The protection of Personal Data in Mobile Instant Messaging applications for mobile devices

Candidate number: 8023
Submission deadline: 1 March 2015
Number of words: 17,865
# Table of contents

1 INTRODUCTION ........................................................................................................................................ 1

1.1 Legal questions and problems considered ......................................................................................... 5

1.2 Delimitation of the scope of the thesis ................................................................................................. 6

1.2.1 Applications for smartphone: A framework of contracts ......................................................... 7

1.3 Legal Method ...................................................................................................................................... 8

1.4 Definitions of the core concepts .......................................................................................................... 10

1.4.1 Privacy ........................................................................................................................................ 11

1.4.2 The proportionality principle ....................................................................................................... 11

1.4.3 The theoretical concept of consent ................................................................................................. 12

1.5 Overview of chapters .......................................................................................................................... 15

2 THE CRITERION OF CONSENT OF THE DATA SUBJECT IN THE EUROPEAN LEGISLATION AND THE WHATSAPP CONTRACT TERMS AGREEMENT .......................................................................................................................... 16

2.1 Introduction ....................................................................................................................................... 16

2.2 The principle of consent in the European legislation ......................................................................... 17

2.3 The role of consent on mobile devices ................................................................................................ 22

2.4 Consent and the Privacy Policy of WhatsApp ..................................................................................... 24

2.4.1 WhatsApp and its Quasi-Social Network features ....................................................................... 26

2.4.2 The access of WhatsApp to the users' phone contacts: Is it legitimate? .................................. 29

2.4.3 The vague clauses of WhatsApp Privacy Policy that undermine the protection of personal data ................................................................. 34
2.4.4 In the event or Merger, Sale, or Bankruptcy ........................................... 35

3 MIM APPLICATIONS AND THE FLOW OF PERSONAL DATA TO COUNTRIES OUTSIDE EUROPE ................................................................. 37

3.1 Introduction............................................................................................................ 37

3.2 The concept of adequate protection of personal data and the differences between Europe and US ................................................................. 39

3.3 The concept of transfer ...................................................................................... 41

3.4 Applicable law .................................................................................................... 43

3.5 The transborder data flow in the WhatsApp contract terms agreement ............... 48

4 CONSENT IN THE ERA OF INTERNET, STILL AN ACT OF SELF-DETERMINATION? ........................................................................................................................................ 49

4.1 Introduction............................................................................................................ 49

4.2 Data subject and the spontaneous disclosure of personal data, the Privacy Paradox . 50

4.3 The mechanism of consent-gathering: How the lack of meaningful choice influence the will of subjects ........................................................................................................... 51

4.4 Privacy policies and their inefficacy to protect personal data .............................. 53

4.4.1 The difficult understanding of privacy policies .............................................. 53

4.4.2 The inflation of privacy notices and the consent desensitisation ................. 55

5 MIM APPLICATIONS AND THE CRISIS OF CONSENT IN THE ONLINE WORLD: THE POSSIBLE SOLUTIONS IN LIGHT OF THE PROPOSED GDPR ........................................................................................................ 56

5.1 Privacy by design and privacy by default ............................................................ 56
5.2 The concepts of the proposed GDPR that might influence the protection of personal data in MIM applications
......................................................................................................................... 58
5.2.1 Consent in the proposed GDPR........................................................................................................... 58
5.2.2 Privacy by design and privacy by default in the proposed GDPR .......................... 58
5.2.3 The consequences of the proposed GDPR on the transborder data flow ...... 59

5.3 The crisis of consent: Would Privacy by design and privacy by default be the best solution?
......................................................................................................................................................... 60

5.4 The crisis of consent: Possible solutions ................................................................................................. 62

6 CONCLUSION ........................................................................................................................................... 65

BIBLIOGRAPHY ......................................................................................................................................... 68
1 Introduction

In the latest years, changes in technology and the diffusion of smartphones, that use the mobile Internet connection to deliver services, increased the amount of personal data that are being processed. These mobile devices, changed the existing relation between online and offline world. Nowadays we do not go online. Applications for smartphones (apps) are constantly connected to Internet to perform their functions. Thus there is a conflation between online and offline\(^1\) world. Moreover mobile applications have a more user friendly and immediate interface compared to a computer browser. This implies that users that connect to Social Networks (hereinafter SNs) via smartphones are more active than those that use a normal computer\(^2\).

Mobile text messaging is shifting from the Short Message Service (SMS) that is becoming obsolete, to Mobile Instant Messaging (MIM) applications. The new technology allows a broader range of functionalities. Furthermore MIM applications can interact with other applications installed on the users' device to facilitate socialization and sharing. These features place MIM applications half way between a text service and a SN.

A SN is a platform where users build up their own profile to interact with each other, maintain existing personal relations and establish new ones\(^3\). The popular application

\(^{1}\) Svantesson Dan Jerker, Extraterritoriality in Data Privacy Law (Ex Tuto Publishing,
\(^{3}\) Chbeir Richard, Al Bouna Bechara, Security and Privacy Preserving in Social Networks (Springer 2013) p.6
WhatsApp run from WhatsApp Inc. (hereinafter WhatsApp) while apparently consists and is designed as a free Internet alternative to SMS, have features typical of a SN.

For the purpose of this thesis WhatsApp will be considered as a quasi-Social Network (QSN). This because WhatsApp, and the most used MIM applications, enables users to create a profile with a profile picture and a status message. Moreover WhatsApp give users the possibility to create chat groups. Chat groups might include also subjects that are not in the address book of the recipient's device. Thus WhatsApp give users the possibility to establish new relations through existing ones. Despite these features the company that run WhatsApp does not provide a clear informative to users. The homepage of the company describe the software as a "simple real time messaging" application. This definition may mislead users. This because the latters cannot imagine the other functionalities, as the QSN features, that involve the processing of personal data. Undoubtedly the features that a MIM service offers are much more limited in comparison to a pure SN. Nevertheless these applications create a flow of personal data on the Internet not foreseeable from users/data subjects that download the MIM application for the first time.

The constant growth in popularity of MIM applications raised the attention of Europeans' Data Protection Authorities (DPAs) on the impact that the use of MIM services could have on the privacy of data subjects. The activities of WhatsApp have been concerning the DPAs of Netherland, Germany and Italy. Critics mainly referred to the non-compliance with the principles in personal data protection laid down in the Data Protection Directive 4


95/46/EC (DPD)\(^6\). In particular the Dutch Data Protection Authority issued a Report\(^7\) in which the main flaws of WhatsApp in complying with the rules of the Dutch Data Protection Act [Wet bescherming persoonsgegevens] are analyzed.

From the point of view of WhatsApp that is an US based company, users/data subjects by giving consent to its Privacy Policies\(^8\), abide to the processing of his/her own personal data from the company.

However consent\(^9\) of the data subject to be considered validly given shall fulfill the requirements of being unambiguous\(^10\), freely given\(^11\), specific\(^12\) and informed\(^13\). Moreover the presence of consent does not indemnify the company from the other legal obligations enshrined in the DPD. A user/data subject is also a consumer from a commercial contract law perspective. The subscription of a MIM service from a user is a contract concluded by electronic means. Thus the regulation concerning consumer protection intertwines with the protection of personal data\(^14\).

\(^6\) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
\(^7\) Dutch DPA Report (n 4)
\(^9\) Article 7(a) DPD
\(^10\) ibid
\(^11\) Article 2(h) DPD
\(^12\) ibid
\(^13\) ibid
\(^14\) Svantesson (n 1) at 61
The fact that consumers waive substantial rights when they enter into contracts is nothing new. Subscribers of a MIM service pursue two different interests. One attain to the social sphere and consists of being part of a particular network, the other is economical and concern the economic advantage for users avoiding the fees on SMSs. Consumers when are giving consent to the processing of personal data do not foresee the possible future implications but the immediate benefits. This phenomenon has been described as Privacy Myopia\textsuperscript{15} and theorizes that the biggest threat for personal data are the data subjects. In the world there are different perceptions regarding what it constitute the right of data protection. While the European legislation have a more paternalistic approach and try to fill in the gap caused by the Myopia of consumers, other legislations, such as the in the US, place more emphasis on the free will of the subjects\textsuperscript{16}.

In February 2014 WhatsApp has been sold to Facebook Inc. (hereinafter Facebook), raising concerns, both in EU and in the US\textsuperscript{17}, on the possibility that there could be an aggregation of the personal data collected from the two companies. The risk is that the personal data so collected would be used to create highly detailed profiles of customers/data subjects. This renewed the concerns of European DPAs on the transborder data flow from Europe and US.

In this thesis will be considered how MIM applications challenge the European Data Privacy legislation and the role of consent of the data subject. Moreover will be analyzed how the criterion of consent function and if it can properly safeguards the privacy rights of

\textsuperscript{15} Froomkin Michael, \textit{The Death of Privacy}? (Stanford Law Review, 2000 Vol 52:1461) p.1502


data subjects. Thus will be considered the risks for Data Privacy Law due to an overreliance on consent. In light of the proposed General Data Protection Regulation\textsuperscript{18} (GDPR), will be valuated if concepts as privacy by design and privacy by default might be final solution for the protection of personal data.

1.1 Legal questions and problems considered

In light of the investigation on WhatsApp of the Dutch DPA\textsuperscript{19} will be analysed which risks MIM applications poses for the protection of personal data. Central relevance will be given to the role of consent, the principles enshrined in the DPD that relate to it and the legitimization procedure for the processing of personal data.

The analysis will critically discuss the criterion of consent in order to highlight its strengths and weaknesses in the online environment. The proposed GDPR\textsuperscript{20} introduce the concepts of privacy by design and privacy by default in the regulation on data processing. These concepts foster the idea that the embedding of data privacy laws directly into the architecture of the hardware/software might increase the level of protection of personal data processing. In Chapter 5 these features will be considered more extensively when will be canvassed which possible scenarios would arise if the proposed GDPR will be adopted. Additional consideration will be placed on the impact that the GDPR might have on MIM applications and the data flows between Europe and US.

\textsuperscript{18} Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012/0011/ (COD)

\textsuperscript{19} Dutch DPA Report (n 4)

\textsuperscript{20} Article 23 GDPR
1.2 Delimitation of the scope of the thesis

MIM applications raise several legal questions concerning the protection of personal data. Since that many companies running MIM software are based in the US will be taken in consideration the transborder data flow from Europe to US and the role of the Safe Harbour Programme. Due to the scope of this thesis will not be discussed the flow of data between Europe and US in general terms, but only in relations to the personal data transferred by MIM applications. The relation between the proposed GDPR, and its influence on the Safe Harbour Programme will also be discussed only to highlight the consequences of the implementation of privacy by design, privacy by default and stricter requirements on the consent of the data subject.

WhatsApp raised many concerns regarding the security of personal data since that the encryption software used to anonymize personal data have not been considered adequate\textsuperscript{21}. Both the DPD\textsuperscript{22} and the new GDPR\textsuperscript{23} state that processors of personal data shall implement appropriate, technical and organisational measures to ensure an appropriate level of security. However a discussion on the risks of security breaches and the possible technological solutions would need a deeper insight of technical issues that fall out from the scope of this thesis\textsuperscript{24}.

Applications for smartphones often use the geo-localization systems embedded into mobile devices to deliver their services. Nonetheless that MIM applications may also take advantage of this systems, this feature will not be analysed in this thesis. This because the

\textsuperscript{21} Dutch Data Protection Authority (n 4) pp.25-26  
\textsuperscript{22} Article 17 DPD  
\textsuperscript{23} Article 30-31-32 GDPR  
\textsuperscript{24} For an overview over the security of personal data, see Wong Rebecca, Data Security Breaches and Privacy in Europe (Springer 2013) Chapters 3-6
main focus of this thesis is on the consent of data subject and the problematic of its effectiveness\textsuperscript{25}.

