Consent as a Basis for the Processing of Personal Data under the European Data Protection Directive:

Case Study on Facebook

University of Oslo **Faculty of Law**

Candidate number: 8014

Word count: 17,981

Supervisor: Olga Enerstvedt

January 2015

Abstract

Personal data that identifies individual persons is given some level of protection in many jurisdictions and for various reasons. In Europe, general privacy rights, mainly under the 1950 Human Rights Convention has, for a long time, been the legal standard under which personal data was protected, at least partially.

In the pursuit of helping create a single market and the role free movement of data has to that end, the 1995 Directive made an overhaul in both the legal and institutional infrastructure of data protection in Europe. At the center of the Directive rests clear stipulation of principles that data controllers should enforce and rights that individual data subjects enjoy. Thus, personal data can be validly processed if there is a legitimate basis for it. The Directive recognizes consent of data subjects as one of them. It further defines consent in such a way that it be 'free' 'specific' and 'informed', and the form of indication should be unambiguous or explicit, based on the type of data.

Within the limits of conceptual difficulties in defining these traits in a meaningfully measurable way, they are meant to ensure that data subjects have a good deal of control over their data. More, technological advances and proliferation of internet based services unforeseen by the Directive, including social networks, are testing the efficacy of consent as a basis for processing and its appropriateness is seriously questioned. Such concerns are sound as the services are vast in reach and consent of their users has been the main refuge for their extensive data related operations. It is within this context that the paper attempts to review some salient features of Facebbook, a leading social network, and the degree of their compatibility with the consent requirements under the Directive.

Acknowledgement

I would like to take this opportunity to thank those who have helped me in the completion of the thesis, and indeed, made my stay in Oslo enjoyable. The first appreciation goes to my supervisor, Olga Enerstvedt, of the UiO for her kind support and guidance. I would also wish to express my heartfelt appreciation and love to my dear Gunn Berit and my beloved family for the support and kindness. Friends in Oslo also deserve my unreserved thanks for the warm companionship.

Acronyms used

Dp - Data Protection

DPD - Data Protection Directive

DPAs - (National) Data Protection Authorities

ECHR - European Convention for the Protection of Human Rights and Fundamental Freedoms

ECJ - European Court of Justice

ECtHR – European Court of Human Right

ICCPR - International Convention on Civil and Political Rights

SNSs - Social Networking Services

TEC - Treaty establishing the European Community

TFEU - Treaty on the Functioning of the European Union

UDHR - Universal Declaration of Human Rights

WP29 - Article 29 Working Party

Table of Content

1 Chapter One: An Introduction

1.1 Background to the Study

Unlike early privacy laws that mainly aimed at protecting individuals from intrusive government practices,[1] the growing private actors with access to immense personal data means that the private sector is now the primary target of regulators.[2] Among others, Social Networking Sites (SNSs) have been operating for some time now and are growing in use and influence. Facebook is an instance with over a billion active users. As a manifestation of the growing connectivity and changes in attitude, SNSs' users tend and arguably are encouraged to disclose more data, and thus its misuse remains a source of worry.

In Europe, as in many other regions, laws have been in place with a view to limiting these side effects. On top of some relevant human rights instruments, the European Data Protection Directive of 1995 (DPD) is currently the principal legal instrument in this regard. It provides some conditions and safeguards for a legitimate processing of personal data. These conditions, which are usually referred to as data protection (dp) principles, *inter alia*, guarantee a fair processing. Among the many ways that make operations on personal data of individuals[3] fair and legitimate, securing the authorization or consent of the concerned individual is one. Consent stands out as a primary basis for a legitimate processing[4] even if other legitimate ways of processing personal data that does not require consent of the data subject also exist.[5] The centrality of consent is to be found in the fact that it "…legitimizes nearly any form of collection, use, or disclosure of personal data."[6] As a result, the Directive requires that the consent secured possesses some qualities, i.e. that it be informed, free, specific, unambiguous or explicit, as appropriate. As important as these qualities are, securing their compliance has been challenging to the extent that the appropriateness of 'consent' as a main factor in a data protection system is questioned. As such, one of the considerable

[1] Edwards (2009) p.447
[2] The new revelations of extensive surveillance may, of course, trigger more laws on government powers once again.
[3] The Directive calls them 'data subjects' (Art.2(a))
[4] Edwards (2013) p.23
[5] For the private sector, the other important bases are contract and legitimate business interest that overrides the fundamental rights of the data subject (Borgesius (2013) p.12)
[6] Solove (2013) p.1880, Custer and et al, (2013) p. 456

changes that the Proposed Regulation intends to make relates to consent. I, therefore, intend to inquire the appropriateness of consent as a justification for the processing of personal data; the place it is given under the existing relevant laws, mainly the Directive and the changes that the proposed data is introducing in this regard. The practical implementation of consent under the Directive will also be tested using Facebook as an instance.

1.2 Research questions

The thesis aspires to mainly inquire if the type of consent that Facebook users are giving to use the platform and in return for Facebook to make use of their data is compatible with the requirements of the European Data Protection Directive. It also intends to analyze the strength and weaknesses of using consent as a justification for the processing of personal data. With a view to answer these main questions, the qualities of 'consent' under the Directive and the application of the Directive on Facebook will be dealt with. The changes looming in the proposed regulation pertaining to the role of consent will also be dealt with in brief.

1.3 Justifications for the study

Data protection remains to be an important issue in public discourses with the increase in internet based services and the accumulation and monetization of mega data. In an attempt to limit the unnecessary pitfalls, laws have tried to limit the excess of data processing. In such a pursuit, the usual means has been to demand that the consent of data subjects is procured, as consent is the most used justification by those processing personal data. However, partly attributable to developments revolving around SNSs, the use of consent is undergoing some revision, at least in Europe. It, therefore, is worthwhile to inquire the existing scope and application of consent as a basis for a legitimate processing of personal data and the changes it is undergoing.

As far as the selection is concerned, it suffices to state that Facebook is the leading social network site universally and in Europe. For instance, it is the single most popular SNSs in the great majority of European countries.[7] Its widespread reach, therefore, makes it a sound choice of study. Of course, this assumes that the operations of Facebook fall under the ambit of the European dp laws, an issue to be investigated in the thesis as well.

[7] Edwards (2013) p. 2

1.4 Methodology

Generally put, the theme of the thesis concerns itself with the regulation of online behavior through law. It inquires the role of consent, as a system of data processing, in the law; its appropriateness and challenges; and tests how its practical implementation is faring as applied on a selected Facebook operations and features.

Among the possible appropriate laws at the European level, the Data Protection Directive will be at the heart of the analysis, even if other relevant laws are also consulted. Accordingly, the conventional dogmatic interpretation of laws features out predominantly with a view to establishing the meaning and scope of the relevant provisions, which in turn, can be tested against its practical application on Facebook. To this end, interpretations rendered by relevant court cases, commentaries by scholars and opinions of relevant authorities, most importantly the Working Party 29 that is established under Art.29 of the Directive, will be reviewed, as its opinions have considerable persuasive authority, even if it is not authoritative.

1.5 Structure of the Thesis

The thesis comprises of three main parts. Following this introduction, an overview of data protection is provided. The chapter aims at introducing the central features of data protection; the values engaged; and the conditions in line with which processing of personal data is legitimate, i.e., data processing principles. Having discussed these themes and, thereby, introducing the tenets of data protection system, it proceeds to discuss the place that consent has been given under the Directive and its qualities/traits. The remaining part, then, goes to analyze the arguments for and against its centrality in dp laws. The discussion on the qualities of consent under the Directive will be used in the last chapter to assess Facebook's operations in this regard.

The third chapter takes on identifying the legal basis of data protection. I first discussed some relevant human rights instruments and how data protection, as a right, is treated in them. I tried to locate the role of consent under these instruments. The chapter, then, quickly moves to look at the Directive, as the main source of data protection. As such, the central elements of the Directive are discussed, particularly its scope of application. By so doing, I lay a foundation for the next chapter that establishes the Directive's application on Facebook's operations in Europe.

