about them is communicated to other people. This idea has been conceptualized with the term “informational self-determination”. In this way, individuals can protect their privacy in a world where the possibility of collecting and processing personal information has been multiplied.

Mobile devices consist a “place” on which part of the private life of the users dwells and falls into the sphere of privacy protection exactly for that reason. It has been argued that mobile devices reality "has given birth" to a new perception of the right to privacy that could be understood as "the right to have at disposal a terminal programmed by default to minimize the data sent and received to the strict minimum needed for achieving the purposes pursued by its user.” Justice John Roberts, member of the Supreme Court of the United States, in the ruling on the case Riley v. California on warrantless search of digital information on mobile phones stated that "Modern cell phones are not just another one technological convenience, with all they contain and all they may reveal they hold for many Americans "the privacies of life". Modern technologies hide important threats for the private lives of individuals. The architecture of mobile devices, together with their utility make them more vulnerable towards "attacks against

---

48 This term was first used in 1983 by the German Federal Constitutional Court in the context of a ruling concerning the collection of personal information. The court ruled that "(… ) in the context of modern data processing, the protection of the individuals against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general rights of the German constitution". These rights entrench for individuals the right to control all the information about them. VerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

49 In its article “A taxonomy of privacy”, Daniel Solove categorized the activities that affect privacy. The first group of activities involves information collection. The second, the information processing. Two means of information processing can be the aggregation of information and the identification, meaning the linking of information to a particular individual. Data may also be processed, when it is provided for secondary use, videlicet the use of information for a different reason to which it was initially collected, without the data subject’s consent. The third group, consist of activities of dissemination of information. “Information dissemination activities all involve the spreading or transfer of personal data”. Finally, the fourth group, comprises activities that invade into peoples’ private affairs.

50 SERGE GUTWIRTH, YVES POULLET AND PAUL DE HERT, "Data Protection in a Profiled World" (Springer 2010) 27

51 SOUPREME COURT OF THE UNITED STATES, Riley v.California 573 US.(2014)
privacy”. A proper understanding of the threats is of utmost importance for the creation of a legal arsenal, effective in the specific circumstances and needs.

3.2 The EU legal framework

In the context of the legal order and academic research in the European Union, there is a tendency to treat data protection issues as part of the right to privacy, despite the fact that the Charter of Fundamental Rights of the European Union establishes an autonomous right for the protection of personal data in Article 8, separate from the right to private life that is established in Article 7. Along this line, the European lawmaker enacted the Data Protection Directive.

Moreover, the European Union’s legislative bodies have considered as necessary to enact a supplementary to the Data Protection Directive legal framework for the sector of electronic communications. The ePrivacy Directive is the successor to the Telecommunications Data Protection Directive and consists part of a large set of directives regulating the sector of electronic communications. The ePrivacy directive consists lex specialis to the lex generalis Data Protection Directive. The latter applies to the processing of personal data unless there is a provision in the first that indicates its own applicability.

---


53 Article 7 of the EU Charter stipulates that “Everyone has the right to respect for his or her private and family life, home and communications” while Article 8 of the same Charter states “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.”.

In the European Union's area, the Data Protection Directive constitutes a text-reference for the protection of personal data of the users and, internationally, it has been an example of high data protection standards. However, both the Data Protection and the ePrivacy Directives were adopted long ago, when the internet was quite different compared to its dimensions nowadays, and mobile applications did not exist at all.\textsuperscript{55} Currently, a General Data Protection Regulation that is going to succeed the Data Protection Directive is under negotiations between the EU legislative bodies. Given that the General Data Protection Regulation is expected to enter into force in spring 2018\textsuperscript{56}, the dissertation evolves on the legal framework formed by the Data Protection Directive.

\textbf{3.3 Elaboration on the legal framework and assessment}

The need for a thorough understanding of all the notions encompassed in the Data Protection and ePrivacy Directives is inescapable if the players in the field of mobile applications attempt to adopt a legally compliant behavior; nonetheless, the dissertation limits its focus on the study of the necessary notions for reaching conclusions on the research question and subquestions. The notions of “processing of personal data”, “personal data”, “data controller”, “establishment of the controller”, and “means of processing information” will shed light on whether the Data Protection and ePrivacy Directives are applicable and the requirements for a valid consent, stipulated on their provisions, should be respected by the developers of the examined applications.

\textbf{3.3.1. The concepts of “processing”, “personal data” and “data controller”}

\textsuperscript{55} SERGE GUTWIRTH, YVES POULLET AND PAUL DE HERT, "Data Protection in a Profiled World" (Springer 2010) 8
The conceptual limitations and therefore the applicability of the Data Protection Directive are mapped in its Article 2. In the scope of our research, those definitions are determinative in figuring out, whether the European legal framework is applicable when Facebook, Google, WhatsApp and Foursquare process personal data of their users.

In accordance with Article 2(b) Data Protection Directive “any operation or set of operations which is performed upon personal data” equals with “processing of personal data”.

Article 2 (a) Data Protection Directive stipulates that

“personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

Recital 26 of the Directive declares that,

“To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used by the controller or by another person to identify the said person ...”.

Nowadays, identification and identifiability are easily achievable, with the aid of the latest technologies. The information stored in the mobile devices are related either to owner of the device or to another individual (data subject). Users usually "sing in" the

---

57 Article 2 (d) Data Protection Directive “processing of personal data ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

58 Article 2(a) Data Protection Directive.

59 Recital 26 Data Protection Directive.

features of their devices by providing their names and e-mail accounts and tend to share more and more information online about themselves and their friends. Therefore, one may conclude that many types of data stored in mobile devices are related to an identified or identifiable person.

In its report on the definitive findings on the investigation into the processing of personal data for the WhatsApp mobile application, the Dutch Data Protection authority stated that,

“As far as WhatsApp users are concerned, WhatsApp has at least their mobile phone numbers at its disposal..... The mobile phone number is a personal data item because it is direct contact data item that anyone can use to identify a person directly or indirectly by taking intermediate steps. In addition, WhatsApp also has at its disposal the unique IMSI customer number, the unique IMEI device number or the MAC address of the iPhone of WhatsApp users. Without disproportionate effort, WhatsApp can link the data items to each other or, if necessary, take intermediate steps to trace the data subjects”.