1.2.1 Applications for smartphone: A framework of contracts

Applications for smartphones usually are purchased and downloaded from Online Stores. These are run from the company that own the Operating System (OS) of the respective device. Users to access these stores have to accept their privacy policies. These companies as e.g. Google and its store Google Play provide many services that systematically fail to make available concise and omni-comprehensive privacy policies for so many services\textsuperscript{26}. Thus is difficult for users/data subjects to understand how the personal data are processed.

The privacy policies of the online store do not cover the downloadable applications for smartphone and each application has a separate privacy policy\textsuperscript{27}. Due to the heterogeneous nature of applications for smartphones a sole privacy policy is not feasible. An omni-comprehensive privacy policy would be hard for users to understand. Moreover will not be tailored on the purpose of the data processing of the single application. Moreover it would cause uncertainty on the company that shall be deemed to be liable for damages due to data breaches or data losses.

\textsuperscript{25} For an overview on geo-localization equipment on smartphone, see King Nancy J. \textit{When Mobile Phones are RFID-Equipped- Finding E.u.-U.S. solutions to protect consumer privacy and facilitate mobile commerce} (Michigan Telecommunications and Technology Law Review, 2008 Vol 15 No 1:107)

\textsuperscript{26} Schwartz Paul M. \textit{Information Privacy in the Cloud} (University of Pennsylvania Law Review, 2014 Vol 161:1623) p.1696

The online stores and the developers of applications are in a business-to-business contract, while users/consumers are in a two-tier of contracts. The first level is a contract with the Online Store. The second level is a contract with the companies that develop the applications.

MIM applications use the infrastructure of third parties to be able to deliver their service, thus personal data are materially hosted and processed from third parties. The legal issues that arise then are not different from the legal challenges posed from Cloud Computing. Viber, a competitor of WhatsApp, store the personal data on server owned by Amazon Web Services LLC\textsuperscript{28}. Viber in this case operates as Software as a Service (SaaS) while Amazon as an Infrastructure as a Service (IaaS)\textsuperscript{29}.

The thesis will only consider the contractual relation between companies that run MIM applications and final users. This because the main scope of this research is to analyse whether consent of the data subject provide a proper protection to personal data in the relation between users and MIM companies on which is placed the duty to comply with data privacy law.

1.3 Legal Method

Primarily this thesis will focus on the processing of personal data of EEA citizens from MIM applications. Therefore the legislative instruments considered are mainly European. However, articles, cases and legal perspectives will be taken both from Europe and US.


\textsuperscript{29} Millard Cristopher Cloud Computing Law (Oxford University Press, 2013) p.4
The opinions of the Article 29 Working Party (hereinafter A29WP) will be used to analyse the legal issues discussed. The A29WP is an advisory board composed "of a representative of the supervisory authority or authorities designed by each Member State"[^30], have an advisory status and act independently. Therefore its interpretation of the DPD has a non-binding nature. However its influential nature is clearer in the proposed GDPR, where the content of the opinions of the A29WP have been included in many recitals[^31].

Investigations and recommendations from the Federal Trade Commission agency (hereinafter FTC), a US regulatory agency, will also be taken in consideration. The FTC is an independent federal agency, dedicated to consumer protection that covers the role of a European DPA. The FTC has more limitations than a DPA, its jurisdiction is not extended over all companies and its way to enforce decisions concentrates on a mechanism based on notice and choice[^32]. However the FTC might apply penalties to companies involved in misleading business practices far beyond the sanctions that are available to European DPAs[^33].

The proposed GDPR taken in consideration for this analysis is the European Commission draft issued the 25 of January 2012. The content of the future regulation is still uncertain,

[^30]: Article 29(2) DPD
[^33]: Bygrave (n 16) p.111
and its text has been amended from the European Parliament in the legislative resolution of 12 March 2014\textsuperscript{34}.

1.4 Definitions of the core concepts

New technologies have been challenging the protection of personal data. This because on one side the existing laws have been conceived in a time when could not be foreseen the effect of the development of the online world. On the other side data subjects compare offline experiences to the online ones and expect to have the same level of protection. Nonetheless Internet faded away the borderline between these two worlds\textsuperscript{35}.

The provisions listed in Article 7 DPD set out the criteria that legitimate personal data processing. However the structure of the DPD place the criteria of Article 7 DPD as complementary of the principles related to data quality listed in Article 6 of the DPD\textsuperscript{36}. Consent of the data subject is one of the precondition for the processing of personal data, but not the sole precondition.\textsuperscript{37} In light of this, consent of the data subject needs to be considered in the frame of the other principles of the DPD. In the following sections of this Paragraph relevant concepts for the analysis will be framed within the scope of this thesis.

\begin{quote}
\end{quote}


\textsuperscript{36} Korff Douwe, Data protection Laws in the European Union (Direct Marketing Association, 2005) p.38

\textsuperscript{37} Bygrave (n.16) p.161
1.4.1 Privacy

Privacy is a concept difficult to define; its nature might vary depending of the social and legal background of a country. Privacy is enshrined in Article 8(1) of the European Convention for Human Rights and Fundamental Freedoms (ECHR)\(^{38}\). The right to privacy as stated in the ECHR Article 8 implies the right to protect individual's own sphere from interferences, or "the right to be left alone". Formally in the European legislation the right to privacy of individuals and the right to data protection seems to be two different things. However privacy and data protection intersect and at certain extent overlap\(^{39}\).

For the purpose of this thesis the concept of privacy that will be used is of "informational privacy"\(^{40}\) that refer to the information collected on individuals. Privacy as data privacy means the right to control what is known about you. More specifically privacy in this meaning is the right for individuals to determine when, how and to which extent information about them is communicated to the others\(^{41}\).

1.4.2 The proportionality principle

The proportionality principle is a general principle of European law. This status of an overarching principle influences the application of the DPD. The proportionality principle

\(^{38}\) European Convention for Human Rights and Fundamental Freedoms available at \(<\text{www.echr.coe.int}>\) accessed 18 September 2014  
\(^{41}\) Bygrave (n 16) p.24
pervades and co-exists with ordinary laws and is applicable to a vast number of different cases\textsuperscript{42}.

Conventionally the proportionality principle is divided in three parts: suitability, necessity and non-excessiveness\textsuperscript{43}. The proportionality principle applies to the provisions regarding the requirements that legitimate the processing of personal data. For the purpose of this thesis, the proportionality principle will be considered to investigate the behaviour of MIM companies. Therefore the criteria of necessity\textsuperscript{44} and non-excessiveness\textsuperscript{45} will be used to assess whether the kind and the amount of personal data collected from MIM companies is justified from the need to perform the contract company-users.

1.4.3 The theoretical concept of consent

The concept of consent is indissolubly connected to the concept of privacy\textsuperscript{46}. Function of consent is the right to exclude from a person's life any interference unless there is a "free, voluntary and undeceived consent and participation"\textsuperscript{47}. John Stuart Mill defined consent as an act of self-determination and expression of autonomy that reveals the decision to disclose personal data to a private or a public processor. Therefore consent generates a

\textsuperscript{42} Harbo Tor-Inge, \textit{The Functionality of the Proportionality Principle in EU Law} (European Law Journal, 2010 Vol. 16 No. 2:158) p.168
\textsuperscript{43} Bygrave (n 16) p.148
\textsuperscript{44} Article 7(b) DPD
\textsuperscript{45} Article 6(1)(c) DPD
\textsuperscript{46} Except those cases in which the invasion of privacy is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country. Article 8(2) ECHR
\textsuperscript{47} Mill J.S., \textit{On Liberty} (Yale University Press, 2003) p.82
permission that allows actions that would be considered wrongful otherwise\textsuperscript{48}. Data subjects through consent authorise processing mechanisms and is fundamental that this authorisation is given due to a clear and affirmative choice of the data subject\textsuperscript{49}.

John Mill's era was different from the present. It belongs to the offline world where consent was the instrument to protect individuals from tangible intrusions. Nowadays, data subjects face bigger challenges due to the fading away of the distinction between offline and online world. The intangibility of the intrusions in the private sphere makes for data subjects more difficult to properly understand which are the real consequences of giving consent to data processing.

In the online world the authorisation through consent is forced within a certain limit. Customers/data subjects that wish to use a service have to consent to complex privacy policies that aim more to protect companies and fulfil their interest than the interests of the data subject\textsuperscript{50}.

MIM applications are usually very cheap or free of charge and they are marketed as a way to save money and to connect with other people. Therefore data subjects have the tendency to think that in exchange of their personal data they would improve their own conditions both from an economical perspective, saving SMSs' fees, and from a social perspective, increasing the numbers of their friends.

\textsuperscript{48} Schermer Bart W. et al., \textit{The crisis of consent: how stronger legal protection may lead to weaker consent in data protection} (Springer Science+Business Media Dordrecht, Ethics and Information Technology, 2014 Vol 16:171) p.172

\textsuperscript{49} ibid p.174

\textsuperscript{50} Alsenoy Brendan et al., \textit{Privacy notices versus informational self-determination: Minding the gap} (International Review of Law, Computers & Technology, 2014 Vol 28 No 2:185) p.188
However consumers/data subjects do not have a real choice. Consent is obtained due to a process that has been named of soft surveillance\textsuperscript{51}. The latter is a process that gives to data subjects the illusion of a choice, while instead shape the individual decision making process\textsuperscript{52}.

In Europe the principle of consent has a preeminent importance, is enshrined in Article 8(2) of the Charter of Fundamental Rights of the European Union\textsuperscript{53} and is listed as the first criterion for making data processing legitimate in the DPD\textsuperscript{54}. Consent can legitimize the processing if is "\textit{unambiguous}\textsuperscript{55}, "\textit{freely given}\textsuperscript{56}, "\textit{specific}\textsuperscript{57}" and "\textit{informed}\textsuperscript{58}". Although the criterion is fundamental for the processing of personal data the characteristics that consent of the data subject shall have led to different interpretations since they have not been clearly defined\textsuperscript{59}.

\textsuperscript{51} Kerr Ian, \textit{Lessons from the Identity Trial, Anonymity, Privacy and Identity in a Networked Society} (Oxford University Press, 2009) pp.6-11
\textsuperscript{52} ibid
\textsuperscript{53} Charter of Fundamental Rights of the European Union [2001] OJ C364/1
\textsuperscript{54} Article 7(a) DPD
\textsuperscript{55} ibid
\textsuperscript{56} Article 2(h) DPD
\textsuperscript{57} ibid
\textsuperscript{58} ibid
1.5 Overview of chapters

The first chapter of this thesis is an introduction to the topic, legal questions considered, definitions of the core concepts and the delimitation of the legal issues considered.

The second chapter will focus on the regulation relevant for the ongoing analysis. Thus will be considered how consent protects data subjects from unwanted interferences in the private life. Moreover an analysis of the WhatsApp contract terms agreement will analyse the discrepancies between theory and practice in Data Protection Law.

In the third chapter will be analysed the issues due to the ubiquitous Internet connection of smartphones. Especially the focus will be on the flow of personal data from Europe to US, the applicable law and how is used consent on these matters.

The fourth chapter will critically discuss whether consent is a criterion that can protect the privacy of data subjects. Moreover will be analysed which factors affect the substantial meaning of consent of the data subject.

The fifth chapter will consider the proposed GDPR and what innovative solutions could be brought from its adoption. Specifically will be critically discussed whether concepts as privacy by default and privacy by design\textsuperscript{60} will improve the protection of personal data. Moreover will be considered which strategies might boost the effectiveness of consent.

The conclusion will consider the possible solutions to improve the consent of the data subject in light of the research.

\textsuperscript{60} Article 23 GDPR
2 The criterion of consent of the data subject in the European legislation and the WhatsApp contract terms agreement

2.1 Introduction

In the first part of this chapter will be considered the criterion of consent and the characteristics that consent shall have to legitimize the processing of personal data. Therefore will be analysed the current European legislation in light of the A29WP opinions. Because of the purpose of this thesis the focus will be mainly placed on the problematic that arise in the online environment.