The last and main chapter briefly introduces how Facebook works and establishes the applicability of the Directive. It then moves to analyze some of its features that have been causes for privacy concern. As consent is the ultimate refuge for the processing users data by Facebook, and it is mainly regulated under Facebook's 'Statement of Rights and Responsibilities' the salient points of the terms of use are analyzed. The chapter, then culminates with an assessment of the main elements of consent under the Directive against the practices of Facebook. Thus, whether the consent of users according to which data is being processed qualifies as informed, specific, free and unambiguous or explicit are tested.

Lastly, the thesis sums up the major points of discussion and concludes with few foresight notes on the future of consent as a basis of data processing.

2 Chapter Two: Data Processing: An Overview

2.1 Data Protection: Conceptual Framework

Attempts that aim at limiting unwarranted access to and use of personal data has been in place for some time now, mainly through a set of rules known as data protection laws, at least in Europe.[8] These set of rules are, nevertheless, fraught with controversies in both their relative normative values and ways of implementing them. As will be shown later, these difficulties principally emanate from the divergence in the understanding of what privacy is and its worth, as its protection usually entails restricting other important values. Thus, we ask: what is in the essence of data protection law?

The following are some of the descriptions provided for the subject matter, data protection laws (dp laws in short). Lilian Edwards wrote that "data protection protects what is known very generally as informational privacy: loosely, the right to control what is known about you."[9] Similarly, Lee Beygrave understands it as a regime that attempts "…to secure the privacy, autonomy and integrity of individuals, and thereby a basis for democratic, pluralistic society in the face of massive growth in the amount of personal data gathered and shared by organizations."[10] In a similar tone, Professor Schwartz takes dp law to be a legal structure "that attempts to regulate knowledge and concealment of an individual's personal information."[11] With more emphasis on the law's 'controlling' functions, it has also been described as a set of rules that "seek to block the flow of information."[12] Lastly, dp law is said to aim at protecting "…individual citizens against unjustified collection, storage, use and dissemination of their personal details,"[13] a description seemingly closer to the way it is presented in actual dp laws, as we shall see.

Many of the above descriptions being purposive in style, what stands out is the fact that dp laws in general aim at ensuring that individuals have a say on what is considered as their

[8] Bygrave, (2002) p.1
[9] Edwards (2009) p.445
[10] Bygrave (2002) p.8
[11] Schwartz, 1995 p.1
[12] Swire and Litan (1998) p.50
[13] Hustinx (2005) p. 62

personal information or what is known about them. This, obviously, goes in line with one of the dominant components of 'privacy', a concept that finds itself at the center of dp discourses. This being substantially in tune with the purposes of actual dp laws in general, the use of terms such as 'control', 'block' or 'concealment' in the above descriptions, deserve some cautious look as their literal reading may give a wrong impression of what dp rules actually do. This is especially visible in relation to the use of SNSs. On this issue, professor Grimmelmann would argue that if attempt is made to control personal data (through dp laws) upon which the whole notion of networking depends and, thus "gets in the way of socializing, users disable and misuse them".[14] In other words, the purpose of dp rules is not to let individuals strictly control one's personal data on SNSs *per se* as "redistribution of information is inevitable in a social network whose very purpose is to make information accessible to others."[15] It seems that such a critique is valuable in so far as it informs us not to take 'controlling' to mean the person being able to 'own' information about oneself and get some form of intellectual property protection, as this would be out of touch with reality, especially in the age of online socializing. As Bygrave has aptly asserted "… it is important to note that data protection laws rarely give persons an absolute right to dispense with data about themselves as they see fit."[16] In short, dp laws help individuals not in controlling their personal information as such, but in influencing the terms under which they can be used. Thus, Culnan's description of dp regimes as dealing with "the ability of an individual to control the terms under which their personal information is acquired and used"[17] can be taken as a better expression.

A glance at dp laws, say the European Data Protection Directive of 1995, also reveals that they are more on safeguarding against unnecessary and excessive intrusions on individuals' personal information. The Directive, for instance, attempts to ensure, among others, that data is fairly collected; is used for the ends it was collected/meant for; and that its integrity is kept intact.

Having said this, it is imperative to note that some alternative expressions are used in laws and literature alike to describe the area of law under discussion. Bygrave identifies data

[14] Grimmelman, (2008) p.1140
[15] Rubinstein and Good (2013) p.1348
[16] Bygrave (2001) paragraph 8
[17] Culnan (2000) p.1

protection, privacy law, and data privacy as the most common ones.[18] As to their relative strength and weaknesses in depicting the subject matter, Bygrave offers us the following analysis. The expression 'data protection', being popular in Europe, "fails to indicate expressly the central interests served by the norms to which it is meant to apply."[19] In other words, the idiom gives a wrong impression that what is being protected is a data, whereas it is actually individual persons that such laws try to protect. On the other hand, it has an advantage over the use of 'privacy law' as it delineates its confines to data/information, thus excluding the wide range of areas privacy traditionally encompasses. Using the term 'privacy' in the expression, he argues, risks both under and over-inclusion.[20] Under-inclusion in that dp laws include notions that are not typically dealt within privacy discourses like the integrity of a data.[21] For instance, Norway's principal dp legislation has "adequate quality of personal information" as one of its objectives.[22] Over-inclusion is also the case as privacy goes well beyond the normal stretches of the dp regime.[23] Instances include privacy safeguards against unlawful raids of one's house on which dp laws are barely relevant.[24]

Apart from their scope, there are also some important differences. It suffices here to mention the fact that in privacy proper, the focus of protection is principally what is understood as 'private sphere'. Whereas in dp what is protected is personal data, i.e., 'any information relating to an identified or identifiable natural person' (DPD, Art.2(a)), which at times may include publicly known information as it does not have to be private or intimate information.[25] On the other hand, 'data privacy', an expression Bygrave prefers to use, mitigates at least the over-inclusion mentioned above by focusing on 'data', and at the same time indicating the substantial similarities with privacy proper.[26] However, it seems that the phrase still suffers from the very same shortcomings of the expression 'data protection' as it does not really tell who the beneficiary is. Besides, as the same writer has in his previous work argued, the use of the term 'privacy' may also have some other unintended effect. This is so because as privacy has been usually portrayed as benefiting individuals and thus "...essentially in conflict with

[18] Bygrave (2014) pp.26-29
[19] Ibid, p.28
[20] Ibid, p.29
[21] Ibid
[22] Bygrave (2010) p. 173
[23] Bygrave (2014) p-29
[24] For instance, the wide scope of the term is expressed as follows. "Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.", Solove, (2008) p.1
[25] Bygrave (2014) p. 129
[26] Ibid, p.29

the needs of society", associating data protection with privacy (here through the use of 'privacy' in the terminology) "…runs the risk of obscuring the fact that data protection laws benefit not only individuals *qua* individuals but society as a whole."[27]

Hence, it is clear that there are difficulties of nomenclature in all the popular expressions just discussed. Thus, we will stick to using 'data protection' as the main focus of this paper is the European regime, where the expression is rather the standard. After all, our discussion will mainly revolve around the Data Protection Directive!

As to the development of the dp regime, even if many factors are mentioned, advance in information technology, computers and now the internet at the center, is agreed to be the single most important reason that necessitated the emergence and growth of dp regimes.[28] The threatening aspect was the automated processing of information on individuals that computers were capable of sustaining and trivializing.[29]

At last, some common features that run across many dp laws deserve some consideration. Bygrave, in his recent work, has identified three of them. Accordingly, dp laws are said to be principally statutory, where the core rules are to be found in a designated legislation as is typical in Europe.[30] Secondly, dp laws usually establish an independent body that oversees their implementation, like that of the National Data Protection Authorities (DPAs) in many European countries.[31] Lastly, he correctly observed that many dp statutes take a form of 'framework laws.'[32] By this he meant that what we usually find in dp laws are principles that need to be observed in processing personal data instead of detailed rules of dos and don'ts, hence a usual reference to 'dp principles'.