The natural or legal person that decides for the purposes and means of the processing is named “data controller” (Article 2(d) of the Data Protection Directive). This

---

64 Article 2(d) Data Protection Directive “controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;”.

-28-
determinative role holds one more high responsibility. That of the compliance with the data protection rules. 65

Assessment

In view of the above and based on the findings (see 2.3.2 Privacy Policies and related documents), the examined apps (among other) access, collect, use and transfer, therefore process, under Article 2(b) Data Protection Directive, information that can identify a natural person and, subsequently, is considered as personal data under Article 2(a) of the Data Protection Directive.

It is worth underlining that despite the fact that Facebook, Foursquare and WhatsApp state what they consider as personal data in their Privacy Policies, the applicability of the law is determined by the definition of Article 2(a) of the Data Protection Directive and not by what each application developer considers as personal data.

Besides, the developers of the examined mobile apps are qualified as data controllers, as in their Privacy Policies, they determine the means and purposes of collection and processing of users' personal information.

3.3.2 Applicability of the Data Protection and ePrivacy Directives by the device and OS manufacturers and app developers

As long as the five examined applications process personal information of their users and qualify as data controllers the applicability of the Data Protection and ePrivacy Directives can be examined.

65 For instance, Article 6(2) of the Data Protection Directive on the principles relating to data quality, clearly states that “it shall be for the controller to ensure that paragraph 1 is complied with.”
3.3.2.1 The Data Protection Directive

In the context of our research, the fact that data subjects may reside in the territory of a state different to the residence of the data controller creates an element of international law that has to be spelled out.

According to Article 4 (1) Data Protection Directive,

“Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;
(......)
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for the purposes of transit through the territory of the Community”.

To begin with, it is worth mentioning that the protection afforded by the Article 4 of the Data Protection Directive is irrespective of the nationality of the data subject. The determinative factor is the location of the processing equipment on the territory of a European Member State.

---

66 Article 4 of the Data Protection Directive under the title “National applicable law”.  
67 ARTICLE 29 DATA PROTECTION WORKING PARTY, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites 5035/01/EN/Final WP ” 7.  
68 ARTICLE 29 DATA PROTECTION WORKING PARTY “Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union 5020/01/EN/Final WP 43”3 and LOKKE MOEREL “The long arm of the EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?” (2011) 1 International Data Privacy Law. The author underlines also that Article 4.(1).(c) of the Data Protection Directive applies also when the controller has establishments in the EU but its activities are unrelated to the processing of personal data.
As far as the subparagraph a, is concerned, the criteria that have to be examined-fulfilled are:

(a) Whether the data controller has an establishment in the territory of one of the member states.
(b) and whether the processing of personal data is carried out in the context of the activities of that establishment.

The notion of “establishment” has been a grey area and has been probed many times by the European Court of Justice, in the context of various cases. Recital 19 of the Data Protection Directive provides the explanation that “(...)establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements;(...)the legal form of such an establishment (...) is not the determining factor in this respect”.

For the second requirement to be addressed, the processing of personal data should be performed as part of the activities of the establishment of the controller in the territory of a Member State. The Article 29 Working Party has argued that three are the criteria that have to be comprehended and examined in each specific case; the nature of the establishment and whether it encompasses processing of personal data activities, the degree of the involvement of the establishment in the processing of personal data activities and, finally, the basic objective of the Directive that is the “effective protection of individuals” towards the processing of their personal data and that shall be taken into consideration as well.

69 CJEU C-33/78 Sinifar SA v Saae-Ferngas AG (1978) ECR 02183, “the concept of branch, agency or other establishment implies a place of business which has the appearance of permanency, such as the extension of a parent body, has a management and is materially equipped to negotiate business with third parties so that the latter, although knowing that there will if necessary be a legal link with the parent body, the head office of which is abroad, do not have to deal directly with such parent body but may transact business at the place of business constituting the extension”.
70 Recital 19 Data Protection Directive.
71 ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 8/2010 on applicable law WP 179"14.
72 Ibid.
For data controllers that do not have establishments in the territory of the European Union, subparagraph (a) cannot be applied. This entails the risk that data subjects in the territory of the European Union may be left unprotected. It might be easy and convenient for data controllers to reside outside of the EU and being absolved by the obligations the EU data protection law stipulates. The EU law maker needed to find a new connecting factor to subject data controllers residing in a third country to the provisions of the Data Protection Directive and avert the circumvention of the law. The equipment used by the data controller for the processing activities was selected as the connecting factor and consists a “physical link between the action (of processing) and (the territory of a Member State and its) legal system”.  

It must be pointed out that the word “equipment” used in the English version of Article 4(c) is different to that used in the other languages’ versions. The respective words in the versions of the Directive for the majority of the Member States is more similar to the English word “means”. On the semantic conflict that arises, the Article 29 Working Party has argued that the word “equipment” should be understood as “means”.  

Additionally, in order for Article 4(c) to be applicable, it is necessary that the data controller exercise control over the equipment as far as the collection and processing of data is concerned. The necessary control is satisfied when the data controller determines the way in which the equipment works and decides on the data collected.

---

73 In its decision C-131/12 Google Spain and INC v. Agencia Espanola de proteccion de datos and Mario Costeja Gonzalez, the Court states that the objective of the European Union legislation is to prevent individuals from being deprived of the protection guaranteed by the Directive and if we limit the territorial scope of the directive, this protection will be circumvented.

74 Recital 20 of the Data Protection Directive states that “the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive”.

75 ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites WP 56 ” 7.

76ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 8/2010 on applicable law WP 179” 20

77 ibid
and the purposes of the processing. The ownership of the equipment does not affect the control that may be exercised by the data controller over it. 78

The Article 29 Working Party has accepted that mobile devices satisfy the requirements of the notion of "means" under Article 4(c) of the DPD, “since the device is instrumental in the processing of personal data from and about the user...” 79; nevertheless, it stresses that the assessment can be different when data are processed only locally, at the device 80 Besides, in its report on the definite findings, the Dutch DPA asserts that WhatsApp uses the smartphones as a means of processing personal data” and accentuates that both the Data Protection and the ePrivacy Directive is imperative law. Unilateral declaration in the Privacy Policy of an application, even if it can be considered as accepted by the users, cannot exempt its application. 81

Assessment

In accordance with the Privacy Policies of the examined data controllers, Facebook Inc. 82 has headquarters both in the USA and in Europe (In Dublin, Ireland), while Google, WhatsApp and Foursquare have headquarters only in the USA. Facebook and Google also own national companies established in several European countries. 83

---

78 ibid
79 ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 2/2013 on apps on smart devices, WP 202" (2013) 7 and ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 13/2011 on geolocation services on smart mobile devices, WP 185" (2011) 12. However, LOKKE MOEREL “The long arm of the EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?” (2011) 1 International Data Privacy Law 38. The author argues that personal computers does not constitute “equipment situated within the EU”. He claims that “The personal computer of a user is under the control of the user rather than of the website. The website therefore does not actively “make use of equipment to collect data”
82 Facebook Inc. is the developer of the Facebook app.
83 Google Company Locations, https://www.google.com/about/company/facts/locations (accessed on 31/01/2016)
In the field of corporate law, headquarters are usually considered as the head offices of a company that are responsible for its overall management. The headquarters of Facebook are stable arrangements in the territory of Dublin. In its Privacy Policy, Facebook states that Facebook Ireland Ltd is the data controller responsible for the processing activities outside USA and Canada. The two requirements for the applicability of Article 4(a) of the Data Protection Directive seem to be satisfied and one may conclude that the Data Protection Directive is applicable by Facebook Ireland Ltd when it processes personal information of its users.

In its own initiative recommendation to Facebook, the Privacy Commission of Belgium reasons that Facebook Ireland cannot qualify as the only data controller for the processing of personal data of Belgian users. Facebook Inc. and not Facebook Ireland determines the means and purposes of processing personal data. It bases this argument on the details that Facebook provided to the Commission about the corporal structure of the Company. It concludes that the offices of Facebook on Belgium is a permanent establishment of Facebook Inc. on Belgium and that Belgian law that implements the Data Protection Directive is applicable.

As far as Google Inc., WhatsApp Inc. and Foursquare Labs Inc. are concerned, mindful of the Opinion of the Article 29 Working Party and of the Dutch Data Protection Authority, the dissertation considers that mobile devices should be qualified as equipment under the Article 4(c) and the Data Protection Directive should be applicable. In spite of the fact that different interpretations has been opined (see 79), the dissertation advocates the argument of the Article 29 Working Party and of the Dutch Data Protection Authority and for adding to their argument, the dissertation underlines that

85 PRIVACY COMMISSION OF BELGIUM, “Recommendation no. 04/2015 of 13 May 2015” relating to 1) Facebook, 2) Internet and/or Facebook users, as well as 3) users and providers of Facebook services, particularly plug-ins”(2015).
86 Google Inc., WhatsApp Inc. and Foursquare Labs Inc. are the developers of the Google Search and Google Maps, WhatsApp and Foursquare apps respectively.
apps are software installed in the mobile device. They interact with it through the API after the user has granted the permissions asked (see 2.1 Actors and their technologies). In this way, they control the processing activity on the mobile device of the user, what data are collected among the data stored on the device or generated by it, and for what purposes.

Facebook, Google, Foursquare and WhatsApp, as data controllers, must, consequently, comply with the obligations stemming from the Data Protection Directive.

Although by following the same argumentation, one can conclude to the applicability of the Data Protection and ePrivacy Directive when Apple and Google process personal data of their users, as manufacturers of the devices and developers of the OS and the apps’ stores, this is out of the scope of the present research. What is of utmost importance, is that device and OS manufacturers, as well the developers of the application marketplaces play a crucial role to the creation of the condition for the granting of a valid consent (see 2.1 Actors and their technologies). For that reason (also), they shall comply with the requirements of the Directives and facilitate the app developers to acquire a valid consent from the users.

### 3.3.2.2 The ePrivacy Directive

The applicability of the ePrivacy Directive is determined by its Article 3:

“This directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the Community”. 87

The question arises, whether mobile applications provide “publicly available electronic communication services” under the meaning of the ePrivacy Directive. The Article 29 Working Party has asserted that these services do not fall into the scope of the strict

---

87 Article 3 ePrivacy Directive
definition of "publicly available electronic communication services" and they are considered as information society services. The ePrivacy Directive does not apply in the processing activities performed by the mobile applications thereupon.

Nevertheless, despite the fact that information society services do not fall into the scope of the ePrivacy Directive, that is not the case for its Article 5(3) under the title “Confidentiality of Communications”. The latter applies to every entity that stores information or gains access to information already stored in the terminal equipment of

---

88 In its Article 2, under the title “Definitions”, Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive) states that a) “electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed; (…) (c) “electronic communications service” means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks; (d) “public communications network” means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services.


90 Even when such processing in performed via a public communications network.” ARTICLES 29 DATA PROTECTION WORKING PARTY, "Opinion 13/2011 on geolocation services on smart mobile devices, WP 185" (2011) 8, 9.

91 Article 5(3) ePrivacy Directive “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

the subscriber or user, regardless of its nature as information society service provider or electronic communication service provider.\textsuperscript{93}

The information stored in the terminal equipment does not need to be personal.\textsuperscript{94} Recital 24 of the ePrivacy Directive implies that the rationale under Article 5(3) is the intervention into the private sphere of the data subject (the terminal equipment and the information stored in that), rather than the nature of information as personal.\textsuperscript{95}

### Assessment

Having regard to the above, the examined apps as offering information society services “in (the territory of) the Community”\textsuperscript{96}, are excluded from the scope of the application of the ePrivacy Directive. Nevertheless, since they store and gain access to information that is stored in the device (see 2.3.2 Privacy Policies and related documents), Article 5(3) of the ePrivacy Directive applies and the requirements stipulated in it about consent must be satisfied.\textsuperscript{97}

#### 3.2.2.3 Location data- a category especially susceptible to interference threats

In the context of the ePrivacy Directive, the EU regulator stipulated specific provisions for the processing of location data.

Article 2(c) of the ePrivacy Directive states that location data are any data processed in an electronic communications network or by an electronic communications service

\textsuperscript{93} Article 5(3) of the ePrivacy Directive.

\textsuperscript{94} ELENI KOSTA, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013) 296.

\textsuperscript{95} ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 2/2010 on online behavioural advertising, WP 171” (2010) 8,9.

\textsuperscript{96} Article 3 ePrivacy Directive.