The second part of this chapter is an analysis of the WhatsApp contract terms agreement that will consider the risks for the privacy due to the use of WhatsApp. Main purpose of this section is to prove that standard contract agreements are challenging the real function of consent of the data subject\(^6\). These contracts are usually long and difficult to understand. Thus they obstacle data subjects from understanding the logic involved in the personal data processing.

The choice to focus mainly on the WhatsApp contract terms agreement was made on the basis of its great popularity and due to the acquisition of WhatsApp from the Facebook. The disproportionate amount of money paid from the latter (19 billion USD) for WhatsApp showed how much personal data could be an economical asset for a company. WhatsApp was a little company with modest infrastructures and a limited number of employees and

\(^{61}\) Edward (n 40) p.475
did not develop any cutting edge technology. Its value consisted in its ability to attract customers and create a network that connects millions of people\textsuperscript{62}.

In the latest decade databases and information became for companies one of the most valuable asset\textsuperscript{63} in economical terms. A SN or a QSN has in the collection of personal data its core business and inevitably its interest clashes with data privacy law.

\section*{2.2 The principle of consent in the European legislation}

Consent of the data subject is one fundamental criterion to allow the lawful intrusion in the privacy sphere of individuals. The EU Charter of Fundamental Rights allows personal data processing "on the basis of the consent of the person concerned or some other legitimate basis laid down by law"\textsuperscript{64}.

In the DPD consent of the data subject is required as a legitimate basis for processing personal data\textsuperscript{65}, for processing special categories of data\textsuperscript{66}, and can legitimize the transfer of personal data to third countries\textsuperscript{67}. Among the criteria that make data processing

\begin{flushright}
\textsuperscript{62} Adrien Jammet, \textit{The evolution of EU law on the Protection of Personal Data} (Cells online paper series, 2014 Vol 3 No 6) p.1  \\
\textsuperscript{64} Article 8(2) EU Charter of Fundamental Rights  \\
\textsuperscript{65} Article 7(a) DPD  \\
\textsuperscript{66} Article 8(2)(a)  \\
\textsuperscript{67} Article 26(1)(a)
\end{flushright}
legitimate consent is listed as the first criterion and is the only one that does not require a necessity test.

The A29WP in its opinion on the definition of consent pointed out that even though data subject gave his/her consent the other principles related to data quality enshrined in the DPD, as fairness, necessity and proportionality, have to be respected from the data controller.

Consent is commonly used to legitimize data processing. Especially in the online environment is easier to obtain consent through the acceptance of the privacy notice displayed on a screen instead of giving proof that data processing is necessary. Moreover the conclusion of an online contract between companies and consumers/data subjects is not possible without the acceptance of the privacy policies. In light of the A29WP opinions now will be analysed the characteristic of consent laid down in Article 7(a) DPD and Article 2(h) DPD.

"Freely given", means the ability to exercise a real choice without a risk of deception, intimidation, or coercion. The freedom of choice of a data subject might be undermined not only from physical violence or coercion but might also be a psychological pressure. These are the cases in which the data subject is under the influence of the processor as the

---

68 Article 7(a)- 7(f) DPD
69 A29WP Opinion 15/2011 (n 59) p.7
70 ibid
71 Article 6 DPD
72 A29WP Opinion 15/2011 (n 59) p.7
73 Article 2(h) DPD
74 A29WP Opinion 15/2011 (n 59) pp.12-13
employment relationships\textsuperscript{75}. Moreover could also be a situation in which the data subject is in such a state of necessity that is willing to subscribe any contract due to the lack of an alternative choice.

Consent has to be "\textit{specific}"\textsuperscript{76} and shall refer to a determined data processing with specific knowledge of which personal data are processed and for which purposes\textsuperscript{77}. Consent interpolate with the purpose limitation principle\textsuperscript{78}. This means that data shall be processed for a specific purpose and furtherly used insofar this purpose is compatible with the original one for which consent was given.

The A29WP considered that the existence of consent should be assessed on a case-by-case basis in relation to the purposes or the recipients of the personal data\textsuperscript{79}. "\textit{Specific}" consent means that if the purpose of the controller changes then the data subject must be placed in the condition to know these changes and renew if necessary his/her consent for the new purpose\textsuperscript{80}. Therefore the fact that a data subject accepts a contract terms agreement does not mean that this automatically legitimize all the contractual conditions on data processing. Especially if some clauses allows a different kind of data processing that departs considerably from the main purpose of the contract\textsuperscript{81}. Implied consent, that take place when the subject continue to use a service after that the controller changed the

\textsuperscript{75} A29WP Opinion 15/2011 (n 59) p.13  
\textsuperscript{76} Article 2(h) DPD  
\textsuperscript{77} A29WP Opinion 15/2011 (n 59) p.17  
\textsuperscript{78} Article 6(1)(b)3 DPD  
\textsuperscript{79} A29WP Opinion 15/2011 (n 59) p.18  
\textsuperscript{81} Korff (n 18) p.42
purpose of the processing is not valid consent for the processing of personal data. For the same principle additional consent is needed when personal data are sent to third parties. The rationale of the need of consent to be specific is to give to data subjects the possibility to foresee how personal data will be used.

"Informed" consent means that data subjects shall receive the basic information regarding the processing of their personal data. Data processors shall provide all the information pursuant Article 10 and Article 11 of the DPD, such as: (i) the nature of the data processed, (ii) the purposes of the processing, (iii) the recipient in case of data transfers and (iv) the rights of data subjects. Therefore the consent shall be obtained in a meaningful way, so that the subject will know and understand how the information will be collected, used or disclosed and for which purposes. Moreover the A29WP specified that the information given shall cover the risks that personal data are transferred to a third country that lack adequate protection and that the information must be clearly visible, preeminent and omni-comprehensive.

"Unambiguous" consent means that there shall be no doubts regarding the fact that the data subjects intentionally agreed on the processing of personal data. Especially in the online environment is important that the data controller can ascertain that the person giving his/her consent is the data subject. The principle of unambiguity of consent is related to

82 Samson (n 31) p.675
83 A29WP Opinion 15/2011 (n 59) p.18
84 Article 2(h) DPD
85 Kerr (n 51) p.12
86 A29WP Opinion 15/2011 (n 59) pp.19-20
87 Article 7(a) DPD
88 A29WP Opinion 15/2011 (n 59) p.21
89 ibid
the purpose limitation principle\textsuperscript{90} because consent must be a clear choice of the data subject in relation to a determined purpose.

Consent is unambiguous if the data subject has taken active steps to signal his/her consent, while inaction will not be enough\textsuperscript{91}. The A29WP in its opinion on consent highlighted the lack of unambiguity of the default settings of SNs. These settings share personal data with "friends of friends" by default\textsuperscript{92}, unless there is an opt-out choice of the data subject. However from a legal standpoint the interpretation of the A29WP seems too strict. Data subjects have already given their unambiguous consent at the moment of the subscription of the SN. If proper information were given then consent was unambiguous and there is no need to renew consent for the same processing. Instead in case that there is a substantial change of the privacy policy then the mechanism is similar to the Contract Law practices. Service contracts between consumers and companies are periodically changed from undertakings. Duty of the company is to notify the relevant changes to customers that can decide whether to end the contract or to continue the contractual relation. In this case inaction signal acceptance of the new contractual conditions.

The processing of special categories of personal data that reveal ethnic origin, political opinions, health or sex life requires an "explicit" consent\textsuperscript{93} that is more stringent than "unambiguous". This means that the process of requesting and providing consent must be a separate process from the other transaction(s) to which consent attaches\textsuperscript{94}. In light of this

\textsuperscript{90} Article 6(1)(b) DPD
\textsuperscript{91} Bygrave (n 16) p.160
\textsuperscript{92} A29WP Opinion 15/2011 (n 59) p.24
\textsuperscript{93} Article 8(1) DPD
\textsuperscript{94} Bygrave (n 16) p.161
"explicit consent" does not fit with opt-out solutions but with opt-in solutions that encourage a clearer expression of the will of the data subject.

Rationale of the criterion of consent is to place data subjects in a privileged position than the data processors. The latters are naturally advantaged due to higher knowledge on how they will process personal data. Therefore is necessary to level the playfield where the conflicting interests meet.

2.3 The role of consent on mobile devices

Mobile technology during the last decade made considerable improvements. Nowadays mobile phones incorporate a set of privacy invading technologies as geo-localization systems, cameras and Internet. Smartphones have been described as a "potentially portable spy" and are challenging the protection of personal data and the existing data privacy laws. When an application is going to be installed on a smartphone, users have to accept privacy policies often long and broadly written. These applications interact with the personal data already stored on the device. In order to do so the application has to ask the permission to users. These consent requests overwhelm users that often give consent to these procedures without being capable to fully understand the consequences.

The formation of an informed consent in the mobile world face both physical and conceptual limits that have a detrimental effect on users' awareness of privacy policies. Physical constraints consist in the fact that users have to deal with long documents

\[95\] A29WP Opinion 15/2011 (n 59) n.25
displayed on a little screen of a smartphone. Conceptual limits are due to the non-capability of users to understand and evaluate all the amount of information contained in Privacy Policies that are often long and broadly written. Moreover, to read privacy policies is an activity time costing, and usually users/data subjects do not want to use their time to read them.\footnote{Liu Yue \textit{User control of personal information concerning mobile-app:Notice and consent?} (Computer Law and Security Review, 2014 Vol 10 No 30:521 ) p.524}

The European legislator considering the growth of personal data processing in the online environment enacted the Directive 2002/58/EC\footnote{Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [2002] OJ L201/37} (hereinafter EPD) in July 2002. This was an attempt to adapt data privacy law to the changes brought by new technologies. However the EPD did not provide a clearer and more exhaustive delimitation of the criterion of consent but only followed the provisions of the DPD\footnote{Article 2(f) EPD}

Data subjects shall be provided of clear and comprehensive information about the processing of personal data and their consent must be given to access the information already stored in the users' devices\footnote{Article 5(3) EPD}. The EPD applies to electronic communications that take place in the Community\footnote{Article 1(1) EPD} this means that applies to all the individuals regardless of the location of the service provider. Therefore the rights of data subjects are non-

\begin{flushright}
99 Article 2(f) EPD
100 Article 5(3) EPD
101 Article 1(1) EPD
\end{flushright}
transferable and not subject to contractual waiver and a contract term agreement cannot avoid the application of European Data Privacy Laws\textsuperscript{102}.

2.4 Consent and the Privacy Policy of WhatsApp

In the prior part of this chapter has been delineated which are the main preconditions that legitimize consent and the problematic areas at a regulatory level. In this second part of the chapter will be analysed the Privacy Policy of WhatsApp, probably the most popular MIM application for smartphones.

SNs and MIM applications became very popular in the latest years. This growing popularity influenced the market strategies of manufacturers of smartphones. On the market appeared cheaper mobile devices that although not able to perform as smartphones, can connect users with the most popular social media\textsuperscript{103}. For the purpose of this thesis is noteworthy that among the few Internet based services already built-in there are both WhatsApp and Facebook. These cheaper smartphones are clearly directed towards less rich markets and young users that presumably have less money than adults. Therefore there is the risk that the main SNs and MIM applications will have an easy way for expanding their network and the personal data so collected beyond any expectation.


\textsuperscript{103} For an overview see Nokia website available at <http://www.microsoft.com/en-gb/mobile/phone/210/#3901754> last accessed 19 November 2014
The A29WP in its opinion 02/2013\textsuperscript{104} argued that there is not a truly valid consent when an application is installed by default on a device. This because consumers/data subjects do not give consent to the application if its implemented in the OS/hardware of the device. Therefore in these cases can be argued that consumers/data subjects should give their consent to WhatsApp before that the device is purchased.

The analysis on the contract user agreement of WhatsApp will focus on the contractual conditions that contain obscure meanings and imprecise statements. Thus will be shown how consent is used in practice to allow uses of personal data not empirically imaginable from users/data subjects.