2.2. Data Protection and the Interests/Values to Balance

As we have briefly discussed, the notion of data protection is greatly interlinked with and usually discussed in relation to privacy. It happens that dp, in the same way as privacy, often competes with other equally important values. In other words, when we try to implement dp principles and thereby ensure that the processing of personal information is allowed only

[27] Bygrave (2001) paragraph $ 20
[28] Fuster (2014) pp. 29-33, Purtova (2011) p.41, Bygrave (2014) p.9, Swire and Litan (1998) p.2
[29] Fuster p. 29. Also, the fact that the DPD's main focus is on processing by automatic means resonates with this.
[30] Bygrave (2014) p.3
[31] ibd
[32] Ibid

under certain conditions, we usually stand at the crossroads against other important values. In the words of a writer named Rath Gavison, "when we study the cases in which the law suggests that a "right to privacy" has been violated, we always find that some other interest has been involved."[33] This, of course, is common in many rights.

The significance and worth of dp laws has been expressed in various forms. Often, the protection of one's privacy is presented as its core justification. Nevertheless, this only tells us little as the idea and values of privacy itself is 'in disarray', as Solove would put it.[34] The other way of justifying the importance of having dp laws is to regard data protection as a fundamental interest to be protected in its own right.[35] Still, some specific purposes that dp laws serve are also provided. Personal autonomy, integrity and dignity of individuals are among the specific interests dp laws help protect, which together try to achieve 'individual goals of self realization.'[36] By this it means that by providing protections against excessive monitoring and surveillance through the collection and analysis of personal data, dp laws help individuals act autonomously and without being 'seen' when they don't want to. Ultimately, helping develop 'capacity to resist social pressures to conform with dominant views'[37] is one of the important values that data protection inculcates on its beneficiaries.

Let us now briefly consider some of the values and interests that often conflict with privacy and data protection values. As a general opposition, dp is said to be "detrimental to societal needs."[38] The needs that allegedly should triumph over dp and its values are usually of societal or economic nature. To mention some, free access to information and its importance for an effective social welfare system is mentioned as an interest against which dp laws stand. This was, for instance, one of the major considerations during the debates that led to the adoption of Swedish dp law in the early 1970's.[39] dp regimes are also attacked as standing in the way of medical researches and thereby contributing 'for patients to die,[40] pointing to the fact that dp laws may put limitations on the accessibility of patients' data that might be used for important medical research. On the same token, storage and accessibility of previous convictions is mentioned yet as another societal need against which dp laws stand. Framing

[33] Gavison (1980), p.422
[34] Solove (2008) The first chapter of the book is aptly titled: 'Privacy: A Concept in Disarray'
[35] Bygraves (2014) p.118
[36] Westin (1967) in Bygrave Ibid
[37] Rouvroy and Poullet (2009) p.46
[38] Bygrave (2010) p.171
[39] Backman (2011) p.115
[40] Brownsword (2009) p. 84

the above arguments along the rights discourse, 'access/right to information' versus dp rights might be a possible description.

Related to this, another societal value, which usually is discussed alongside with dp is freedom of expression. These values may at times supplement one another and at other times stand against each other. For instance, dp laws help freedom of expression by barring IT companies from disclosing the identity of dissenters to oppressive governments.[41] On the other hand, as the *Linqvist* case before the ECJ demonstrated, extended application of dp laws means that even mentioning relationships on the net maybe found to be faulty on account of dp laws.[42] Still on societal needs against dp, it is claimed that these laws "increase the risk that people misrepresent themselves and defraud others."[43] As to the economic arguments against dp laws, the common trend is to emphasize on the importance of information in the market-based economy and thereby show the need and economic benefits of free information accessibility for the economy and consumers involved.[44]

Many of these arguments seem to overlook the fact that dp laws mainly empower and not dictate the individual beneficiary, as we shall see. Moreover, they overlook the balancing attempts that dp laws between the values of protecting personal data and other legitimate interests.

2.3. Data Protection Principles

As mentioned above, dp laws usually take the form of principles. Such a formulation is advantageous as it provides an opportunity for subsequent development of the laws as needs arise, mainly in keeping with advances in technology.[45] In what follows, the core principles that the principal EU data protection instrument, the Data Protection Directive (DPD), contains will be introduced. It is understood that the Directive is the most visible among similar instruments and has directly influenced national dp legislations in Europe,[46] and, thus, it is our focus of study.

[41] Leenes and Oomen (2009) p.154. The case of Yahoo! aiding the Chinese government is relevant here.
[42] Poullet (2006) p.224
[43] Bergkamp et al (2002) p.35
[44] Ibid, p.32
[45] Bygrave (2014) p.3
[46] Nouwt (2009) p 288

Among the important dp principles, which are mainly to be found under Art.6 of the Directive, is the principle of fair and lawful processing.[47] The essence is that personal data shall be processed fairly and lawfully. The application of the principle extends right from the collection of personal data to any form of processing and is arguably the broadest in scope. It also overlaps with many of the other principles. While the requirement of 'lawfulness' in the principle is more or less self-explanatory, 'fairness' is rather ambiguous. Recital 28 of the DPD talks about being fair to the individual concerned. It is argued that fairness, among others, implies that any data controller[48] should take into account the interests and reasonable expectations of the data subjects when processing.[49] Fairness also dictates that regard should be had on the methods of obtaining consent.[50] Further, the requirement implicates balancing and proportionality between dp and other values.[51] Consent, for instance, is one requirement that makes the processing of personal data lawful and legitimate, even if the fairness principle may require more.

Another principle enshrined under the DPD is the principle of minimality. Mainly targeted at the stage of collection, the principle demands that data is relevant and non-excessive in relation to the purpose for which it was collected,[52] and stands against data collection if a specific purpose can be achieved without the processing of personal data.[53] Accordingly, the principle tries to ensure that even if a legitimate ground for processing of personal data exists, it does not mean that the controller has a free ride on that data. Instead, the collection should be limited to data that is necessary for the purpose allowed and its storage and use is also limited in time. Echoing the temporal limitation, Art.6 (1(e)) requires that personal data is erased once it serves the purpose for which it was collected. The possibility of erasing irrelevant data under Art.12(b) of the DPD can also be considered as an additional expression of the principle.

Related to the principle of minimality is what is usually termed as the principle of purpose specification or the 'finality principle'. At the crux of the principle is the requirement that

[47] DPD, Art.6(1(a))
[48] Data controller is defined as a person who "…determines the purposes and means of processing of personal data, DPD, Art.2(d)
[49] Bygrave (2014) p.146. Processing under the DPD (Art.2(b)) is understood broadly and includes collection, recording, organization, storage , adaptation or alteration, retrieval , consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
[50] Edwards(2009) p. 464
[51] Bygrave (2014) pp.146-147
[52] Art.6 (1)c)) of the DPD mainly stipulates this principle.
[53] Rodot`a (2009) p.81

from the outset[54], personal data needs to be collected for a specified purpose. Besides, the data so collected should not be used or reused in a way incompatible with that purpose.[55] Bygrave relates the rationale behind the principle to respecting the reasonable expectation of the data subject.[56] In other words, when a person consents to the collection of certain personal data, she would reasonably expect that the data is solely used for the purpose for which the consent was given. The breach of such a legitimate expectation ends up in over disclosure of personal data, meaning "… more uses of information than a customer has agreed." [57]

The principle, therefore, tries to alleviate some problems like that of unintended use of data, as is also called as 'scope creep' and that of collecting data for no particular reason or otherwise known as 'fishing.'[58] However, as thoughtful as the principle is, it is hard, or to some, almost impossible to enforce[59] mainly because assessing the compatibility or otherwise of a purpose for which data was legitimately collected with that of a further purpose for which the same data might be needed is usually extremely difficult.[60] The advance in the storage capacity of computers and database technology is yet another source of difficulty, as "increasingly refined methods of data analytics is improving the ability to draw meaningful correlations between ever larger data sets."[61]

The principle of proportionality is yet another dp principle that lurks in some principles like that of 'fair and lawful' or 'purpose limitation'. In relation to fairness, for instance, proportionality is manifested "in the balancing of the respective interests of data subjects and controllers"[62] and, therefore, is applicable even if processing is based on consent of a data subject.[63] As an element of the 'purpose limitation' principle, proportionality figures in the identification of the very purpose for a certain processing.[64] Incidentally, the fact that the principle has not been clearly provided under the DPD is considered, by some, as providing