\textsuperscript{97} ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 2/2013 on apps on smart devices, WP 202” (2013)7,14.
indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.\textsuperscript{98}

Moreover, Article 9 (3) of the ePrivacy Directive says that:

\textit{“Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.”}\textsuperscript{99}

This choice implies that location data are considered to contain especial pitfalls against the privacy of the user; \textsuperscript{100} still and all, the ePrivacy Directive and, consequently, its Article 9 (3) do not apply on information society services.

The Article 29 Working Party has pronounced that location data always relate to an identified or identifiable person; hence, location data are always personal data and, when processed, Data Protection Directive is applicable. \textsuperscript{101} Generally speaking, this statement holds partly true\textsuperscript{102}; however, in the context of the highly individualized

\textsuperscript{98}Article 2(c)ePrivacy Directive. Recital 14 ePrivacy Directive stipulates that “ Location data may refer to the latitude, longitude, and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded”.
\textsuperscript{99}Article 9(3)ePrivacy Directive.
\textsuperscript{101}ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion on the use of location data with a view to providing value-added services WP 115”(2005) 3.
\textsuperscript{102}ELENI KOSTA, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013) 327 and COLLETE CUIJPERS AND BERT-JAAP KOOPS, “How fragmentation in European law undermines consumer protection: the case of location-bases services” (2008) 33 European Law Review 888. KOSTA argues that “This statement is correct insofar as location data are treated in the context of the ePrivacy Directive and are examined in compliance to the definition of Article 2(c) of the Directive.(..)Therefore location information that cannot be linked directly or indirectly to a natural person does not qualify as location data under the meaning of Article 2(c) of the Directive.” and CUIJPERS AND KOOPS opine that “(...)it is questionable whether this statement is correct, since location data can also related to objects that are not linkable to individual natural
mobile applications’ terrain, location data are personal data and the application of the Data Protection Directive is triggered.

**Assessment**

In the context of our research and according to the findings, all of the examined apps, except WhatsApp, collect and process location data (see 2.3.2 Privacy Policies and related documents). Google Maps and Foursquare are Location Based Services. Nonetheless, since apps provide information society and not electronic communication services, the strict prerequisites for the processing of location data provided in Article 9 (3) of the ePrivacy Directive are not applicable.

Given the highly individualized mobile ecosystem that makes easy and possible the identification or identifiability of a person, in the context of the present research location data are personal data and, as far as their processing is concerned, the Data Protection Directive is applicable.

### 3.3.3 Legal ground for the processing of personal data: Consent

According to Article 2(h) of the Data Protection Directive,

> “the data subject's consent shall mean any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”

Article 2(f) of the ePrivacy Directive says that “consent by a user or a subscriber corresponds to the data subject’s consent in Directive 95/46/EC”.

---

persons." CUIJPERS AND KOOPS present a figure with the relationship between personal, traffic and location data.

103 Article 2(h) Data Protection Directive.
104 Article 2(f) ePrivacy Directive.
In accordance with Article 7 of the Data Protection Directive the data controller needs a legal ground to process personal data.\textsuperscript{105} In the mobile applications ecosystem, the most commonly applicable legal ground is the consent of the data subject (Article 7(a)).\textsuperscript{106} Consent shall be provided unambiguously.\textsuperscript{107} Furthermore, Article 5(3) of the ePrivacy Directive states that the storing or the gaining of access to information in the terminal device of the user is allowed only after the user has given his consent \textit{“having been provided with clear and comprehensive information”}.\textsuperscript{108}

It can be concluded that the requirements for a valid consent under the Data Protection Directive and the ePrivacy Directive are overlapping and in practice, the two types of consent are merged.

Consent must be obtained before the storing or accessing of information. This has been an interpretation based on the wording of the Article 5(3) of the ePrivacy Directive.\textsuperscript{109} The same Article stipulates that consent is not required when the storing or the gaining access to information is strictly necessary for an information society service provider to provide a service explicitly requested by the user. This norm, consisting an exemption to the consent requirements, must be narrowly interpreted. The Article 29 Working Party interprets that the technical storage or access must be so necessary for the provisions

\textsuperscript{105} Article 7 Data Protection Directive stipulates that “Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with legal obligation to which the controller is subject or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).


\textsuperscript{107} Article 7(a) Data Protection Directive.

\textsuperscript{108} Article 5(3) ePrivacy Directive.

\textsuperscript{109} ARTICLE 29 DATA PROTECTION WORKING PARTY, ”Opinion 15/2011 on the definition of consent WP187“ (2011) 32.
of the specific functionality that the user has requested as if it is disabled, the functionality will not be available.\textsuperscript{110}

Consent must be freely given, specific and informed as well as an unambiguous indication of the data subject’s will. Indication can be any sign, understandable by the data controller that shows the wishes of the data subject. The Article 29 Working Party encourages data controllers to create the necessary tools so as to be able to prove that valid consent has been granted by users and, in particular, by the data subject.\textsuperscript{111}

Consent is related to the concept of informational self-determination and if it is properly used, it provides data subjects control over the processing of their data.\textsuperscript{112} Connected to the notion of control is also the right of the data subjects to withdraw their consent.\textsuperscript{113} Nonetheless, consent, if incorrectly used, instead of offering data subjects an actual control, it may lead to an illusion of it.\textsuperscript{114} Therefore, the prerequisites for a valid consent must be followed with fidelity by the data controllers.

\textbf{3.3.3.1 “….freely given...”}

The exercise of the data subjects ‘control over the processing of their personal data can be real only if it is their “genuine free choice” and “voluntary decision”\textsuperscript{115}. This means

\begin{footnotesize}
\textsuperscript{110} ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 04/2012 on Cookie Consent Exemption WP 194”\textsuperscript{4}.
\textsuperscript{112} ELENI KOSTA, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013) 220.
\textsuperscript{113} For more information see, ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 15/2011 on the definition of consent WP187” (2011) and ELENI KOSTA, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013) 251.
\textsuperscript{114} ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 15/2011 on the definition of consent WP187” (2011) 8,9.
\textsuperscript{115} “free consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological, or other (…)Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment” ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 15/2011 on the definition of consent WP187” (2011) 13.
\end{footnotesize}
that, in case the data subjects decides not to consent, they should not face important aftereffects. Practically put, when asked to give their consent for the processing of a specific category of data, users must be given the choice to give, or not give their consent. ¹¹⁶