Preliminarily is important to point out that the WhatsApp's Privacy Policy is long and without a proper systematic structure. The contractual conditions are not numbered and the regulation on one type of data processing is often fragmented among different clauses (as for e.g. the disclosure of personal data of users to third parties) placed in different pages. This creates uncertainty in users/data subjects on how the personal data will be used, especially in a mobile context. Moreover the little screen of smartphones can be an additional barrier for the proper understanding of the Privacy Policy.

Some contractual conditions of the WhatsApp's Privacy Policy are vaguely written. This leaves the door open to unknown uses of the personal data from the company or its buyers in case of sale, merging or acquisition. In this way the right to data privacy is jeopardized because data subjects are not in control of their personal information.

In the next sections will be described how WhatsApp and its QSN features may affect individuals' privacy. Moreover will be discussed the collection of phone numbers from

\textsuperscript{104} A29WP Opinion 02/2013 (n 102) p.16
WhatsApp, the disclosure of the personal data collected to third parties and the contract terms on the future changes of the Privacy Policy.

2.4.1 WhatsApp and its Quasi-Social Network features

When WhatsApp is used for the first time ask to users the permission to access the address book stored on their smartphones\(^\text{105}\). Only on the latest versions of the software, due to the concerns raised on this procedure from some European DPAs, is now possible to not grant to WhatsApp the access to all the phone contacts stored in the users' devices\(^\text{106}\). However this new feature may vary depending on the OS on which the application is running.

WhatsApp, by accessing the address book seek for a correspondence between the contact in data subjects' phones and the internal database of the company where all users are registered. In this way a can see immediately who among his/her contact is available on WhatsApp.

This indiscriminate collection of phone numbers in combination with the QSN features of WhatsApp may harm the right to privacy of data subjects. Nowadays many people use the same phone number both for personal and professional purposes. A person might have published his/her phone number on Internet for reasons that have nothing to do with the will of being involved in social relations through SNs or QSNs. For example a doctor might have the phone number published on Internet in case that one of his/her patient need urgent health care.

\(^{105}\) Dutch DPA report (n 4) p.11

\(^{106}\) ibid p.8
WhatsApp allows every user to create a simple personal profile made of a profile picture and a status message of 139 characters. This profile is as "default" visible from all the other users that are in the network of WhatsApp and have the user's phone. Therefore unknown people can see the profile picture, published status messages and the last moment when the user/data subject accessed WhatsApp without being noticed. Nonetheless that WhatsApp does not allow users to download the profile pictures of others, new smartphones can take the screenshot of what is displayed on the screen. There is then the possibility that the profile pictures would be saved and shared among unknown people.

When a user/data subject allows WhatsApp to access his/her phone contacts is not aware and cannot be aware of the aforementioned features of the software, unless he/she is willing to carefully read all the clauses of the contract term agreement and the Privacy Policy. For a substantial protection of personal data users should be placed in the condition to choose before the first run of the software whether being visible to other users or not.

In the latest release of WhatsApp users can opt-out from the automatic transmission of all the information contained in the profile. However in this way the user experience will be frustrated. The limitation will include also the contacts with whom the user want to share status, pictures and emotions. Therefore users are discouraged from opting-out and keep the default settings. Another possibility is to add unwanted contacts to a block list, however this procedure can only include subjects those phone numbers are known, leaving the problem unsolved.

The status published from users in the WhatsApp terms of agreement is not included in its Privacy Policy. The Dutch DPA notified this to WhatsApp that made available a privacy

\[107\] Dutch DPA Report (n 4) p.17
notice to users that informed that their status is shared with all the other users of the application\textsuperscript{109}.

In the example below will be shown how the WhatsApp visibility mechanism could have negative consequences for the privacy of users.

The data subject (X) is aware of all the risks and read the privacy policies carefully. However wants to join WhatsApp and share emotions, profile picture and even the places where he/she is, but only with close friends. On the other side there is another subject (Y) that had a sentimental relationship with the previous one and is obsessed about the ex partner and monitor all of her/his actions. Notwithstanding that (X) aware of the obsession of the ex partner decide to protect himself/herself by blocking the phone number of (Y) nothing impede (Y), to: (i) buy a new SIM card, (ii) create a new account on WhatsApp, (iii) add the phone number of (X) and (iv) monitor his/her activity online. This will have detrimental consequences for the privacy of X. The impossibility to exclude unwanted intrusions in the private sphere may make users an easy target for invading behaviours.

The scope of the practical example delineated above is not to prove the liability of WhatsApp for actions of subjects that deliberately decides to invade the privacy of others, but to show the limit that have both consent and opt-out practices. WhatsApp is in constant evolution but only due to the pressure of some European DPAs implemented new features that aim to increase users' privacy. However the settings as default are still on "share" therefore the only possibility that users have to protect their privacy is to opt-out or to not use the application at all.

\textsuperscript{109} Dutch DPA Report (n 4) p.18
2.4.2 The access of WhatsApp to the users' phone contacts: Is it legitimate?

WhatsApp when run for the first time upload the entire contact list of users' smartphone onto the server of the company where the phone numbers are converted in a hashed format. This encrypted database is used to find which phone numbers in users' address book correspond to WhatsApp customers. This system does not distinguish among WhatsApp users and subjects not part of the network of WhatsApp.

The encryption of phone numbers in a hashed format is a way to anonymize personal data. Article 2(b)\textsuperscript{110} state that the processing of personal data covers "any operation or set of operations which is performed upon personal data, whether or not by automatic means". Following the wording of Article 2(b) can be inferred that the activity of WhatsApp that collects, record, storage, use and combine phone numbers constitute a data processing. Convert personal data in an anonymous format fit with the definition of personal data processing therefore encryption is a kind of processing\textsuperscript{111}. Moreover the Dutch DPA in its report affirmed that when a subject is identifiable without a disproportionate effort than a person is still identifiable and then there is data processing\textsuperscript{112}.

In response to the critics on its programme that collect phone numbers of non-users WhatsApp argued that the disidentification and hashing process make it extremely difficult for the company to retrieve the original data. The Dutch DPA specified that the hashing

\textsuperscript{110} Article 2(b) DPD
\textsuperscript{112} Dutch DPA report (n 4) pp.7-8
change the nature of the data if the hashing formula is not known from WhatsApp\textsuperscript{113}. This is not the case of WhatsApp that know the hashing formula.

The process of anonymisation can extinguish the individuals' privacy interest\textsuperscript{114}. This is coherent with Recital 26 DPD that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable". However it is not an easy task to determine when the data subject is "no longer identifiable" and a mere difficulty in retrieving the original data does not means that personal data are no longer identifiable. The DPD leaves to codes of conduct to provide "guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible\textsuperscript{115}.

The rationale of Recital 26 DPD is in connection with the purpose limitation principle\textsuperscript{116} that allows process of personal data for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes\textsuperscript{117}". Therefore, due to the unclarity concerning the concept of anonymisation, the proportionality principle may apply since that there is a need to balance competing rights\textsuperscript{118}. The fact that in the case law of the ECtHR the proportionality principle has been used to assess cases where consent has not been given this does not means that the proportionality principle shall not operate.\textsuperscript{119}

\begin{enumerate}
\item \textsuperscript{113} Dutch DPA Report (n 4) p.28
\item \textsuperscript{114} Walden Ian, Anonymising Personal Data (International Journal of Law and Information Technology, Vol 10 N 2:224) p.230
\item \textsuperscript{115} Recital 26 DPD
\item \textsuperscript{116} Article 6(1)(b) DPD
\item \textsuperscript{117} ibid
\item \textsuperscript{118} Walden (n 114) p.232
\end{enumerate}
The systematic collection of phone numbers from WhatsApp seems to be excessive for the purposes targeted, by doing so WhatsApp does not respect the principles relating to data quality enshrined in the DPD.\(^{120}\).

The conduct of WhatsApp is peculiar because collect personal data legitimately from users that gave consent but also from non-users. However the lack of consent of non-users do not mean an automatic lack of legitimization of the processing of personal data. Article 7 DPD grant an equal level of legitimacy to the processing of personal data if alternatively one of the grounds listed in Article 7(a) DPD to 7(f) DPD is fulfilled. Therefore excluded consent\(^{121}\), the processing of personal data is legitimate if it is fulfilled the necessary test of one of the criteria listed in Article 7(b)-7(f) DPD\(^ {122}\).

The processing of non-users' personal data from WhatsApp cannot be included in any of the activities listed in Article 7(b) DPD to Article 7(d) DPD. The residual ground on which WhatsApp might base its legitimization is Article 7(f) DPD. The latter allow the processing of personal data only if the "processing is necessary for the purposes of the legitimate interests pursued by the controller"(...)"except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection"\(^ {123}\). The rationale behind Article 7(f) DPD is to not hamper commercial activities that imply the use of personal data while ensure adequate flexibility if there is a

\(^{120}\) Dutch DPA report (n 4) p.3

\(^{121}\) Article 7(a) DPD

\(^{122}\) Bygrave (n 119) p.165

\(^{123}\) Article 7(f) DPD
legitimate interest of the controller. Nevertheless flexibility is an enemy of certainty and it may lead to a lack of protection for data subjects.\textsuperscript{124}

The notion of "legitimate interest" is not easy to delimit. The A29WP in its opinion on the notion of legitimate interest\textsuperscript{125} stated that an interest is legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection law and other laws\textsuperscript{126}. From a literal interpretation, legitimate interest should be in accordance with data protection law "and" other laws not "or" other laws, therefore a processor shall primarily implement the requirements of the data protection law and then apply the other laws afterwards.

A legitimate interest is delimited from the way in which is substantiated the legally protected interest\textsuperscript{127} and the absolute right shall prevail on relative rights. Data protection qualifies as a relative right not completely separated from the right to respect private life\textsuperscript{128}, and is not absolute but must be considered in relation to its function in society. Therefore the concept of legitimate interest of the controller refers to the need to balance the right to data privacy with the rights and freedom of others\textsuperscript{129}. Thus, there must be a balancing test between the colliding interests of the data processors and the data subjects. The balancing

\textsuperscript{126} ibid pp.24-33
\textsuperscript{127} Ferretti p.859
\textsuperscript{128} ibid p.860
\textsuperscript{129} ibid
test shall be carried out through the principle of proportionality\(^{130}\), and has to be assessed case by case.

The balancing test has been used from the ECJ to assess the *Lindqvist* case, where the right to data privacy was balanced with the right of freedom of expression. The notion of "legitimate interest" has been used widely to allow lenders to share consumers’ personal financial data via third party commercial entities. The interests of creditors to make informed decisions have been considered prevailing the right to privacy of customers\(^{131}\).

In the case *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*\(^{132}\) the Court of Justice of the European Union stated that the application of Article 7(f) "necessitates a balancing of the opposing interests concerned"\(^{133}\). Moreover the CJEU affirmed that serious intrusions in the life of data subjects are not excused by the economic interest of the operator.\(^{134}\) However the balancing test may depend "on the nature of the information in question and its sensitivity for the data subject's private life."\(^{135}\)

In light of this analysis can be argued that the collection of phone numbers of non-users from WhatsApp does not have a legitimacy basis. An economical interest can legitimize the processing of personal data depending on which types of personal data are processed. However in the case of WhatsApp is not clear which economical interest WhatsApp is

\(^{130}\) Bygrave (n 119) p.165  
\(^{131}\) Ferretti pp.862-863  
\(^{132}\) Case C-131/12 CJEU *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014]*  
\(^{133}\) ibid [74]  
\(^{134}\) ibid [81]  
\(^{135}\) ibid [81]
pursuing by collecting phone numbers from non-users. It seems that WhatsApp collects non-users phone numbers not to deliver the messaging service but to simplify the software programming. Improved software could find the correspondence between users by accessing the address book of users' device and only process the phone numbers of those subjects that already result as WhatsApp customers.

2.4.3 The vague clauses of WhatsApp Privacy Policy that undermine the protection of personal data

Privacy policies shall be written in a plain intelligible language. However the Privacy Policy of WhatsApp contains clauses with vague and obscure meaning that, in some cases clash with each other and affect the awareness of the data subject on how and which kind of personal data are processed.