[54] DPD recital 28 states that purpose be determined at the time of collection.
[55] DPD, Art.6(1(b))
[56] Bygrave (2014) pp.153-154
[57] Swire and Litan (1998) p.8
[58] Edwards (2009) p.449
[59] Ibid
[60] Bygrave (2014) p.153, attributing the assertion to the Norwegian Supreme Court in a certain case. Possible meanings of the 'not incompatible' criterion is discussed in Bygrave (2014) pp.56-57
[61] Bygrave, Ibid
[62] Bygrave and Schartum (2009) pp.162-163
[63] Bygrave and Schartum (2009) P.164
[64] Bygrave (2014) p.148

the judiciary with an additional leverage to impose limitations on data processing operations.[65]

On top of the above principles, which come in the form of imposing obligations mainly on the data processors, the DPD also enshrines principles that directly empower data subjects.[66] The principal part of them are what Bygrave, fittingly, termed them as 'principle of data subject influence'.[67] These are various rules that aim at informing data subjects about data processing and granting them access to their personal data and possibility of erasure. Instances include the important pieces of information that data subjects need to get from data controllers as provided under Articles 10 and 11 of the DPD. Besides, the access rights recognized under Art.12(a) of DPD that enable data subjects to inquire and get a confirmation as to whether their personal data is being processed and if so its details makes part of the principle. Furthermore, data subjects have a right to get rectification, erasure or blockage of further use if the data is collected or held illegally or is irrelevant or incomplete or inaccurate.[68] The right to object processing under Art.14 and the prohibition against the making of decisions that affect persons' interests based on fully automated assessment of one's character, as enshrined under Art.15, also provide data subjects with more influence.

Lastly, principles of data quality (integrity) that focuses on the need to keep personal data 'accurate and up to date'[69] and data security, which tries to guard personal data against unauthorized access or alteration are also recognized under the DPD.[70]

2.4. Justifications and limitations of consent as a basis for the processing of Personal Data

2.4.1. Consent under the DPD

As briefly highlighted above, consent of data subjects is one of the grounds that render the processing of personal data *prima facie* legitimate, as the title of Art.7 of the DPD reveals. To begin with, consent is defined as "…any freely given specific and informed indication of his

[65] bid p.149
[66] DPD Recital 25 talks about the dual way of protection.
[67] Ibid pp.158ff
[68] DPD, Art.12 (b and c)
[69] DPD, Art.6(1(d)). Incidentally, the title 'principles of data quality' preceding Art.6 of the DPD seems rather confusing.
[70] Art.17 of DPD. A processor according to the same instrument being the person "…which processes personal data on behalf of the controller." DPD, Art.2(e)

wishes by which the data subject signifies his agreement to personal data relating to him being processed."[71] The qualities that the indication of data subject's agreement be 'freely given', 'specific' and 'informed' are of great importance in the definition. Specifically, it should be borne in mind that these are ingredient elements of the very term 'consent' on top of whatever further quality is attached as a requirement for processing.[72] The Working Party has furnished us with a good deal of guidelines as to the possible meaning of these elements, as discussed below.

Accordingly, for a consent to be considered as 'freely given' the data subject should be "…able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent."[73] This is quite high threshold. In particular, the notion of significant negative consequence for not consenting seems to resonate to the realities of SNSs, where the decline to give consent has the result of denying access. Even if, as the Working Party explained, the application of 'free consent' is clearly problematic in a situation where the data subject would not have a real choice due to subordination as in an employment relationship, 'financial' or 'emotional' dimension of the consequence are also relevant.[74] It should also be noted that free consent also implies that consent can be withdrawn, arguably without 'significant negative consequence,' as an implicit requirement under the Directive.[75]

Concerning 'specific' consent, at the core of the requirement is that the consent should relate to a named and clearly identified aspect of processing. One way of defining it is to say that it 'cannot apply to an open-ended set of processing activities.'[76] This would mean that specific consent should be acquired for possibly different purposes for which the data can be employed, be it promotion, studying customer preferences or transferring of data to a third party. In this regard however, the Working Party has pointed out that a separate consent might not be needed if operations are related and thus falls within data subjects' reasonable expectation.[77] It seems that a narrower interpretation is called for not to defeat the very purpose of the requirement. Besides, specificity of consent means that the data subject knows

[71] DPD, Art.2(h)
[72] On this, Article 29 Working Party (WP29), an advisory body to the European Commission on DP issues that was set up under Art.29 of the DPD, opined that "the consent required in Article 7(a) must also be interpreted taking into account Article 2(h) of the Directive. WP187
[73] WP187
[74] Ibid
[75] Ibid
[76] Ibid
[77] Ibid

"which data are processed and for which purposes."[78] From the forgoing discussion, we can notice how specific consent greatly depends on the data subject being informed, which is incorporated in the very definition of consent under Art.2(h).

An informed consent is given when it is "based upon an appreciation and understanding of the facts and implications of an action."[79] This requirement is helped by the obligations that the DPD imposes on controllers as envisaged under Articles 10 and 11. Both the content and the presentation of the information given are crucial here. Thus, enough information as to what happens with the data need to be given. The presentation also needs to be simple and understandable, for instance, using plain text, avoiding jargons, and visible in terms of location, size and font choices.[80] An important yardstick of a 'regular/average user' is used to decide if the information provided is understandable, and thus consent given to it is 'informed.[81] Relevant to SNSs, it is suggested that dialogue boxes are among the appropriate tools.

In addition to these intrinsic traits of consent, data processing is legitimate if, among others, the data subject "… has unambiguously given his consent" as per Art.7(a) of DPD.[82] Further, the processing of 'special categories of data', also called 'sensitive data' such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and concerning health or sex life require an explicit consent.[83]

According to WP29, the 'unambiguous' requirement implies that no doubt exists that the data subject has given consent.[84] The need for an action from the side of the data subject can also be read from the words 'indications' and 'signifying' in the definitional provision of Art.2(h). As a result, a positive action from the data subject is needed and "a mere inaction will not be enough"[85] In addition, consent has to be given before the processing starts.[86]

[78] Ibid
[79] Ibid
[80] Ibid
[81] Ibid
[82] The same requirement is provided for the transfer of personal data to a third country under Art. 26 (a) of the DPD
[83] DPD, Art.8(1 and 2(a))
[84] WP187
[85] Bygrave (2014) p.160
[86] WP187

As to sensitive personal data, the fact that they are considered intensively personal seems to be clear from the way the Directive treats them, and thus stringent requirements for their processing. Hence, the 'explicit consent' under Art.8 is understood to demand more than what unambiguous consent under Art.7 requires. For instance, 'explicit consent' would mean that there needs to be a clear and separate request for the processing of such data from the side of the controller that needs to be clearly and affirmatively replied to by the concerned data subject, even if it does not have to be in a written form.[87] Of course, the latter conclusion is clear from the fact that a 'written' qualification of explicit consent is now deleted from a similar provision in the earlier draft of the DPD.[88] Opt-out solutions are also, obviously, excluded.[89] Incidentally, it is to be noted that the selection of the so called 'sensitive' data under the Directive is criticized as outdated, not fitting the prevailing worries of the 21 century.[90]

Under the DPD, consent is only one of the grounds that make the processing of personal data fair and lawful. The other grounds are: when processing is necessary (1) for the performance of a contract to which the data subject is party; (2) for compliance with a legal obligation to which the controller is subject; (3) to protect the vital interests of the data subject; (4) or for the purposes of the legitimate interests pursued by the controller that override data protection interests of data subjects.[91] In relation to the last ground, the justification only lasts until data subjects object the processing under Art.14 of the DPD.