In the mobile devices ecosystem, consent is freely given when end users have the choice to accept or refuse the processing of their personal data. The question arises, if in the case that refusal of consent equals the deprivation of the possibility to use the app, the consent can still be considered as freely given. One may think that in this case, the decision of users is not free, as it is leads to their exclusion of the use of the app. Recital 25 the ePrivacy Directive, clarifying the provisions about cookies and similar technologies states that, if the storage of a cookie by a website in the terminal device of the user is justified by a legitimate purpose, such as to facilitate the provision of the services, then access to the particular website can be refused, if users, after having been properly informed, do not give their consent to the storage of cookies. ¹¹⁷ An analog interpretation of this Recital for the case of the mobile applications can lead to the conclusion that, the accessibility to the application may be conditional on the granting consent by the users for the processing of their data, or better, of a specific category of


¹¹⁷ Recital 25 ePrivacy Directive “However, such devices, for instance so-called ‘cookies’, can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.”
data, if this process is justified on legitimate purposes. Consent can be considered as freely given in that case thereupon.\textsuperscript{118}

\subsection{3.3.3.2“….specific...“}

For consent to be specific, the data subject must be clearly and precisely informed about which data are processed and for what purposes.\textsuperscript{119} Therefore, for consent to be specific, data subjects must be properly informed.\textsuperscript{120}

It has been argued that consent should be limited to the processing of a specific data group and should not consist a general "green light" to the accessing and processing activities.\textsuperscript{121}

In its recommendations to the different players in the mobile apps field, the Article 29 Working Party has been in favour of granularity in the acquisition of consent mechanisms and it calls the players to work on it. Besides, a practical implementation of the right on informational self-determination requires that users are given the possibility to permit process on a specific category of their personal data and refuse access to another.

In this framework, users should be given the possibility not only to consent on the processing of a specific category of data, but also to opt-out of the processing for a specific purpose. Given the high privacy concerns connected to online behavioural

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{118} ELENI KOSTA, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013) 312.
\item \textsuperscript{120} ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 15/2011 on the definition of consent WP187” (2011) 17
\item \textsuperscript{121} Ibid.
\end{itemize}
\end{footnotesize}
advertising, data controllers are expected to have implemented opt-out possibilities at least for the processing of data for advertising purposes.\textsuperscript{122}

### 3.3.3.3 “….informed…” – Obligation of providing information (Article 10 and 11 of the Data Protection Directive)

Consent is informed when it is based upon knowledge by data subjects on the facts around the processing of their personal information and the consequences of refusing to consent. This information should be provided to users prior to the consent granting and should be based on \textit{“the reasonable expectations of the parties”}. \textsuperscript{123}

Articles 10 and 11 Data Protection Directive set the obligation of data controllers to provide information to the data subjects. This obligation is distinct but, in most cases intrinsically connected to the notion of informed consent. \textsuperscript{124}

Thereupon, when processing data, the data controller must mandatorily inform users about:

- (a) Its identity (who is legally responsible for the processing and its contact details, physical and electronic address)\textsuperscript{125},
- (b) what precise categories of personal data it processes and for what precise purposes (Article 10(a) and (b))

\textsuperscript{122} Opt out mechanism for sharing information for advertising purposes. The Article 29WP on its........ remarks that this system is an improving step however, it cannot be considered as valid consent. 'It cannot be conclude that users who have not objected to being tracked for purposes of serving behavioural advertising have exercised a real choice.


In the circumstances of mobile applications, it is considered that the data controller is obliged by Article 10(c), and it is necessary in order to make the consent informed, to provide additional information on whether data will be disclosed to third parties and on how users may exercise their rights. ¹²⁶

Before end users decide whether they consent on the processing of their personal data by an application, this information must be given to them through the application marketplaces. Likewise, it is necessary that this information is accessible after the installation within the app.¹²⁷ In both cases, it must be visible and easily accessible by the users and written in plain language, understandable by an average user of the audience the app is addressed to.¹²８

It has been a challenge to the data controllers to decide how much information needs to be provided to users, and not exceed the limits that would lead to the provision of an exaggerated amount of information, with the danger of misleading the data subject.¹²⁹ This decision becomes even harder in the context of mobile application, where data controllers have to face the additional challenge of the small screen.

3.3.4.4 “…unambiguously…”

For consent to be unambiguous (article 7(a) Data Protection Directive), the action of the data subjects must leave no doubt that consists a consent to the processing of their data.¹³⁰

¹²⁶ Ibid In addition to the above minimum scope of information, necessary in order to seek consent from the app user, the Working Party in view of fair processing of personal data strongly advises that the data controllers also provide to the users information on: [Symbol] proportionality considerations for the types of data collected or accessed on the device, [Symbol] retention periods of the data, [Symbol] security measures applied by the data controller.
¹²⁷ Ibid 23.
¹²⁸ Ibid.
Consent is an interaction between the data subject and the data controller, not easy to take place online. It is important that the means used for acquiring consent are the expectable and that controller make sure that the subject has actively and validly given his consent. Users must be provided with guidance about which exactly of their action signifies their consent.  

### 3.3.4 Layered information notices

Privacy and Data Protection organizations internationally prompt data controllers to provide users with the necessary information through layered privacy notices.\(^{132}\) The Article 29 Working Party in its Opinion 10/2004 on more harmonized information provisions elaborates on a model of three layers of information with the purpose of providing users meaningful and appropriate information and consequently enhance awareness on the data protection issues.\(^{133}\) The information that should be included in each layer will be further elaborated in Chapter 4 (see 4.2 Layered information and consent-granting-mechanisms).

**Assessment**

Evaluating the findings of the research in the light of the provisions of the Data Protection Directive for a valid consent has not been an easy task. There are a lot of parameters that should be examined. The most important are the way and time that the information is provided to the users, as well as the language used.

Summarising the findings, the language used during the installation procedure and in the Privacy Policy documents is generally plain without jargon. When permissions are

---


133 Ibid.
requested, users are informed about the category of data the application needs access to and the reason why access to the specific category is needed. On the page of the application in Google Play Store there is a link named “Permissions” where users can learn more on the permissions needed by the app. Full information on the data processing activities is provided in the Privacy Policies of each application, the link to which is presented on the page of the app on both Google Play Store and App Store. The information provided to the users covers the requirements of the Article 10 of the Data Protection Directive. Applications access personal information of the users stored in or generated by the mobile device for purposes of, among others, the provision of advertising services.