WhatsApp in its Privacy Policy affirm its commitment to not disclose Personally Identifiable Information with other third parties for their commercial marketing use without consent of the data subject. Nevertheless the company at the end of its Privacy Policy state that the Privacy Policy may be revised periodically. Therefore if a user/data subject wants to be aware of the risks for his/her privacy have to check periodically the website and go through pages of obscure clauses that are not even numbered to find out which terms changed.

A general clause that allow future changes of the WhatsApp's Privacy Policy without an obligation to notice users, have the effect to dilute the principle of consent of the data subject. Exacerbating this concept to the limit it could be inferred that this is almost

\[\text{\textsuperscript{136}}\] WhatsApp Terms of Service (n 8)

\[\text{\textsuperscript{137}}\] ibid
comparable to what it would happen if the data subject adhered to a blank privacy policy that the company might shape over and over again after its need and purposes. Data subjects have the right to have the control over their personal data. Consent shall be renewed at any change of the privacy policies; otherwise it would be an implied consent that does not have the characteristics of being *specific*\(^\text{138}\) and *unambiguous*\(^\text{139}\).

### 2.4.4 In the event or Merger, Sale, or Bankruptcy

The conditions of the Privacy Policy of WhatsApp concerning the events of merging and sale of the company are relevant in light of the recent acquisition of WhatsApp from Facebook. WhatsApp reserve to itself the "right to transfer the information collected from our users as part of such merger, acquisition or sale". Therefore Facebook may take over the control of the personal data of users/data subjects of WhatsApp.

The acquisition of WhatsApp from Facebook raised many concerns regarding the privacy of its users. The founders of WhatsApp affirmed on the company's official blog "there would not be any changes in the policy of the company regarding privacy and advertisements"\(^\text{140}\). However these concerns are not mere conjectures. Facebook announced in 2013 that it would help advertisers by letting them target their adverts to users on the basis of their phone numbers\(^\text{141}\). Due to this ambivalent statements the FTC notified both

\(^{138}\) Article 2(h) DPD

\(^{139}\) Article 7 (a) DPD


\(^{141}\) Chbeir (n 3) p.61
companies that they should honour their obligations to protect the privacy of their users. Anyhow there are no guarantees that WhatsApp will respect its commitment. This because from a contractual law perspective WhatsApp might transfer the data collected "as part of such merger, acquisition or sale".

The skepticism around the real objective that Facebook pursue is motivated from its past behaviour in a similar case. When Facebook purchased Instagram Inc. (hereinafter Instagram) its users were not subjected to advertisements based on the content they uploaded on the site. Like WhatsApp, Instagram Terms of Service included the stating that in the event of acquisition, users’ “information such as name and email address, user content, and any other information collected through the Service may be among the items sold or transferred”. Although Facebook publicly affirmed that personal data would not be transferred, Facebook accessed Instagram users’ personal data anyway. After the merging Instagram changed its Terms of Service. Instagram in its actual Privacy Policy affirm "We may share user content and your information with businesses that are legally part of the same group of companies that Instagram is part of, or that become part of that group.".


WhatsApp Terms of Service (n 8)

Instagram Privacy Policy before the acquisition from Facebook available at <https://instagram.com/about/legal/privacy/before-january-19-2013/> accessed 18 November 2014


In conclusion there is no guarantee that Facebook and WhatsApp will continue to operate as separate entity for two reasons. Firstly, WhatsApp from a legal perspective has the right to transfer data as part of merger, acquisition or sale. Secondly, it is hard to believe that Facebook acquired WhatsApp for 19 billion USD without any clear profitable purpose.

One of the core businesses of Facebook is to gather personal data and then deliver this information to advertisers so that they can target the market more effectively. This practice is quite consciously accepted from users that waive their right to privacy in exchange of having access to the popular SN. However the centralization of a huge quantity of personal data, in only one company should be a primary concern in light of the transfer of personal data overseas where there the protection of personal data is less incisive than in Europe.

In light of the fact that most of the MIM companies are US based, in the next chapter will be analyzed the flow of data from Europe to Us.

3 MIM applications and the flow of personal data to countries outside Europe

3.1 Introduction

In this chapter will be considered how consent legitimizes the transfer of personal data to third countries. MIM application to carry out their service processes personal data that (as e.g. WhatsApp) are transferred in a country outside the EEA. The DPD forbid the transfer of personal data to a third country that do not afford an adequate level of protection\textsuperscript{147}.

\textsuperscript{147} Article 25(1) DPD
Consent of the data subject is one of the grounds that legitimize the transfer of personal data\textsuperscript{148}.

European laws in data protection have not been conceived for a connected environment as it is nowadays. This lag between the law and the real world challenged the application of the DPD. This because the latter has been conceived in an era when personal data were transferred through a point-to-point connection between companies' mainframes\textsuperscript{149}.

Article 25(1) DPD has to be considered in connection with Article 4 DPD on the applicable law. The DPD is the first and only main data privacy instruments that deal with the determination of applicable law\textsuperscript{150}. The DPD applies when "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State"\textsuperscript{151} and when the controller operate from outside EEA but makes use of "equipment, automated or otherwise, situated on the territory of a Member State"\textsuperscript{152}.

Article 4 DPD raised many interpretative doubts. Due to the fact that most of the companies are based overseas will be analyzed how and at which extent consent of the data subject is capable to allow the transborder of personal data. This chapter will consider the difference in data privacy law between Europe and US, the concept of data transfer and which law shall be applied pursuant Article 4 DPD.

\textsuperscript{148} Article 26(1)(a) DPD
\textsuperscript{149} Schwartz (n 26) p.1625
\textsuperscript{150} Bygrave (n 16) p.199
\textsuperscript{151} Article 4(1)(a) DPD
\textsuperscript{152} Article 4(1)(c) DPD
3.2 The concept of adequate protection of personal data and the differences between Europe and US

The DPD allows the transfer of personal data if the third country ensures an adequate level of protection. However the DPD does not define "adequacy". Nonetheless the DPD list the main principles to use to assess whether a third country give an adequate protection\(^\text{153}\). This assessment shall consider (i) the circumstances surrounding a data transfer, (ii) the nature of the data, (iii) the purpose of the transfer and (iv) the rules of law in force in the country of destination. Rationale of Article 25 DPD is that the data protection laws in the destination country shall have principles and procedural enforcement requirements that give to data subjects a similar level of protection as in Europe\(^\text{154}\). Although the concept of "adequacy" is not as strict as the concept of "equivalent", obliges third countries to implement an adequate protection as set forth in Article 25(2) DPD. Due to this limit the DPD had a global impact\(^\text{155}\), forcing other countries to follow the principles of the DPD.

The protection of personal data in the US does not have the rank of a fundamental right. In the US where instead is given more importance to contracts and market mechanisms to set data-privacy standards\(^\text{156}\). Overseas the model of informed consent is based on the concept that privacy has to do with the ability of data subjects to control information about them

\(^{153}\) Article 25(2) DPD

\(^{154}\) Korff (n 36) p.85


\(^{156}\) Tourkochoriti Ioanna, The Snowden revelations, the transatlantic trade and investment partnership and the divide between U.S.-EU in data privacy protection (University of Arkansas at Little Rock Law Review, 2014 Vol 36:161) p.165
and that people have a different idea of privacy\textsuperscript{157}. Therefore data subjects in US can waive their data protection rights in exchange of contractual benefits.

The US legislation does not meet the adequacy test of the DPD\textsuperscript{158} since that there is a lack of a harmonized legislation on data protection. Privacy laws in the US are fragmented in numerous sectoral rules, some legally binding, some self-regulatory, some federal and some at a single state level\textsuperscript{159}. The US government to avoid a data flow blockade that would have implied a negative impact on the economy, settled down an agreement with the EEA called "Safe Harbour"\textsuperscript{160}. In this agreement are listed the principles that US companies shall respect to be allowed to import data from Europe to US.

The mechanism of compliance of the Safe Harbour is based on a voluntary self-certification basis\textsuperscript{161}. This mechanism raised many concerning that significantly increased after the revelations over the electronic surveillance program PRISM run by the National Security Agency (hereinafter NSA)\textsuperscript{162}. The involvement of the US government in data mining due to national security reasons in nothing new especially after the 9/11-terror attack\textsuperscript{163}. The European commission have been evaluating if the Safe Harbour shall be kept

\textsuperscript{157} Mc Carthy Mark \textit{New directions in Privacy: disclosure, unfairness and externalities} (Journal of Law and Policy for the Information Society, 2011 Vol 6 No 3) p.9

\textsuperscript{158} Article 25(2) DPD

\textsuperscript{159} Korff (n 36) p.248

\textsuperscript{160} Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7

\textsuperscript{161} Schwartz (n. 32) p.1981

\textsuperscript{162} Bygrave (n 16) p.195

\textsuperscript{163} Klosek Jacqueline \textit{The War on Privacy} (Praeger-West part, Connecticut London, 2007) p.45
in light of the fact that all the companies involved in the PRISM programme appears to be Safe Harbour certified\textsuperscript{164}.

### 3.3 The concept of transfer

The concept of data transfer is not clearly defined in the DPD\textsuperscript{165}. The Court of Justice of the European Union (CJEU) addressed the question on what it constitutes a data transfer in the case Bodil Lindqvist v Åklagarkammaren i Jönköping\textsuperscript{166}. The case concerned the upload of personal data on the Internet through an Internet homemade website. The CJEU in the decision stated that the upload is not a direct transfer to a third country in the meaning of the DPD since that the transfer occurred through the hosting provider\textsuperscript{167}. Moreover the CJEU considered that there is transfer of personal data only when these data are received in a third country and not when these data are just available on the Internet. Due to Internet the data might be accessible from any part of the world\textsuperscript{168}. Therefore a transfer take place only when personal data are uploaded onto a server of a third country and the access is purposely granted to other subjects in the country of destination.

The Lindqvist case did not clarified what may be considered as a transfer. The CJEU in its interpretation left the door open to loopholes that may affect the protection of personal data. In Lindqvist the CJEU affirmed that is necessary the knowledge that the data center

\textsuperscript{164} Communication from the commission to the european parliament and the council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU COM(2013) 847, p.16

\textsuperscript{165} Bygrave (n 16) p.191

\textsuperscript{166} Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping [2003]

\textsuperscript{167} ibid [61]

\textsuperscript{168} Samson (n 31) p.671
on which the information are uploaded is sited outside the EEA territory, however is no

clear how this knowledge shall be acquired\textsuperscript{169}. Another shortage of the Lindqvist
decision is that link the concept of data transfer to the idea of a pinpoint territorial transfer. This clash

with nowadays reality. Internet allows users located in third countries to access data that

are materially stored in Europe. Moreover is not science fiction to imagine that very soon

data center might be sited in international spaces as for e.g. on high seas\textsuperscript{170}.

In the era of Internet the legal distinctions between national and international data

processing are fading out and to try to delimit these two concepts is less meaningful than in

the past\textsuperscript{171}. The law should be capable to follow and foresee the changes. A legislation that

refers to a world that does not exist in reality might have two detrimental effects. On one

side might create uncertainty among operators depressing economical activity and on the

other side might leave data subjects without an effective protection for their personal data.

In Lindqvist the transfer of data occurred without the consent of the data subjects. The

subscribers of WhatsApp service instead give, their consent to transfer their personal data.

In light of this it is then necessary to analyze the concept of applicable law\textsuperscript{172} in order to

assess whether the data subjects from EEA are covered from the DPD when they subscribe

the WhatsApp service.