This said, among the valid grounds for personal data processing, consent stands out in its popularity in use[92] and its scope. Consent has a wider application in that it "legitimizes nearly any form of collection, use, or disclosure of personal data."[93] The other grounds, on the other hand, should go through, mainly, the test of necessity and can only be used in relation to the designated purpose. On this, the Working Party concedes that the other grounds "… require a "necessity" test, which strictly limits the context in which they can apply."[94] Of course, it should be noted that consent does not give a free ride to controllers as basic duties that the DPD imposes on them still remains intact and data subjects cannot contract out all of the

[87] Ibid
[88] Ibid
[89] Ibid
[90] Edwards (2009) p.459
[91] DPD, Art.7(b-f). Similar grounds are also to be found in relation to the processing of sensitive personal data under Art.8 and transfer of personal data to a third country under Art.26.
[92] Edwards (2009) p. 462
[93] Solove (2013) p.1880, Leopold and Meints (2010) p.232
[94] WP187

protections guaranteed such as access rights.[95] Besides, there seems to be a consensus that consent, however frequently in use, is not given precedence in normative weight under the DPD, even if it is not disallowed.[96] Meaning, the other grounds justify processing of personal data as much as consent does.

Yet, consent is wide in scope and, thus, frequently used as a ground for the processing of personal data. This is particularly common in SNSs. Hence, the strengths and weaknesses of this consent-based processing system deserve a scrutiny. Following are some of the major arguments from both sides.

2.4.2. Justifying Consent as a Basis for the Processing of Personal Data

One way of justifying as to why consent should remain as a ground for processing of personal data is linked to the very conception of the dp regime as an enabling system for individuals to decide on the dissemination of data identifying them. With this comes an argument that "as nobody is better placed to judge if he or she wants to disseminate data about his or her self, individual consent is necessarily a legitimate ground for the processing of personal data.[97] The fact that the argument rests on the ideal of individual autonomy, I think, makes is appealing.

Besides, Brownsword convincingly provides some more specific advantages of using consent as a justifying reason for the processing of personal data. The first is that consent makes specific, 'in personam' response possible.[98] This means, "consent does not comprehensively justify the action as such"; rather, it only prevents the consenting person from claiming as wronged.[99] Accordingly, other persons in similar situations can refuse processing. This aspect of consent has a particular relevance where data from many data subjects is necessary to make a processing meaningful. The other advantage of consent that Brownsword identified is that consent justifies an action by 'negating a wrong rather than by way of overriding a right.'[100] By this, the writer refers to the advantages of consent in sparing us from comparing and choosing between values. By consenting to a processing, individuals are not valuing their personal data any less compared to any other value that the consent might bring them. Indeed, as the main right holders and beneficiaries of the dp system, it is only logical to let individuals

[95] Bygrave (2014) p.162
[96] Bygrave and Schartum (2009) p.165, Edwards (2009) p.462
[97] Rouvroy and Poullet (2009) p.72
[98] Brownsword (2009) p.88
[99] Ibid
[100] Ibid

decide for themselves the extent and time of disclosure of personal data in order to get what they deem important at a certain time.

2.4.3. Limitation of Consent as a Basis for the Processing of Personal Data

Against the above and related justifications of consent as a legitimatizing tool for personal data processing, three strands of critique can be observed, namely those that consider consent as being too difficult/costly to meet; those that consider consent as being too easy to acquire and/or evade; and those who neutrally challenge its appropriateness as a norm. To begin with the last, it is held that permitting processing of personal data based on consent tantamount to making personal data appear like alienable commodity and thus borders to denying the moral status of privacy as if it is only protected at the discretion of individuals.[101] In response to this, I would adhere to Brownsword's assertion that in a right-based dp system, which the DPD is, choice or "consent functions as a dynamic between agents"[102] meaning that consent is an indispensable tool that enables individuals to show preferences of values at a certain moment and based on their circumstances.

Proceeding to the first set of arguments, we find various utilitarian viewpoints that run on the assumption that the requirement of consent stands in the way of other important societal gains. They would, accordingly, treat the requirement of consent as a 'tax on transaction'[103] and thus, uneconomical or claim that consent and its qualities (such as it being specific, informed, unambiguous or explicit) are obstacles to achieve societal benefits, be it in the form of security, administration, or medical research or international trade. The most important flaw of such arguments, at least from the perspective of the DPD, is what Brownsword would label as 'the fallacy of necessity'.[104] Accordingly, these arguments wrongly assume as if consent is always necessary for personal data processing to ever happen. This simply ignores the considerable number of grounds that equally justify the processing of personal data without data subjects' consent, as discussed above.[105]

The last and more challenging string of arguments against consent comes from those who underscore the easiness of acquiring consent or inefficiency of the consent-based system in

[101] Rouvroy and Poullet (2009) pp.72-73
[102] Brownsword, (2009) p.100
[103] Ibid p.85
[104] Ibid pp.90ff
[105] Such possibilities abound under the DPD. See, Recital 34; Art.7(b-f), 8(2(b-e)-8(3-5), Art.9, Art.26 (1(b-f), Art.26(2)

protecting personal data. Even if the arguments may take different forms, a concern that individuals are, to a large degree, not in a position to give the kind of consent required by the laws in the age of information technology services is the central point. Besides, even if they can, there is little, if any, way of ensuring that the data acquired according to their consent is only used for the purpose for which it was given.

In support of this, there are plenty of studies, which reveal that Internet, and mainly SNSs, users do not either read or understand the terms of use that include issues on personal data processing.[106] This might relate to the use of difficult jargons, lengthy policies, difficult layout, exhaustion to frequently and carefully think through privacy issue,[107] or even thinking that there is no advantage of so doing, anyways.[108] For instance, a recent study concluded that "it would take 76 work days to read the privacy policies that a normal person encounters in a year!"[109] Facebook's privacy policy in 2010, for instance, was ca 6000 words in length, 'longer than the US Constitution.'[110] Besides, data controllers might not sufficiently inform the data subject on the purpose and manner of processing because of trade secrecy.[111] Under these conditions, it is questionable is the consent 'given' qualifies as informed. Besides, a difficulty remains as to the actual quantum or degree of information that a person needs to have to make an informed decision, including consenting.

In addition, even if there was a chance that users read and understand the terms,[112] the kind of consent they give is not free as they "cannot choose to refuse certain conditions."[113] As noted above, for a consent to be considered as freely given, data subjects need to have a real choice. In the vast majority of internet services, there is a binary choice "between a full registration and abandoning the service."[114] Cognizant of this specifically in social networks, the WP29 stressed that they need to provide potential users with an option, where consent for processing of personal data can be freely given independently of users 'ability to access the service.[115] This, however, is not what is happening in practice, as we shall see. Similarly, it is also forcefully argued that in the context of workplace, the consent that employees provide for the

[106] Edwards (2013) p.24; Solove (2013) p. 1884
[107] Bygrave and Schartum (2009) p. 161
[108] Casper (2013) p.2, Edwards (2013) p.24
[109] Jammet (2014) p.14
[110] Edwards (2013) p.25, citing the New York Times
[111] Kamp and it al (2010) p.203
[112] And there is not usually a means to prove that they have read or understood the conditions (Edwards (2013) p.24)
[113] Jammet (2014) p.14
[114] Ibid, Solove (2013) p.1885
[115] WP187

processing of their personal data hardly qualifies as freely given.[116] The same goes to consent given to data controllers in monopoly position.[117] It is, therefore, not hard to argue that a consent given under a situation where the alternative is a putative denial of service is hardly free. Besides, as consent, for example, in many SNSs is secured by ticking privacy policy boxes as part of registration, the requirement of 'specific' consent becomes rather an illusion.[118] Cognizant of this problem, the WP29 has indicated that users need to be provided with the possibility of selecting among the uses of their data by SNSs,[119] which is not being followed, as we shall see.

It appears that the tangible problems of using consent as a justification for the processing of personal data are primarily practical and specifically that of enforcement. Among others, there are difficulties in defining the notion of informed consent in such a way that it extracts a needed level of compliance. Besides, a clear divergence between the legal requirements of 'free' and 'specific' consent and the practice is noted. Some of these limitations seem to be attributable to the difficulty of succinctly defining these terms. In general, as Bygrave and Schartum would put it, "there are legal difficulties with properly interpreting consent requirements."[120] In addition, we have seen that in few areas, consent does not seem to be the appropriate tool to ensure personal data is protected.