It is apparent that the examined data controllers attempt to interpret and apply the legal provisions. Nonetheless, the following concerns create doubts on whether the practices followed satisfy the requirements for a valid consent.

First of all, in no step of the downloading and installation procedure are data subjects clearly asked to give their consent to the processing of their personal data; when applications ask for permissions, they ask to be granted access to a particular category of data stored on the device without any explicit and specific reference to what data are actually collected and for what purposes. When investigated by the Office of Privacy Commissioner of Canada, Google, as the owner and overseer of Android OS, explained that “permissions are a security and transparency feature, and do not necessarily equate with functions that the App will, in practice, perform without further notice to the individual” and that “permissions are not ‘consent’ per se”. In other words, permissions is like opening a technical gate to the apps to access these categories of data. This does not equate to providing information about what data are collected and for what purposes. Permissions are not a notification on data processing and a call for consent granting.

134 In Android, this depends on the information that the application developer has provided. 135 Google Privacy Policy does not include the contact details of the data controller. 136 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, “Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA) PIPEDA report of findings #2014-008” (2014) 8,9.
The Canadian Privacy Office concluded that:

"As it currently exists, the Android permissions model is unclear. In particular, it is not clear that: (i) the permissions represented data and functions to which an app has access, and not necessarily its behaviors; (ii) the description provided for each permission does not necessarily describe the app’s actual use of that permission; and (iii) an individual should look elsewhere for a full description of an app’s actual collection, use and disclosure of personal information."

Secondly, the use of plain language does not mean that this information is always meaningful. In a survey conducted in 2012, a high percentage of the surveyed, after reading the Privacy Policy of Facebook and Google, could not understand how their information were shared by the applications and with whom. In the same survey, the surveyed found easier to understand a bank credit card agreement and a government notice than to understand Google’s and Facebook's Privacy Policies. Long documents, as that of Facebook does not guarantee that essential information is efficiently communicated to the end user. Succinct information should be provided. Phrases such us, "Foursquare may share..." undermine the satisfaction of the requirement for a specific and informed consent. Users are not able to understand whether and under what circumstances their data are shared. Terms that may not be a jargon but at the same time the average user is not expected to understand, like 'background location" are widely used. The language used to present the information and the respective ability of users to understand the meaning of the information is determinative for the exercise of the right of informational self-determination. A prove is that more than 30% of the surveyed-users of Facebook and Google, after comprehending the information included in the aforementioned Privacy Policies, planned to change the settings of their applications and being more circumspect in sharing information.

137 Ibid 13.
139 https://foursquare.com/legal/privacy (accessed on 03/02/2016)
140 Ibid.
Help Centre etc may be helpful to provide detailed information to the users, however they create the feeling that endless hours are needed to understand how their data are collected and processed, and this practice should be avoided. The information provided is not always comprehensive and coherent.

Opting out of the processing of personal information for the provision of interest-based advertisements is actually offered by no one of the examined applications. As far as Facebook is concerned, one may wonder whether opting out of "seeing online interest based ads from Facebook"\textsuperscript{141} equals opting out of the processing of the data for purposes of online behavioural advertising. From the wording of the information provided on Facebook’s Help Centre it seems more possible that users can opt-out only of the provision of interest-based advertising services. The same doubts arise of the wording used by Google. "You can opt-out of interest-based ads by Google...".\textsuperscript{142} When users opt-out are still their personal data processed for the purpose of providing interest-based ads? After all, Google and Facebook have interest in providing immediately online behavioural advertising services in case users change their decision and opt-in. Additionally, are personal information shared with third parties for the same purposes? Foursquare do not provide any opt-out possibility. As far as WhatsApp is concerned, based on the findings, it does not use information for advertising purposes. In this way users cannot specifically and freely decide and protect their personal sphere from interferences based on the tracking of their activities and on profiling. Yet, for Facebook and Google, their popularity results to them being important tools for many people’s everyday life and activities. This requires that first, further and clearer explanations are provided as far as what the opt-out possibilities mean and second, that alternatives are offered so as users are not excluded of using the services if they wish to opt-out of behavioural advertising.\textsuperscript{143}

\textsuperscript{141} https://www.facebook.com/help/164968693837950 (accessed on 03/02/2016)
\textsuperscript{142} https://support.google.com/ads/answer/2662922?hl=en (accessed on 03/02/2016)
Moreover, there are data processed by the apps that do not depend on a permission granted by the user, such as the information that users provide while using the app (e-mail address, posts, their location etc) (see 2.3.2 Privacy Policies and related documents). Users can learn about the processing of this category of information only if they read the Privacy Policy documents (the link to which can be found at the bottom of the page of the app in the application marketplaces). Reading a long Privacy Policy document to get informed about the processing procedures cannot be expected by the users. 144 Moreover, they are not notified about that processing neither before nor after they have installed the app on their devices. The European Court of Justice has asserted that offering a hyperlink that does not oblige users to read the entire text is insufficient.145 Therefore, the installation of the app should not be viewed as consent. Even if, hypothetically, information were provided to users before the installation, clicking the “install” button for Android and the respective icon for iOS, would equal a general authorization to the processing of personal data, which cannot qualify as specific consent 146

Finally, the fact that users actually use the application, without having been properly notified about the processing activities and without having been given the information that Article 10 Data Protection Directive provides for, does not consist an action indicating consent to the processing of personal data.

One may summarize that, in the aforementioned conditions, it is highly doubtful whether users can exercise their rights to informational self-determination and effectively protect their privacy. Information about the actual data protection activities are provided only in the Privacy Policy documents of the applications. One can be also dubious on whether the general presentation of information in those documents can create the conditions for a specific and informed consent to be granted. Users are never

actually asked to give their consent and the implementation of the recommendations of
the Article 29 Working Party and other Privacy authorities seem necessary in order to
create a veritable shield for the protection of the private sphere of the users.
Chapter 4: Paths to compliance

Each application has its particular characteristics and a particular context surrounding it. At the same time, there are many alternatives that a data controller could adopt to achieve compliance. Based on the particularities of each mobile app, a different alternative may be considered as the most appropriate. Data controllers, with the aid of expert legal advisors, hold the key to understanding the required conditions for a valid consent and adapt the particular characteristics of their applications to it.