\textsuperscript{169} Samson (n 31) p.665
\textsuperscript{170} ibid p.664
\textsuperscript{171} Schwartz (n 26) p.1625
\textsuperscript{172} Article 4 DPD
3.4 Applicable law

Applicable law is a different notion than jurisdiction. The latter pertains to the enforcement of Court Resolutions on a determined spatial area. However, due to the rank of fundamental right of personal data processing the two concepts at a certain degree conflate in data protection\textsuperscript{173}. The DPD is applicable when a controller process data: (i) in the context of the activities of an establishment of the controller on the territory of the Member State\textsuperscript{174}; (ii) the controller is not established on the Member State’s territory, but in a place where its national law applied by virtue of international public law\textsuperscript{175}; (iii) when the controller is not established on Community territory and, for purpose 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 purposes of transit through the territory of the Community\textsuperscript{176}.

The aim of Article 4 DPD is two-folded. On one side aim to avoid that processor by relocating the activities of data processing in third countries elude the application of the DPD. On the other side aim to prevent that more than one national law could be applied for the same processing. This need for an effective protection has been remarked from the A29WP that in its opinion on applicable law affirmed that no loopholes or lacunae shall arise in the high level of protection of personal data provided by the DPD\textsuperscript{177}.

\begin{flushleft}
\textsuperscript{173} Colonna (n 155) p.6
\textsuperscript{174} Article 4(1)(a) DPD
\textsuperscript{175} Article 4(1)(b) DPD
\textsuperscript{176} Article 4(1)(c) DPD
\end{flushleft}
Companies that run MIM application are often small/middle sized and have one physical location. Despite this, they are able to offer a worldwide service. Therefore it is necessary to analyze Article 4 DPD and determine which law shall be applied in consideration of the place of establishment of data controllers irrespectively of where the data processing occurs.\textsuperscript{178}

Article 4(1)(a) DPD shall be interpreted in light of the decisions of the CJEU. Article 4(1)(a) state that the DPD apply in case that the process of personal data is carried out in the "context of the activities of an establishment of the controller" placed on a Member State. Nevertheless the DPD does not specify what is included in this "context of the activities". Recital (19) DPD specifies that the exercise of the activity shall be effective and real. In the decision Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González\textsuperscript{179}, the CJEU gave a broader interpretation of what constitute "context of the activities"\textsuperscript{180}. The case concerned \textit{inter alia} whether Google Inc. that run the search engine from US where the data processing took place, have in the subsidiary company Google Spain, an establishment in the meaning of Article 4(1)(a)\textsuperscript{181}. Google Spain does not process personal data but promote the sale of advertising products to third parties.

The Court stated that even if the data processing is carried out from Google Inc. located in the US, the activities of promoting and sale advertising space "constitutes the bulk of the

\begin{thebibliography}{9}
\bibitem{179}Case C-131/12 Google Spain (n 132)
\bibitem{180}Article 4(1)(a) DPD
\bibitem{181}Google Spain (n 132) [43]
\end{thebibliography}
Google group’s commercial activity and may be regarded as closely linked to Google Search”\(^{182}\).

The CJEU in its decision emphasized the effectiveness and real exercise of activity through stable arrangements despite where the effective data processing take place and the different legal personality of the subsidiary branch. The judgement looked at the core business model of Google to rule what is covered from the "context of the activities".

MIM companies are small sized and without branches in different countries. In light of the recent Google Spain\(^{183}\) decision a MIM company sited in the US it would fall under the application of Article 4(1)(a) of the DPD if it has a branch on the EEA territory. Instead in case that the MIM company is only based outside EEA the DPD may still apply since that Article 4(1)(c) rule the applicability of the European law if the "controller not established on the Community territory makes use of equipment automated or otherwise situated on the territory of the Member State".

The word "equipment" raised many concerns due to its unclarity in a technological context. "Equipment" might have different meanings depending on the context. Prima facie the term "equipment" gives the impression that something materially substantial and solid must be used\(^{184}\). This interpretation fit with the time in which the DPD have been conceived, where the data were stored in physically tangible mainframes\(^{185}\). From another point of view

\(^{182}\) Google Spain (n 132) [46]
\(^{183}\) ibid
\(^{184}\) Bygrave (n 178) p.254
\(^{185}\) Colonna (n 140) p.9
"equipment" is not necessarily to intend as something solid, tangible or materially substantial\textsuperscript{186} and might consist of a software system as for e.g. cookies.

The A29WP excluded the application of the National Law of a Member State when the "equipment" is used only to ensure the transit through the EEA\textsuperscript{187}. The A29WP pointed out that in consideration of the rationale of Article 4(1)(c) DPD, when a tool is designed primarily with the purpose of collecting data shall be considered as "equipment"\textsuperscript{188}. Coherently to this reasoning, cookies used from websites to gather the preferences of web surfers have been considered to fall under the application of Article 4(1)(c) DPD.

The definition of the term "equipment" is semantically broad and may lead to the risk of a regulatory overreaching. That risk occurs when rules are expressed in such general terms that \textit{prima facie} seem to apply to a large range of activities without that there is a real chance for them of being enforced\textsuperscript{189}. Having said this, a good example of how the broad terminology of the DPD affected the certainty of the law, can be observed in the different translations in other languages of Article 4(1)(c) DPD.

In the French, German and Italian translation of the DPD equipment is respectively translated as moyens, mittel and strumenti. The term equipment in other languages is more akin to the English word "means"\textsuperscript{190}. More precisely in the Italian version even though the literal translation of strumenti is tools, the context of the sentence suggests the different

\textsuperscript{186} Kuan Hon et al., Data Protection jurisdiction and cloud computing, when are cloud users and providers subject to EU data protection law? The Cloud of unknowing Part 3 (International Review of Law, Computers & Technology, 2012 Vol 26 No 2-3:129) at 138
\textsuperscript{187} A29WP 8/2010 (n 177) p.23
\textsuperscript{188} ibid p.21
\textsuperscript{189} Bygrave (n 178) p.255
\textsuperscript{190} Bygrave (n 16) p.201
meaning of medium or means. The word strumenti in the specific case in fact has the meaning of "tools of communication". In light of these difficulties, that concerned the interpretation of Article 4(c) of the DPD, the A29WP suggested that the criteria of equipment/means would more clear if complemented with the concept of targeting\textsuperscript{191}. The latter means to focus not only to the use of equipment/means but also on the nationality of the subjects that are targeted from the company. However this solution has not been implemented for the difficulties concerning the enforcement of the rules due to the difficulties to prove that a controller targeted a particular area\textsuperscript{192}.

In light of the broad meaning of equipment, will now be made a comparison between MIM applications and cookies. The latter are software that monitors users' activities online. The A29WP gave a broad interpretation of cookies, defining them as equipments that have as primary purpose the collection of data\textsuperscript{193}.

A MIM application is not primarily designed for the scope of data collection, however these applications are gathering and transmitting personal data from users as part of their normal functioning. Therefore could be argued that aside their primary purpose of deliver messages, MIM applications are also pursuing the collection of personal data as cookies from the legal perspective of data protection.

The difference between cookies and MIM applications is that while websites need to clearly ask the permission to data subjects to use cookies, MIM applications do it more hiddenly. This means that users to not have the perception that a transfer might occur.

\textsuperscript{191} A29WP 8/2010 (n 177) p.24
\textsuperscript{192} Schwartz Paul (n 26) pp.1651-1653
\textsuperscript{193} A29WP 8/2010 p.21
3.5 The transborder data flow in the WhatsApp contract terms agreement

In the WhatsApp contract term agreement there is a section entitled "Special Note to International Users". In this contractual condition WhatsApp asks users/data subjects to accept that the processing of personal data will be regulated from the law of California. Moreover the contractual conditions state that by accepting the Privacy Policy users/data subjects accept to expressly consent to the data transfer in California.

This clause pursues the interest of the company and not of the users. In this case the consent of the data subject is used from WhatsApp to override the application of the DPD. Article 4 DPD aim to avoid that companies bypass the level of protection to personal data afforded from the European legislation. WhatsApp clearly target its activities to European users. The website is available in many languages and accept payment in different currency moreover all the advertisements placed online from the company are calibrated on the nationality of the final user. This can mislead the perception of consumers/data subjects that might believe that the personal data would be processed in compliance to the European legislation.

Furthermore, even though the transfer of personal data is allowed if there is consent of the data subject\textsuperscript{194}, WhatsApp also transfer and process personal data without consent, i.e. the phone numbers of non-users. Therefore WhatsApp is not respecting the prohibition on data transfer\textsuperscript{195} since that the company is not part of the Safe Harbour frameworks.

\textsuperscript{194} Article 26(1)(a) DPD

\textsuperscript{195} Article 25(1) DPD
4 Consent in the era of Internet, still an act of self-determination?

4.1 Introduction

In the previous chapters has been considered how consent of the data subject is structured in today's legislation and how is used. Data controllers base on consent their legitimacy for different kinds of data processing. The DPD by requiring that consent shall be unambiguous, specific and informed has two main objectives. Firstly make consent an effective safeguard criterion for the privacy of individuals. Secondly aim to level the playfield between data controllers and data subjects by flattening the informational asymmetries. However these objectives have not been fully achieved.

Individuals consent to contract terms that only rarely are willing to read. The protection of personal data intertwines with commercial contract law and shares with the latter the issues regarding imbalanced contracts. When a consumer/data subject purchase/download a MIM application enter into a contract with the company that run that software. Privacy policies are part of the contract terms agreement and require an additional consent from the consumer/data subject. These two separate actions of consent usually take place one after the other in fast sequence. Therefore for data subjects to consent to the processing of their personal data become a natural action that follows their will of purchasing/downloading the software. In this way to consent to the processing of personal data becomes more a routinary action that diminishes the value of consent.

The main difference between Commercial Contract Law and Data Protection Law concern the rank of the interests that are protected. In Commercial Contract Law the strongest part of the contract can legitimately pursue its economical interest and use its higher bargaining

\[\text {Alsenoy (n 50) p.186}\]
power. Data protection law instead protects a fundamental right that shall not be influenced from this imbalance of the bargaining power.

Internet and online contracting changed the way in which consent is obtained. The process of drafting contracts shifted from being an act between physical subject to be a lonely act between the consumer/data subject and the computer interface\textsuperscript{197}. Therefore standard contracts and Privacy Policies are becoming more similar to products. Acceptance of contract terms is not anymore an expression of a bargaining process. Their content is decided only from the side that offers goods/services. This process made the contract terms not more important that the features of the goods purchased\textsuperscript{198} influencing the free will of consumers/data subjects.

In this Chapter will be analysed whether the criterion of consent is capable to protect the personal data in the online environment. Then will be taken in consideration the elements that undermine the power of consent.

\textbf{4.2 Data subject and the spontaneous disclosure of personal data, the Privacy Paradox}

One of the biggest threat to privacy are the data subject themselves that spontaneously disclose their personal information despite their concerns about their privacy. This phenomenon has been described as the Privacy Paradox\textsuperscript{199}. Individuals shows concern for

\textsuperscript{197} Nancy S. Kim, \textit{The Duty to Draft Reasonably and Online Contracts} in Larry A DiMatteo, Qi Zhou, Severine Saintier, and Keith Rowley (eds), Commercial Contract Law: A Transatlantic Perspectives (Cambridge University Press, 2014:181) p.186

\textsuperscript{198} Nancy (n 197) p.187

\textsuperscript{199} Holland Brian \textit{Privacy Paradox 2.0} (Widener Law Journal, 2010 No 19:893) p.893
privacy but routinely disclose personal data for economical convenience or for their social need to be part of a determined network.

SNs are a good example on how the Privacy Paradox works in practice. SNs as Facebook attracts users due to the personal data hosted on the website. Facebook does not sell anything, but only provide the platform where users can upload personal information\textsuperscript{200}. Nonetheless that these features of Facebook are well known their users are concerned about their own privacy.

A good example of this behavioral contradiction is the reaction of the users of Facebook when the company update/change the Privacy Policy. Status messages of users in which they state to not accept any unauthorized use of their data from Facebook went viral on the web\textsuperscript{201}. These users' statements represent the stigmatization of the Privacy Paradox. Data subjects spontaneously disclose personal data although they are concerned about their privacy.