In summation, I would concede that the legitimacy of consent-based dp system is open to question as can be seen from the visible definitional and practical flaws it is fraught with. Yet, given its advantage of relying on personal autonomy and hoping on the potential gains and indeed possibilities of improved application of consent requirements still gives consent-based dp system a strong bent. Moreover, the absence of a better alternative in place gives it a relative advantage. For instance, reverting to the paternalistic comprehensive licensing scheme, where processing is much conditional upon DPAs' approval instead of data subjects' permission, is ruled out as unrealistic.[121] Similarly, a suggestion of data protection system based on informational obligations of confidentiality instead of data subjects' rights is well refuted by Brownsword as inefficient and for being limited in scope.[122] Hence, it seems that

[116] Leopold and Meints (2010) p.221
[117] Bygrave and Schartum (2009)p.160
[118] Edwards (2013) p 14
[119] WP187
[120] Bygrave and Schartum (2009) p.160
[121] Bygrave and Schartum (2009) pp.159-162. The system is touched upon under the DPD Art.20(1) cum recitals 53 and 54 and only few country are said to be operating as their main dp system (Bygrave, 2014, p.184)
[122] Brownsword (2009) pp.99ff

improving the enforcement of consent requirements, including through awareness creation of data subjects would be the way forward.

3 Chapter Three: Legal Standards for Data Protection in Europe: Focus on Consent as a Basis of Personal Data Processing

In this chapter, I will briefly discuss relevant legal instruments that lay the legal basis for the protection of personal data. Understandably, the discussion is mainly based on European laws and consent of data subjects as a basis for the processing of personal data will be the central theme. Among the laws, the Directive is given a relatively lengthy coverage as it is the major instrument and its analysis is aimed at establishing its application on Facebook, which is to be taken up in the subsequent chapters.

3.1. Human Rights as a Basis for Data Protection

3.1.1. Un Human Rights Instruments

As noted above, right to data protection is interlinked with privacy and dp laws usually present right to privacy of individuals as one of their rationales. It is within this context that, for instance, the UDHR's recognition of right to privacy under Art.12 is understood as including data protection, as well.[123] Besides, Art.17 of the ICCPR that recognizes a right against the interference of one's privacy is authoritatively interpreted by the Human Rights Committee so as to include the protection of personal data. Accordingly, "individuals should have the right to ascertain…whether, and if so, what personal data is stored in automatic data files, and for what purpose."[124] Rights of rectifying incorrect personal data is also recognized in the interpretation.[125] It is also imperative to note that the right is understood to be equally applicable on both governments and private actors alike under the Convention.[126] Hence, it can be argued that the human rights basis of data protection, albeit indirectly, can be traced back to the early codification of the modern human rights system.

[123] Bygrave (2010) p.180
[124] Human Right Committee, General Comment 16 (1988), paragraph 10
[125] Ibid
[126] Ibid

3.1.2. The European Human Rights Convention and Convention 108

The 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) has been the major legal standard for the right to privacy, and by extension, right to data protection for a long time. Article 8 of the Convention declares that "everyone has the right to respect for his private and family life …" With time, this right of respect for 'private life' has been widely interpreted in the rich jurisprudence of the European Court of Human Rights (ECtHR), as including personal data. This is in line with the Court's general approach of "regarding the ECHR as a living instrument to be interpreted each time in light of 'present-day conditions.'"[127] Some case decisions such as *Amann v Switzerland*,[128] and *Rotaru v Romania*[129] attest to this. However, it is argued that the way the court has interpreted Art.8 as including personal data is not purely based on the ECHR, but rather in conjunction with an important instrument, the Council of Europe Data Protection Convention (Convention 108) of 1981.[130]

The observation is sound as this latter Convention, after all, was resulted from the doubts that the Council of Europe felt with the emergence of modern technologies in the 1960s and their implications on the protection of 'private life'. Specifically, it felt "doubtful whether Article 8 of the ECHR offered any satisfactory safeguards in this area, particularly because …[it] was only applicable to interferences by public authorities, and not by private parties."[131] In response to the personal scope issue, Article 3(1) of Convention 108 made it clear that it applies on both public and private sectors. Concerning its relation to the fundamental right of privacy under Art.8 of the ECHR, two related observations are in order.

The first is that despite its human rights foundations, the instrument also provides the achievement of greater unity in Europe through free flow of information as its objective, as the first preamble reveals. This objective is, actually, said to have persisted ever since its

[127] Fuster (2014) p.95
[128] ECtHR, Amann v Switzerland App no 27798/95, ECHR 2000-II,
[129] ECtHR, Rotaru v Romania App no 28341/95, ECHR 2000-V
[130] Kokott and Sobotta (2013), p.224
[131] Fuster (2014), p.84,

inception, for the consensus was for it "… to refrain from laying obstacles in the way of international trade and commerce."[132]

The second observation, flowing from the first, relates to the fact that even if Convention 108 was meant to further the application of Art.8, the jurisdiction of the ECtHR over it is contested.[133] Of course, the Court has used Convention 108 in cases dealing with Art.8 and indeed, Convention 108, more or less, replicates the permitted interferences on Art.8 based on 'law, legitimate purpose, and necessity in a democratic society'.[134] Yet, the differences persist and personal data is only partly protected. For instance, in both *Amann v Switzerland*, and *Rotaru v Romania*, the ECtHR considered the respective data as part of 'private life' under Art.8, not simply because it 'relates to an identified or identifiable individual' as Convention 108 requires (Art.2(a)), but because 'the event recedes into the past' (it has been there for a long time) and information was stored systematically. Similarly in *Gaskin v. United Kingdom*,[135] while the court recognizes access rights of personal data based on Art.8, it, nonetheless, insisted that Art.8 does not give a general right to access personal data. Besides, in *Gaskin*, the focus was not on the information being related to the applicant as an identified individual, but on the impact of not being able to access it.[136] In a way, to the Court "there is processing of personal data that affects private life and processing of personal data that does not affect the private life of individuals."[137] What is more, the Court uses difficult-to-grasp criteria in making the choice. Recently, the Court has indicated that it considers among others, "…the context in which the data had been collected and stored, their nature, the way they were used and treated and the results obtainable from the processing,"[138] which does not really provide a meaningful guide.

What we observe from the discussion above is that reading data protection from Art.8 of the ECHR is rather immersed with caveats which limits its protection. Yet, the inclusion of Convention 108 within its remits means that the Court "… has put some additional constitutional pressure on [its] implementation."[139] Indeed, as a pioneer in providing many of the dp principles in Europe and its potentially wide territorial scope (Art.23), Convention 108

[132] Ibid p.187
[133] Kokott and Sobotta (2013), p. 223
[134] Convention 108, Art.9(2)
[135] ECtHR, Gaskin v. United Kingdom, para 37
[136] Fuster (2014) p.103
[137] Hert and Gutwirth (2009), p.24
[138] ECtHR, *Khelili v Switerland* [2011] App. No. 16188/07, §55
[139] Hert and Gutwirth (2009), p.27

has served as basis for 'all subsequent European legislation,'[140] and thus its importance cannot be undermined.

Setting aside the difficulty of finding the conditions under which personal data can be protected under Art.8 of the ECHR, where does consent figure out as a justifying ground for personal data processing? To begin with, as in many human rights instruments, the ECHR provides admissible interferences against the right to privacy, and by extension right to data protection. Accordingly, it is not an interference if privacy right is limited based on a law and the limitation is necessary in a democratic society (Art.8(2)). In addition, the limitation should be to pursue a legitimate aim or interest that the Convention exhaustively lists, including national security, public safety and rights and freedoms of others. Convention 108 also provides similar conditions, but with few changes in the list of interests that privacy may give way to under the conditions of lawfulness and necessity.

From the preceding discussion, we can notice that 'consent' is not specifically provided for as a legitimate ground for the limitation of data protection right under both the ECHR and Convention 108 unlike, say, the DPD. However, it can be argued that with a different formulation and perhaps stringent requirements, consent is indirectly recognized. This is because 'consent' provides a justification for the processing of personal data under the DPD. The DPD, in turn, is an EU law according to which Member States have adopted laws to give effect to its provisions.[141] Thus, the legality requirement under Art.8(2) of the ECHR is duly satisfied. However, as the Court has hitherto been engaging cases of non-consensual data processing, it is yet to be seen how it will weigh consent-based processing with the 'necessary in a democratic society' requirements.[142]

3.1.3. The European Human Rights Charter

Since its adoption in 2000, the Charter of Fundamental Rights of the European Union has elevated the human rights status of data protection to a new high. Unlike the 1950 ECHR, where data protection is considered as a facet of the right to privacy, the charter treats data protection as an autonomous right of its own.