Having consideration to the recommendations of the Article 29 Working Party\textsuperscript{147}, to the findings of the present research and to the provisions of the law, the dissertation proposes possible alternatives that could build the path to a valid consent, in the context of the present research. The following constitute indicative examples and alternatives and are certainly not the only pathways through which compliance can be achieved. Reconciling with the requirements of the Directives is not always easy to achieve, however app developers shall trigger their innovative capabilities, ask for the advice of expert lawyers or of the Data Protection Authorities and understand that protecting the privacy of users and building trust with them result to their own benefit as well.

\section*{4.1 Common responsibilities}

The terrain of mobile applications is based on the interrelationship of the actors involved. As has been explained in Chapter 2, the choices of one of the actors affect the others. It can be securely said that compliance can only be achieved with the cooperation of all the parties involved. As the Article 29 Working Party observes, the responsibilities of those parties under the European data protection legal framework usually overlap.\textsuperscript{148} Along this line and with the purpose of facilitating compliance with

\textsuperscript{147} ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 2/2013 on apps on smart devices, WP 202" (2013).

\textsuperscript{148} Ibid 27.
law and building trust with end users, device and OS manufacturers, application marketplaces, app developers and third parties should work together on:

- Providing to users meaningful, specific and adequate information before their personal information is being processed.
- Provide users tools of control.
- Create mechanisms needed so as to be able to prove that users have granted a valid consent.

The application of the privacy by design principle can facilitate the achievement of the above.

The role of the end user is equally determinative. It holds true that, in most countries, the majority of the app users do not read at all, or have a cursory glance to the Privacy Policies. One of the reasons is the length of these documents and this is generally understandable; nonetheless, users must be conscious, first, about the possible dangers hidden when their personal data are accessed and processed and, second, that by trying to get informed on the data processing activities of the data controllers is one of the most effective ways to, indirectly, force them to comply with the law and the only way to make mature decisions about the unveiling of their data. Users should realize that they are also one of the players in the mobile apps field; the most important one, to the protection of whom the legislation is aimed.

4.2 Layered information and consent-granting-mechanisms

With the view to provide users with shorter privacy notices, a system of three layers of information has been promoted internationally.\(^{149}\)

The first layer (short privacy notice) should include the information required under Article 10 Data Protection Directive, as well as information on the way users can exercise their rights and any other information that is considered as necessary for each particular case. When information is shared with ad companies, opt-out possibilities shall be presented in the first layer.\(^{150}\) This layer could be presented in the application marketplace, near the install button or icon, so as users read it before they decide to install the application. \(^{151}\) Alternatively, it could appear in a pop-up window after users click on installing the app.

The second layer (condensed privacy notice) should consist of the following:

- The scope of the application of the privacy notice
- Information accessed
- Purposes & disclosures to third parties
- Rights and options for the users
- Contact details
- Special requirements of the national law and, optionally, information on the national data protection authority.\(^{152}\)

The condensed privacy notice should appear if users clicks to learn more about privacy in the first layer.

The Privacy Policy of the app can be considered as the third layer (full privacy notice) that provides all the needed information in details. The full notice does not need to be adjusted to the requirements of a small screen. Two categories could be created about the data processed, the mandatory for the provision of the service and the optional. Mechanisms should be provided so as users can opt-out from the optional category. Additionally, when information is shared, users shall be informed on the identity of the


\(^{151}\) Ibid.

\(^{152}\) Ibid.
entities that their personal data are shared with. Data controllers must pay attention so that the full notice includes all national legal requirements and specifications. A solution can be a different full notice of each country where the services are provided. \[153\]

Each one of the layers shall provide the information needed at the particular point of time and circumstances for the user to make an informed decision. Cumulatively, the three layers shall satisfy the requirements of Article 10 Data Protection Directive. \[154\]

Information provided should be succinct and the language used should be simple and direct, so as to be meaningful to all people expected to use the app. On that line, the WhatsApp Privacy Notice can be an example. “In order to provide the WhatsApp Service, WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other users”; clear and direct language like this that describes, how data is processed, what data is processed and for what purposes holds the attention of the user focused on the notice. App developers can play with the colour or add icons to put emphasis on, for instance, information processed that may be unexpected by the end user. It is useful that the same language and expressions are used in all the layers.

Attention should be paid to the requirement for a granular consent. \[155\] This can be possible through the permissions mechanism. Nevertheless, as has been explained in Chapter 3 (see 3.3.3 Legal ground for the processing of personal data - Consent) permissions do not consist per se a consent granting mechanism. \[156\] A solution could be that apps ask for permission strictly only in the case that they use it and they give more information on the processing (data, purposes and identity of the data controller) asking clearly the consent of the users. Following when the users are asked to grant permission the pop-
up window should include a clear reference that granting permission means consenting
to the processing of personal data.

A specific and informed consent requires the notification of the users, in case the Privacy
Policies are modified by the app developers. WhatsApp’s practice that calls users to
revisit the website in order to stay aware of any changes cannot be accepted. Google
provides an exemplary archive where the old versions of the Privacy Policies are kept.
The points that have changed are marked.

App developers can build various communication canals with their users. Blogs, for
instance, that allow direct communication between users and the data controller can be
proven mutually beneficial. Users can ask their questions and get immediate and
concrete answers on privacy issues.

Data controllers should realize that the Privacy Policies are like a Charter for the data
processing activities. Whatever they write or omit to write in that Chapter creates
responsibilities for them.

Yet, Privacy Policy documents should be named in a way that calls users attention on
that personal data are processed by the app. For instance, the title “Data policy” implies
that the document refers to the data processing policies. In contrast the title “Privacy
Policy” resembles a safety statement and brings in mind the idea that privacy is
protected and may quell the interest of the users.

4.3 Tools of control

Both OS offer their users the possibility to withdraw a permission that has already
granted to an app. This practice is endorsed and encouraged; howbeit, given all that has
been analyzed above concerning permissions (see 3.3.3 Legal ground for the processing of

personal data- Consent), a withdrawal of permission is not a withdrawal of consent. The right to privacy, understood as a right to informational self-determination, should guarantee users not only the possibility to give their consent, but also to modify and withdraw it anytime. Consequently, the present system of controlling permissions should be complemented by a feature that provides control over the granting, modifying and withdrawal of consent over the categories of data actually processed by the applications. A reasonable period of time after users has granted consent, they should be reminded that several categories of their data are processed. Users could potentially choose how often they wish to be reminded.