\textbf{4.3 The mechanism of consent-gathering: How the lack of meaningful choice influence the will of subjects}

Consent of the data subject has a key role in legitimizing the processing of personal data. The rationale of this resides in the nature of consent that is an act of self-determination and expression of the individuals' free will. However the practice differ from the theory. Companies see consent as an easy way to achieve their duties to compliance with data

\textsuperscript{200} Holland (n 199) p.918

\textsuperscript{201} Emery David *Facebook "Privacy Notice" Posting is totally useless* available at \<http://urbanlegends.about.com/od/facebook/ss/Facebook-Privacy-Notice.htm> last accessed 19 January 2015
privacy law. Due to the legitimizing strength of consent, companies do not have to provide the substantive reasoning behind the processing of personal data. Thus consent is used to legitimate situations in which the rightness or appropriateness of the personal data processing is questionable\textsuperscript{202}. Therefore a validly given consent from a legal standpoint does not mean that a morally transformative action inside the subject took place\textsuperscript{203}.

Moreover the structure of the consumer market affects the bargaining power of consumers/data subjects. There are only two choices available, acceptance of the contract terms agreement and the respective privacy policies as they are or to not purchase the product\textsuperscript{204}. This lack of an alternative choice implies that consent is given to all the practices regarding the processing of personal data that are included in a privacy policy. In this way companies grant themselves the legitimacy to process personal data for several purposes in one move. Thus consent is downgraded to a mere formality instead of being a real act of self-determination where morally transformative consent takes place\textsuperscript{205}.

Data subjects are humans and not rational machines. The consent gathering mechanism exploits this weakness. When a consumer/data subject decide to purchase services/goods online makes a simple cost-benefit assessment between the protection of privacy and the immediate gratification\textsuperscript{206}. At the moment of purchasing/downloading the perception of the risk represented from the gathering of personal data is felt from consumers as something distant while instead the services/goods can provide an immediate gratification.

\textsuperscript{202} Alsenoy (n 50) pp.188-189
\textsuperscript{203} Schermer (n 48) p.176
\textsuperscript{204} Custers (n 80) p.447
\textsuperscript{205} Schermer (n 48) p.176
\textsuperscript{206} Holland (n 199) p.906
In light of this appears unrealistic that consumers/data subjects will boycott those companies that do not provide a proper protection of personal data\textsuperscript{207}.

### 4.4 Privacy policies and their inefficacy to protect personal data

In theory Privacy Policies shall cover all the aspects concerning the reasoning of the personal data processing and help data subjects to decide whether accept or not a contract and its privacy policy. However this does not happen in the real world, especially in the online environment where privacy policies are most likely unread. There are two main reasons that undermine the efficacy of privacy policies. The first is that privacy policies are difficult to understand. The second is the consent desensitisation. The growth of the market online increased the number of privacy notices that require consent from consumers/data subjects. This overflow of consent requests lead to a consent desensitisation that undermine privacy protection\textsuperscript{208}.

#### 4.4.1 The difficult understanding of privacy policies

Standard contracts and privacy policies are often written and structured in a way that discourage consumers/data subjects from carefully read and acknowledge what are they consenting to. Nevertheless in Contract Law ignorance of the contract terms agreement cannot be a legitimate excuse on which a data subject can base a complaint. The burden to read contractual terms is placed on consumers.

\textsuperscript{207} Shaffer Gregory \textit{Globaliation and Social Protection: The Impact of EU and International Rules in the ratchening up of U.S. Privacy Standards} ( Yale Journal of International Law, 2000 Vol 15:1) pp.29-35

\textsuperscript{208} Schermer (n 48) p.171
Privacy Policies are written in a difficult language mainly for two reasons. Firstly because the subjects that materially write privacy policies are lawyers that use a language not easily understandable. Moreover they aim primarily at the protection of the company and the controller from possible lawsuit\textsuperscript{209}. Thus the content of privacy policies have the tendency to be all-inclusive so that it covers all the possible future uses of the personal data collected\textsuperscript{210}. Secondly because drafters of privacy policies seem to assume that the consumer/data subject is a perfect, rational individual with a limitless attention\textsuperscript{211}. On the contrary individuals have a limited capacity of attention. The reading of long and complex privacy policies is a time-costing activity\textsuperscript{212} that requires a high level of attention.

A recent investigation on consent\textsuperscript{213} proved that there is an overall difficulty to understand privacy policies. Moreover the investigation have been showing that even the subjects that feel to have understood privacy policies do not acknowledge where and how their personal data are going to be processed.

Nevertheless would be unfair to think that companies are only trying to trick users and gather personal data. There is a lack of communication skills in drafting privacy policies. WhatsApp in the beginning was a start-up company. These are formed mainly by software

\begin{itemize}
\item \textsuperscript{209} Alsenoy (n 50) p.188
\item \textsuperscript{210} ibid p.190
\item \textsuperscript{211} ibid p.189
\item \textsuperscript{212} For a deeper insight on the cost of reading Privacy Policies: McDonald Aleecia \textit{The Cost of Reading Privacy Policies} (Journal of Law and Policy for the Information Society, 2009 Vol 4:543)
\item \textsuperscript{213} CONSENT available at <www.consent.law.muni.cz> accessed 28 January 2015
\end{itemize}
engineers that focus more on the programming and have little, or none understanding of the requirements that Privacy legislation demands\textsuperscript{214}.

### 4.4.2 The inflation of privacy notices and the consent desensitisation

In the online environment, the consent of data subjects is obtained through a broad use of privacy notices. These are pop-out window that remind users that to continue the purchasing/downloading procedure, is necessary to accept the respective Privacy Policy. These unceasing consent requests in combination with complex privacy policies weaken consumers/data subjects that at the end give consent to whatever is asked them\textsuperscript{215}.

An example of this consent fatigue is the implementation of pop-ups that alert users that a website use cookies. This way to inform data subjects has proven its inefficiency. Notwithstanding that users understand the real purpose of the privacy notice about cookies they find it annoying\textsuperscript{216}. Therefore a mechanism that was conceived to protect the personal data became an extra burden for data subjects. Thus their consent is mentally downgraded to a click-exercise without that the morally transformative consent takes place\textsuperscript{217}.

\begin{flushright}
\textsuperscript{214} Balebako Rebecca et al., \textit{The Privacy and Security Behaviors of Smartphone App Developers} (Carnegie Mellom University, Workshop on Usable Security, February 2014:1) pp.1-4
\textsuperscript{215} Schermer (n 48) p.171
\textsuperscript{216} ibid p.177
\textsuperscript{217} ibid p. 176
\end{flushright}
Numerous privacy notices can increase the consent desensitisation. Thus it could be argued that the consent so obtained is not really consent\textsuperscript{218}. For these reasons is necessary to evaluate which strategies will boost the effectivity of consent.

5 MIM applications and the crisis of consent in the online world: The possible solutions in light of the proposed GDPR

In this chapter will be considered which strategies could strengthen the principle of consent. The proposed GDPR to improve the protection of data subjects introduce a new definition of consent\textsuperscript{219} and the concepts of privacy by design and privacy by default. The analysis will firstly consider the theoretical foundations of privacy by design and privacy by default and the problems that might arise from their implementation in general terms. Then will be critically discussed the relevant articles on consent and privacy by design/privacy by default of the proposed GDPR. The final part of the chapter will focus on the effect that privacy by design and privacy by default could have on the criterion of consent of the data subject.

5.1 Privacy by design and privacy by default

The core meaning of privacy by design is to consider privacy not as an afterthought but as a way to build systems that process personal data. Although the meanings of privacy by design and privacy by default overlap they do not coincide. Privacy by design means to implement privacy rules into the hardware architecture. Privacy by default applies to the default setting of the system that does not process personal data unless there is a positive

\textsuperscript{218} Schermer (n 48) p.178

\textsuperscript{219} Article 4(8) GDPR
action of the data subject. This action is part of an opt-in structure and represents the
decision of the data subject to allow the personal data processing. Therefore privacy by
default is a part of privacy by design because the systems shall be designed in a ways that
its default settings does not process as default personal data.

Privacy by design and privacy by default belong to the paradigm of the Privacy Enhancing
Technologies (hereinafter PETs). PETs might be hardware, software or apply to privacy
preferences. PETs have been used from years, for e.g. the process of cryptography is a
PET that applies via software. Privacy by design and privacy by default can be
considered as the idea behind PETs. The implementation of privacy by design and
privacy by default means to use existing PETs or to create new ones in response to the
privacy threats posed from new technologies.

At first glance the implementation of legal rules into the architecture of systems that
process personal data seems to be the perfect solution for data privacy law. Technological
solutions would guarantee the uniform application of data protection laws since that in this
way they can be enforced without have to deal with jurisdictional issues. However the
relation between regulation and technology is difficult to balance because technology
evolves faster than law. Technology can be an aid for data privacy but can also be against

220 Froomkin (n 15) p.1529
221 ibid p.1531
222 Koops Bert-Jaap and Leenes Ronald Privacy reagulation cannot be hardcoded. A
critical comment on the 'privacy by design' provision in data-protection law (International
223 Klitou Demetrius A Solution, But not a Panacea for Defending Privacy: The
Challenges, Criticism and Limitations of Privacy by Design (Privacy Technologies and
Policy, 2014 Vol 8319:86) p.90
it. Therefore the law should be enough flexible to foresee which technology might be a threat and which might be helpful to defend privacy\textsuperscript{224}.

On one side if the law is too rigid a machine that does not have the ability to make judging assessments might wrongly consider a new technology as a threat. On the other side a flexible legislation would lead to uncertainty and not accomplish the objective of improving the protection of personal data.

5.2 The concepts of the proposed GDPR that might influence the protection of personal data in MIM applications

5.2.1 Consent in the proposed GDPR

The proposed GDPR does not distinguish between unambiguous and explicit consent. Article 4(8) GDPR flattens this difference and state that consent shall always be explicit. In this way the proposed GDPR heighten the legal requirements that consent shall have. Nevertheless the requirement of explicit consent do not mean that will be achieved a higher protection of personal data. Privacy policies might just add the word "explicit consent" to their text without any real improvement for the protection of personal data.

5.2.2 Privacy by design and privacy by default in the proposed GDPR

Article 23 GDPR define privacy by design as the implementation of appropriate technical and organisational measures and procedures\textsuperscript{225} that shall ensure that by default, only those

\textsuperscript{224} Klitou (n 223) p.94
personal data necessary for each purpose of the processing will be processed\textsuperscript{226}. However Article 23 of the proposed GDPR does not specify what are these "technical and organisational measures" and leave to the European Commission the task to lay down technical standards that should be used to fulfill the law requirements\textsuperscript{227}.

If the proposed GDPR will be adopted the definition of privacy by design and privacy by default laid down in Article 23 of the proposed GDPR will pose many issues for its application. The proposed GDPR does not say how to implement the rules into the architecture of IT systems. The lack of a standardized process may create confusion among controllers that will comply with the law requirements each one in its way. Thus there would be an increased uncertainty that could have a detrimental effect on the protection of personal data\textsuperscript{228}.

5.2.3 The consequences of the proposed GDPR on the transborder data flow

The proposed GDPR follow the rules of the DPD concerning the flow of personal data to third countries outside EEA. Transfer of personal data to countries outside EEA will not be allowed unless these countries pass the adequacy test\textsuperscript{229}, or there is the consent of the data subject\textsuperscript{230}.

\textsuperscript{225} Article 23(1) GDPR
\textsuperscript{226} Article 23(2) GDPR
\textsuperscript{227} Article 23(4) GDPR
\textsuperscript{228} Traung Peter The Proposed New EU General Data Protection Regulation (Computer Law Review International, 2012 n 2:33) p.44
\textsuperscript{229} Article 41-44 GDPR
\textsuperscript{230} Article 44(1)(a) GDPR
The real innovation will be the possibility for companies based outside EEA but that operate in different Member States to have a one-stop shop. Thus will be ensured a higher level of uniform application throughout the EEA and compliance procedures will be simplified\textsuperscript{231}.