[140] Fuster (2014) p.93
[141] Articles .4(1) and 32 (1) being the clear indications to this effect, the great majority of the DPD provisions also address Member States to recognize and enforce the dp regime, within a margin for maneuvers,
[142] Bygrave (2014) p.91

Apart from providing right to privacy under Art.7, the Charter states that "[E]veryone has the right to the protection of personal data concerning him or her."[143] This being the first of its kind in providing a separate fundamental right to data protection, it also includes many of dp principles like that of fairness, purpose specification, access and rectification rights (Art.8(2)). Further, true to the salient data protection laws, it requires that an independent authority oversees the enforcement of the right (Art.8(3)). The Charter also envisages that with "consent of the person concerned or some other legitimate basis laid down by law" (Art.8(2)) processing of personal data is permissible, thus, echoing the DPD. As both Convention 108 and the DPD are mentioned in the official explanation of the provision, it is argued that they need to be taken into account in its interpretation.[144] This is particularly significant development in relation to the definition of 'personal data' as it markedly differs from Art.8 of the ECHR, as understood by the ECtHR, that makes 'private life' at the center of its analysis and thereby leaves some 'personal data' unprotected.

It would, therefore, be sound to treat the inclusion of Art.8 of the Charter as a remedy to the partial protection of personal data under the ECHR. It is to be noted that the incorporation of a separate right under Art.8 of the ECHR was rejected based on the reasoning that the provision, as developed by case law, was 'effective enough to offer satisfactory protection,'[145] which is doubtful as we have seen.

The importance of the Charter for a stronger protection of personal data in Europe is also observed from a different angle, as follows. After its adoption, the Charter was given a legal effect with the same value as the Treaties[146] during the Lisbon Treaty.[147] Then followed the reproduction of Art.8(1) of the Charter in the TFEU itself (Art.16). This latter provision empowers the European Parliament and the Council to establish rules on 'the protection of individuals with regard to the processing of personal data.' This said, under Art. 100a[148] of the former Treaty establishing the European Community (TEC), according to which the DPD was adopted, EU laws could only be passed for the establishment and functioning of the internal market, thus it "does not confer on the European legislator a competence in the sector of

[143] EU Charter (2000) Art.8(1)
[144] Kokott and Sobotta (2013) p.225
[145] Emergence (2014) p.94
[146] Under Art.1(1) of the Treaty on the Functioning of the European Union (TFEU), 'the Treaties' refers to it and the Treaty on European Union (TEU)
[147] TEU (2007), Art.6(1)
[148] Now TFEU Art.114

human rights."[149] Hence, according to Romano, Art.16 of TFEU gives a new competence to the EU institutions to enact laws that might not align with the internal market,[150] and the Charter is where it all begins. The draft General Regulation on Data Protection that the Commission introduced in 2012, thus, logically opens by referring to this competence.

3.2 The Data Protection Directive 95/46/EC

The Directive, as discussed in relation to different topics above, is clearly the other important legal standard for the protection of personal data in Europe. It is framed in such a way that it obliges Member States to enact laws that ensure the conditions under which 'personal data' can legitimately be 'processed' by a 'data controller,' are met and thereby the interests of data subjects are safeguarded. Thus, what is protected is a personal data, when processed by an agent qualifying as 'data controller' under the Directive. The core concepts have specially gained complexity with the growth of internet based services that has not been foreseen by the Directive, among them being SNSs.[151] With a view to laying a foundation against which the operation of Facebook is analyzed in the subsequent chapter, these core elements are briefly discussed below.

3.2.1. Personal Data under the Directive

A personal data, according to the Directive, is "*any* information *relating* to an identified or *identifiable* natural person; ….an identifiable person is one who can be identified, directly or *indirectly*..." (Art.2(a)) (emphasis mine). The information being 'any' and only 'relating' to an individual, who has a potential to be 'identified' even 'indirectly' attest to the broadness of the term. As Bygrave puts it, "there is no prima facie requirement that the data relates to a particular … sphere of person's activity."[152] Thus, it suffices that the data can potentially help identify a person. The centrality of 'identifiability' is provided for under recital 26 of the Directive, where it is provided that "… to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." At the crux of the recital is that the capability or

[149] Romano (2013) p.4
[150] Ibido, p.5
[151] Edwards (2013) p.22
[152] Bygrave (2014) p.129

potential of identification of a person, and not an actual identification as such is what matters most.[153]

Even if disagreements abound as to its precise scope,[154] relevant case laws show that, among others, name, address, place of residence, salary amount of a public servant, data of birth, contact details, financial, medical, and social work details, relationship status, political allegiance, sexual, genetic, and racial details, school records, domestic situation are among those that are considered personal under the DPD.[155] Whether Internet Protocol (IP) addresses are personal data is not well settled. While the Working Party considers it as safer to treat them as personal data[156] as do many European PDAs, courts are divided on the issue.[157] The problem emanates from the fact that dynamic IP addresses may not identify a user, but only a device and only at a certain timeframe.

3.2.2. Processing of Personal Data

Processing is defined under the Directive as an operation on personal data and includes activities such as 'collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction' (Art.2(b)). Such a broad understanding implies, among others, that the instrument used is immaterial as far as it is automated or, if manually operated, it is done in an accessible manner (Art.2(b-c)). Besides, there is a processing under the Directive even if the data has not been communicated to a third party as collection or storing alone is 'processing'. It can also be argued that the intention of the one processing the data is not at issue, as the definition is rather an objective one. However, the purpose and effect of processing are important as they implicate the exception provided for under Art.3(2). Thus a processing "by a natural person in the course of a purely personal or household activity" is excluded from the application of the Directive. It is observed that the ECJ has developed a restrictive interpretation of the exception.[158] For instance, in the leading but controversial case, the *Lindqvist*,[159] the ECJ considers Lindqvist's posting on a homepage she created regarding a colleague as a 'publication on the Internet so

[153] Ibid p.132
[154] Edwards (2009) p.445
[155] Ibid, Romano (2013) pp.7-8
[156] WP136
[157] Bygrave (2014) p.137
[158] Romano, p.9
[159] ECJ Case C-101/01, Criminal proceedings against Bodil Lindqvist [2003] ECR I-12971

that those data are made accessible to an indefinite number of people' and thus clearly not falling under the exception.[160] The fact that a person does not economically benefit from an activity in relation to personal data does not make the activity personal or household. It seems that the number of people who have access to it is what is rather important. In line with this, in Italy, an entry of personal data into sites that are visible only to a limited number of people, is considered as falling under the exception.[161]

It can be observed that as social networks normally work through collection (through registration or otherwise) and storing personal data, among other things, their activities would simply qualify as processing under the DPD.

At last, the issue of anonymisation deserves some remarks as it touches both notions of personal data and processing and given its relevance to SNSs including Facebook.[162] It is defined as a 'process by which information is manipulated (concealed or hidden) to make it difficult to identify data subjects.[163] According to recital 26 of the Directive, data rendered anonymous in such a way that the data subject is no longer identifiable is no longer personal. This, indeed, bodes well with the fact that identification is at the center of establishing what is 'personal data'. Meaning, if data is no more serving the purpose of identification, it is logical not to treat it as personal and worthy of protection.

This said, what becomes an issue rather is whether the activity of anonymisation itself is 'processing' and therefore needs prior consent or other legitimate grounds for processing. Against such a temptation, it is asserted that as the very process of anonymisation aims at rendering the data unidentifiable and therefore benefits data subjects, it should be encouraged instead of subjecting it to the dp laws (by treating it as processing).[164] This is not convincing to me. For once, anonymisation does not necessarily benefit the data subject, for instance, in relation to exercising one's right to access (DPD, Art.12). In addition, as the WP29 has brilliantly opined recently, anonymisation can be fittingly considered as 'further processing' and a justification for it can be found either in the consent of data subjects or other grounds, mainly Articles 7(d) and (f).[165] By so doing, we are only adding more safeguards of the dp laws. The application of the DPD can then be lifted regarding the data which is and until it

[160] Ibid, para 47
[161] Romano p.9
[162] Edwards (2013) p.4
[163] Ohm (2010) p.1707
[164] Hon (2011) p.15
[165] WP216

remains reasonably unidentifiable. This, of course, assumes that the data was acquired in accordance with the relevant dp laws.