Google Services have developed a Dashboard where users can have an overview of their recent activity with regard to Google Services and manage their product settings. This Dashboard could be the right beginning and it could be supplemented with information about what data are accessed, in the context of which activities and how these data are used. Google has also developed an application, pre-installed in Android devices named “Google Settings" that offers users control on their Google account. Through these settings users can opt-out of several processing activities, learn more about those activities and change the setting on the environment of each application. Through those interfaces users could also be given the possibility to decide, up to a certain extent, on the retention periods for their personal data. This system could also give users an easy way to manage and refuse updates and deactivate or delete an app.

It is necessary that the consent is granted by the data subject and not by someone else accidentally or periodically using the device. Request for a password before consent is requested could constitute an efficient solution. The relevant practice adopted by the App Store is encouraged (see 2.3 Current Practices).

4.4 Structure of the Policies

Facebook is an exemplary of clearly structured Privacy Policy document. The general categories are divided into subcategories. Different categories are presented with
different colour and accompanied by a different sign. That way, users can read the
document more easily and without intermittent attention

It can be said that Google Services Privacy Policy is an exemplary on the line of providing
layered information to users. Nevertheless, this practice is different to that discussed
above (see 4.2 Layered information and consent-granting-mechanisms) for the three
layers of privacy notices recommended by the Article 29Working Party and cannot be
considered as an alternative to it.
Chapter 5: Conclusion

The assessment of the findings in the light of the legal framework formed by the Data Protection and ePrivacy Directives concludes that the information stored in or generated by mobile devices is personal, as, given the intimate connection of mobile devices to their users, in the majority of the cases it is linked to an identified or identifiable person.¹ These data are processed by the examined application. The developers of the examined applications determine the means and purposes of accessing and processing this information and enunciate them in their Privacy Policy documents, qualified that way as data controllers.

Facebook Ireland Ltd shall apply the provisions of the Data Protection Directive. Its headquarters in Ireland (that is a Member State of the European Union) is the data controller for the processing activities connected to data collected in the Territory of the European Union. Google, WhatsApp and Foursquare fall also under the scope of applicability of the Data Protection Directive, given that mobile devices are considered as means used by the data controller (Google Inc., WhatsApp Inc. and Foursquare Labs Inc.) for the collection and processing activities. On the other hand, the strict definitions of electronic communication services in the ePrivacy Directive exclude its applicability in the examined cases and, as far as location data are concerned, they are protected as personal data. All the actors examined in the present research are considered to be offering information society services. Applicable is, however, the Article 5(3) of the ePrivacy Directive. The applicability of the latter extends to information society services when they stores data and/or obtain access to data stored in the terminal equipment of the user. The apps, as such, are software stored in the device and they have access in information stored in the same device. Therefore, Facebook, Google Services, Foursquare and WhatsApp must ask for the consent of the user before the respective they access their data.

The prerequisites for a valid consent under the ePrivacy Directive overlap with those under the Data Protection Directive. Consent, under the latter, consists one of the legal
grounds for the processing of personal data and must equate with a freely given, specific and informed, unambiguous indication of the wishes of the data subject. A well informed user can create genuine and mutually beneficial dialogue with the app developers, “asking them” that way compliance with the law in return for trust and loyalty.

The conditions for a valid consent can be created only with the collaboration of the app developers with the device and OS manufacturers and the app stores. Presently, despite the fact that both Android and Apple have improved their OS and app marketplaces on the direction of providing more information and control to the users, it can be said that, mainly because of the non-easily accessible and non-adequate information provided to the users, it is questionable whether valid consent for the processing is acquired.

The Article 29WP as well as the privacy authorities of Canada and the United States of America have issued detailed recommendations with the purpose of facilitating app developers to create the tools for achieving compliance with the law. The final result must safeguard the balance of the legitimate rights of all the parties involved.

Data controllers are called upon to apply their technical and entrepreneurial innovative skills and to build mechanisms able to overcome the challenges of the mobile applications ecosystem. An open dialogue with users, consumer unions and Data Protection Authorities can guarantee transparent and effective solutions awarded by the acceptance and preference of the users.
Bibliography

Treaties and Directives


Case Law


Investigations by Data Protection Authorities


PRIVACY COMMISSION OF BELGIUM, “Recommendation no. 04/2015 of 13 May 2015” relating to 1) Facebook, 2) Internet and/or Facebook users, as well as 3) users and providers of Facebook services, particularly plug-ins”(2015).

Opinions, Recommendations and Working Documents of the Article Data Protection Working Party and Recommendations of other Data Protection Authorities

ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 02/2013 on apps on smart devices, WP 202" (2013).

ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 04/2012 on Cookie Consent Exemption WP 194” (2012).


ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 8/2010 on applicable law WP 179” (2010).
ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 2/2010 on online behavioural advertising, WP 171" (2010.)


ARTICLE 29 DATA PROTECTION WORKING PARTY, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites WP 56" (2002).


Books

GUTWIRTH S, POULLET Y AND DE HERT P, "Data Protection in a Profiled World" (Springer 2010)

KOSTA E, “Consent in European Data Protection Law” (Martinus Nijhoff Publishers 2013)

Articles

CLARKE R, “Introduction to Dataveillance and Information Privacy, and Definitions of terms” available at http://www.english.illinois.edu/people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf


Surveys


Online sources


"What are mobile device identifiers", https://www.aerserv.com/mobile-device-identifiers/ (accessed on 19/12/2015)


http://techscience.org/a/2015103001/ (accessed on 19/12/2015)

Appendix

Figure 2 Nexus 7 mobile device on which the research was conducted
iOS 9.2
Your software is up to date.

Figure 1 iPhone 5 on which the research was conducted
Figure 2 Available information on Google Play Store
Figure 3 Permissions’ details pop-up window on Google Play Store
Figure 4 New permissions' system on Android Marshmallow 6.0.1
Figure 5 Facebook mobile app asking for permissions on Android Marshmallow 6.0.1
“Facebook” Would Like to Access Your Photos
This allows you to share photos from your library and save photos to your camera roll.

Don’t Allow      OK
Figure 7 Facebook mobile app asking access to location services on iOS 9.2
Figure 8 Privacy Settings of iOS 9.2

As applications request access to your data, they will be added in the categories above.
Figure 9 Settings of iOS 9.2
Figure 10 Location permissions on Android Marshmallow 6.0.1
Figure 11 Google Maps Application permissions on Android Marshmallow 6.0.1