The introduction of privacy by design and privacy by default might influence the transborder of personal data overseas. If the proposed GDPR will be adopted and so the privacy by design and privacy by default, in light of the non-adequacy of the protection of personal data in the US there might be a freezing down of the data flow. Due to the fact that many digital online services originate in the US there might be serious economical consequences. In light of this worries and the damage that this would cause to the US economy privacy by design and privacy by default became a popular topic also in the US. In 2011 senator John Kerry and John McCain introduced a legislation that would provide a safe harbour for companies engaged in privacy by design.

5.3 The crisis of consent: Would Privacy by design and privacy by default be the best solution?

The criterion of consent in the online environment has been challenged from long and difficult privacy policies and numerous privacy notices that overwhelmed data subjects. Thus the latters consent to data processing without giving to it the attention that deserve.

MIM applications have default settings that focus more on the user experience than on the privacy protection. These default settings can be sticky and even if there is the possibility to change them, few users are going do that or because is difficult to understand how to do it or for simple laziness. Companies that run applications that process personal data discourage users from changing the default settings in two ways. One is to make the opt-out procedure difficult to access and execute, the other is to reduce the functionalities of the application and to make users aware of it in order to discourage any change.

Prima facie might seems that higher consent requirements and the implementation of these rules into the design of IT systems would be the perfect solution. However these measures might increase the number of privacy notices and then augments the phenomenon of consent desensitisation.

The implementation of privacy by design that as default (privacy by default) does not allow the processing of personal data means to shift from opt-out practices to opt-in practices. This for MIM applications will mean that for every option of the application that once activated process personal data will be needed the consent of the user/data subject. Thus data subjects will have to face a higher number of privacy notices increasing the phenomenon of the consent desensitisation.

The adoption of opt-in procedures in new technologies as MIM application will not automatically increase the knowledge that users/data subjects have about the logic of the

233 ibid p.72
234 ibid p.95
235 Lundblad Nicklas, Masiello Betsy Opt-in Dystopias (Scripted Vol 7 Issue 1:155, 2010) p.159
processing. MIM applications due to their main scope to deliver text messages in the common perception are compared to the SMSs service. Thus the attitude of the user/data subject is of someone that already knows what is the functioning of the application. Moreover, due to the lack of appeal of privacy policies, users/data subjects will not understand the new features of MIM applications till they opt-in. Thus the desired effect of an opt-in mechanism that shall increase the level of informed choice will be diminished. Therefore is important to not implement opt-in procedure \textit{per se}. The implementation of opt-in procedures in the IT architecture should be done in such a way that increase the knowledge of users/data subjects on the data processing of the application.

The act of giving consent to data processing is a much more multi-faceted decision than simply choose to have the personal information collected\textsuperscript{236}. Consumers/data subject when they decide to accept determined contractual conditions make a cost/benefit assessment where the personal data may figure among the costs. The future implementation of privacy by design and privacy by default will have to balance this psychological aspect of consent and intrigue users/data subjects more than be the barrier that hinders their desires.

\section*{5.4 The crisis of consent: Possible solutions}

The downloading/purchasing of a MIM application is a decision spontaneously taken from individuals. The criterion of consent give to the data subjects the possibility to choose whether to allow or not the processing of their own personal data. In this way each individual can decide according to his/her sensivity regarding privacy. The high number of privacy notices and difficult privacy policies frustrated data subjects that no longer give to consent the value that deserves. In light of this will now be considered which solutions will increase the attention of data subjects for the content of privacy policies.

\textsuperscript{236} Lundblad (n 234) p.160
One possible solution would be to decrease the number of consent requests and decrease the consent desensitisation. This would imply that consent is required only when might involve serious risks or consequences for the protection of personal data of data subjects without lowering the standards of data protection\(^\text{237}\). A lower threshold for consent means that certain actions or inactions will signal consent without the need for an express notice. This solution requires precise rules that establish which action or inactions can objectively signal consent\(^\text{238}\).

Privacy by design and privacy by default might be useful to implement this model of solution. The rules into the IT architecture will automatically decide which type of data processing is allowed. The flaws of this model are that precise rules implemented in the IT architecture might block also legitimate data processing. The machine, that have a limited capacity to make judging assessments, might not recognize new procedures of data processing because these are not listed among the permitted actions. Thus there might be a detrimental effect on innovation and development of new technologies.

Another possible solution to improve the effectiveness of consent would be to increase the level of knowledge on data processing of users/data subjects. This does not mean that privacy policies should be even longer, but that they should have a different structure and be more users friendly. The information concerning the processing of personal data should change from the actual mental scheme that "tell" to data subjects to one that "show" to data

\(^{237}\) Schermer (n 48) p.180

\(^{238}\) ibid p.180
subjects\textsuperscript{239}. This will change the psychological predisposition towards privacy policies that will not be seen only as a burdensome time costing activity\textsuperscript{240}.

The A29WP in its opinion on application for smartphones suggested that developers of applications should invent innovative solutions to communicate in an easy and accessible way privacy policies to users\textsuperscript{241}. These solutions might include audiovisual elements that will guide the user through the different options available\textsuperscript{242}. The implementation of audiovisual elements that communicate privacy policies would be an example of privacy by design. However can be argued that these tutorials should be not too long and have a certain appeal to users. This means that the information given through these tutorials should be limited to the most important practice of the companies that are privacy invading. Audiovisual description of privacy policies that are too long might be annoying for users. There they will not pay the attention required and they will not improve the knowledge concerning the data processing.

An increased knowledge of data subjects about thee processing of personal data would also increase their awareness about which company offer a higher data protection. Experimental studies proved that consumers/data subjects, when they buy goods online, are willing to pay a higher amount of money (privacy premium) to companies that have better privacy practices\textsuperscript{243}. The market of MIM applications is different because they can be downloaded

\begin{flushleft}
\textsuperscript{239} Calo Ryan Against Notice Skepticism in Privacy (Notre Dame Law Review, 2012 Vol 87:1027) p.1041
\textsuperscript{240} Calo (n 238) p.1027
\textsuperscript{241} A29WP Opinion 02/2013 (n 102) p.24
\textsuperscript{242} ibid
\textsuperscript{243} Tsai Janice et. al, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study (ICIS Proceedings,2007) available at <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1177&context=icis2007> pp.11-14
\end{flushleft}
free of charge or have a low cost annual subscription. However this "privacy premium" shows the will of data subjects to have the best protection for their personal data. Thus this additional cost might translate into the migration of users to MIM companies that have the best privacy practices. This might increase the competition among MIM companies in a favourable way for the protection of personal data.

6 Conclusion

MIM applications shows how new technologies can challenge data privacy law. The DPD is a product of its time. The imprecise language of the DPD has provided a flexible tool adaptable to the new technologies. On the other hand the vague language is inadequate to take the challenges that the online environment poses.

The proposed GDPR aims to harmonize the European data privacy laws and to provide a modern regulation that increases the protection of personal data. Undoubtedly a Regulation, directly applicable into National Laws of Member States will avoid differences among them. However still have to be seen when the proposed GDPR will be approved and which will be the final text.

Privacy by design and privacy by default could be valuable instruments to improve the efficiency of data privacy laws. The problem of the definition given from the proposed GDPR of privacy by design and privacy by default is to not explain how these new concepts shall be implemented. Thus this uncertainty might affect the real efficacy of privacy by design and privacy by default.

The revelations on the PRISM programme of the former NSA agent Edward Snowden increased the concerns about the flow of personal data between Europe and US. The PRISM programme gathered personal data also from the servers of popular SNs. This vulnerability of the personal data gave to privacy by design and privacy by default the
power to be the symbols of the best solution practicable for the protection of privacy. However Europe and US despite the tensions, share common features in data protection and US consider with attention the right of privacy. This is also proved from the activity of the FTC that issues reports on the same issues considered form the DPAs of Europe. Privacy by design and privacy by default will be valuable mechanisms that will increase the efficacy of data privacy laws if the proposed GDPR will regulate how these measures shall be implemented. The risk is that privacy by design and privacy by default could represent more a political manifesto than a real solution for the protection of personal data.

The crisis of the criterion of consent subject reflects the inadequacy of the DPD to counteract the wide spectrum of activities that can take place in the online environment. MIM applications and the mobile environment further exacerbated the criterion of consent. The adoption of measures such as the implementation of audiovisual privacy policies might increase the knowledge of data subjects about the processing of personal data. Nevertheless is my opinion that these measures will not have the desired effect in the mobile environment. The peculiarity of the mobile context is that users/data subjects accept the conditions of privacy policies during outdoor activities. The latter is not an environment that can help data subjects to focus on the mechanisms that relate to data processing.

For a better solution is necessary to go further out than "show" the privacy policies to users. It is necessary to move to a scheme of "learning by doing". This means that a user/data

\[244\] Bygrave (n 16) pp.107-116

subject when download the application accept the contract terms agreement but not the privacy policies. The application will be a demo identical to the final product that does not process any personal data. During this trial time, users/data subjects can explore the software and receive the main information regarding the data processing while they familiarize with its functioning. In this way the time of acceptance of the privacy policies is postponed to a moment when full knowledge of the data processing is acquired. Therefore consent will be the expression of a real morally transformative action that takes place inside the data subject.
**Bibliography**

A. EC DIRECTIVES

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31


B. INTERNATIONAL AND EUROPEAN TREATIES

European Convention for Human Rights and Fundamental Freedoms available at <www.echr.coe.int>

Charter of Fundamental Rights of the European Union [2001] OJ C364/1

B. LIST OF JUDGEMENTS

Case C-131/12 CJEU Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014]

Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping [2003]

A. BOOKS AND JOURNAL ARTICLES

Adrien Jammet, *The evolution of EU law on the Protection of Personal Data* (Cells online paper series, 2014 Vol 3 No 6)


Dumortier Franck 'Data Protection in a Profiled World (ed)' *Facebook and Risks of De-contextualization of information* (Springer Science+Business Media, 2010)


Holland Brian *Privacy Paradox 2.0* (Widener Law Journal, 2010 No 19:893)


Shaffer Gregory *Globaliation and Social Protection: The Impact of EU and International Rules in the ratchening up of U.S. Privacy Standards* ( Yale Journal of International Law, 2000 Vol 15:1)


Tourkochoriti Ioanna, *The Snowden revelations, the transatlantic trade and investment partnership and the divide between U.S.-EU in data privacy protection* (University of Arkansas at Little Rock Law Review, 2014 Vol 36:161)


Wong Rebecca, *Data Security Breaches and Privacy in Europe* (Springer 2013)
REPORTS AND OTHER DOCUMENTS

European Union

(i) Commission

Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7

Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012/0011/ (COD)

Communication from the commission to the european parliament and the council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU COM(2013) 847, at 16

(ii) European Parliament


(iii) Article 29 Working Party

Article 29 Data Protection Working Party Opinion 8/2010 on applicable law (16 December 2010; WP179)

Art. 29 Working Party Opinion 15/2011 on the definition of consent (13 July 2011; WP 187)
Article 29 Data Protection Working Party Opinion 02/2013 on apps in smart devices (27 February 2013; WP 202)

Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (9 April 2014; WP 844)

Netherland


United States of America


Miscellaneous

CONSENT available at <www.consent.law.muni.cz>

Electronic Privacy Information Centre available at <https://epic.org/privacy/internet/ftc/whatsapp/default.html>

Emery David Facebook "Privacy Notice" Posting is totally useless available at <http://urbanlegends.about.com/od/facebook/ss/Facebook-Privacy-Notice.htm>


Instagram Privacy Policy before the acquisition from Facebook available at <https://instagram.com/about/legal/privacy/before-january-19-2013/#!>

Instagram Privacy Policy available at <http://instagram.com/about/legal/privacy/#!>


WhatsApp communication on privacy available at <http://blog.whatsapp.com/?lang=it>

WhatsApp Legal Info Terms of Service availabe at <http://www.whatsapp.com/legal/>
WhatsApp main page available at <https://www.whatsapp.com/?l=en>