3.2.3. A Data Controller

Even if the processing of a personal data triggers the application of the DPD, the 'data controller' occupies a central role in the overall application of the Directive and, thus, frequently comes into picture. Among others, the main dp principles target what data controllers should do[166] and, as a result, the material scope of the Directive under Art.4 is defined mainly around the data controller. Indeed, it is the 'controller' who, in principle, is liable for damages resulting from unlawful processing.[167] Thus, who is a controller?

A data controller is a "natural or legal person, public authority, agency or any other body which alone or jointly with others *determines* the *purposes* and *means* of the processing of personal data" (emphasis added).[168] The personal aspect of the definition being very broad, it follows a factual approach in identifying the controller.[169] Meaning, it is determined irrespective of its actual legal capability to do so or an otherwise contractual designation as such.[170] Given the fact that many people can get involved in the processing of personal data and, thus, complicating the identification of the controller, the WP29 takes a more pragmatic solution. Accordingly, it holds that the person who determines the purpose, as understood mainly in relation to the dp principle of purpose specification, is the *de facto* controller, as the determination of 'means' is usually delegated.[171]

In light of this, SNSs simply qualify as data controllers under the Directive. This is so because as platforms for online communication, they enable individuals to publish and exchange information with other users and thereby decide the means to processes users' data and determine what to do with it.[172]

[166] Art.6(2) of the DPD clearly states that 'It shall be for the controller to ensure that paragraph 1 is complied with' referring to the major dp principles.
[167] DPD, Art.23 (1)
[168] DPD, Art.2(d)
[169] WP169
[170] Ibid.
[171] Ibid, p.15
[172] WP163

3.2.4. Material Scope of the Directive (Art.4(a,c))

The relevant question here is as to in what sort of processing of personal data is the Directive applicable. Definitely, not whenever personal data is processed. Art.4 provides the solution based on, mainly the establishment of the data controller, thus following 'territoriality principle.'[173] Accordingly, the processing of personal data 'carried out in the context of the activities of an establishment of the controller on the territory of the Member State' is the first yardstick for the application of the Directive (Art.4(1(a)). In its extensive opinion,[174] the WP29 stressed that by establishment, legal personality is not required, instead "the effective and real exercise of activities in the context of which personal data are processed" is decisive.[175] This resembles recital 19 of the DPD. Further, while a mere existence of a server or a computer in a Member State would not qualify as an establishment, a one-man office or simple agent may be considered as such if it is 'actively involved in the activities in the context of which the processing of personal data takes place' and if such presence shows a sufficient stability.[176] Appearance of permanency is also said to be embraced by the ECJ.[177] Further, the Working Party gave a hypothetical case of a controller headquartered outside the EU with "an office in Ireland dealing with issues connected with the processing of personal data, including in particular IT support" as satisfying the criteria.[178] Thus, locating an establishment, in this way, in the Member States triggers the application of the Directive. It should be noted that the controller does not have to be established in the EU, nor does the actual processing need to happen there.[179] Also, it does not require that the processing is carried out by the establishment.[180]

The second ground for the application of the Directive, under Art.4(1(c) is to be found when the controller is not established or have an establishment but, 'for purposes of processing personal data makes use of *equipment* … *situated* on the territory of the … Member State' (emphasis added). The provision is of great importance in relation to the operations of most SNSs. While Moerel framed the use of the equipment in an EU member state as processing

[173] Morel (2011a) p.29
[174] WP179
[175] Ibid
[176] Ibid.
[177] Moerel (2011b) p.35
[178] Ibid, p.16
[179] Moerel (2011b) p.97
[180] Ibid., p.100

taking place in the same,[181] the Working Party considers it as signifying that 'the processing of personal data has a clear connection with such territory.'[182] The latter interpretation seems to go more in line with the wide application of the Directive that is meant to ensure that individuals are not left out.[183]

Understood this way, it stands to fill a possible legal lacuna under Art.4(1(a) by covering situations where data is collected without a controller having an establishment in EU members or even if there is an establishment under (a), data is not processed in the 'context of the activities' of the establishment. In tune with this purpose, 'making use' of equipment is understood to involve some kind of activity that is meant to process personal data, which implies that ownership or full control of the equipment is not necessary.[184] The meaning of an 'equipment' under Art.4(1(c)) remains controversial[185] and this is understandable given its ramification on the scope of application of EU dp laws on modern technologies that are known for deploying sophisticated ways of running their businesses. The Working Party almost equates 'equipment' with a 'means',[186] a word that has proven to have a very wide coverage as observed in national states practices.[187] The purpose of the provision and the fact that many national laws and majority versions of the Directive use 'means' or expressions of similar effect, are forwarded as justifications for the broad interpretation.[188] As a result, deploying cookies, for instance, is considered as 'making use of an equipment' by the Working party,[189] even if writers would find this as unintended overstretching of the legal system.[190] In addition "other doubts have been raised about the nature of cookies as personal data, since cookies definitively identify a terminal (or a session opened into a terminal), but not an individual as such."[191] Besides as cookies normally give a notification and they need to be installed by a computer user, rejecting this installation seem to deprive the user of the dp protection as Art.4(1(c) applies only if the controller uses an equipment, which is the users' computer.

[181] Ibid. p.103
[182] WP179
[183] DPD, recital 20.
[184] Ibid
[185] For instance, Moerel (2011b)
[186] WP179
[187] Moerel (2011a) p.33
[188] WP179
[189] Ibid,
[190] Moerel (2011a) p.40, citation 63 in particular.
[191] Poullet (2010) p.14

Based on such wide scope of application of the Directive, SNSs have been treated as, one way or the other, falling under the ambit of the Directive in relation to personal data from European users. The Working Party has repeatedly reaffirmed that[192] and indeed the broad construction of Art.4 means it is likely to be applicable on SNSs even if they are headquartered outside the EU. The broad interpretation in such a way that IP addresses are treated as personal data and that cookies constitute an equipment makes it easier for the Directive to have an application on many of the US based internet giants, like Facebook.

3.3 The Proposed Data Protection Regulation: Changes Regarding Consent

3.3.1. Background to the Regulation

In January 2012, the Commission proposed a comprehensive data protection regime with a view to strengthening data protection rights. Most importantly, it has proposed a General Data Protection Regulation, to replace Directive 95/46/EC.[193] Two main reasons were forwarded by the Commission in support of the proposal, namely, difference in the implementation of dp laws among Member States and 'legal uncertainty concerning how to deal with the significant risks associated notably with online activity'.[194] As it stands now, the Parliament has, on March 12, 2014, significantly endorsed the Commission's Proposal with some amendments and an adoption by the Council is what is mainly left for it to become a law.[195]

As the Memo that the Commission released following the endorsement by the Parliament shows, there has been three main innovations the Regulation would bring, looked from the side of businesses. The first being the introduction of a single law to all EU member states as the Regulation will be directly applied, the second is establishing a single supervisory body.[196] The third purpose aims to expand the application of the European dp law on non-European entities by expanding its territorial scope and equipping European regulators with strong enforcement mechanisms.[197]

[192] For instance, WP163
[193] See Art.88 Proposed Regulation
[194] Explanatory Memorandum to the Reform Package, I. Context of the Proposal, COM(2012) 11 final, p. 2, cited in Kotschy (2014), p.1
[195] European Commission, MEMO/14/186 (2014)
[196] Ibid
[197] Art.3 and Art. 79 of the Proposed Regulation.

3.3.2. Consent under the Proposed Regulation

A Eurobarometer in 2011 reveals that nine out of ten Europeans are concerned about mobile apps collecting their data without their consent, and seven out of ten are worried that their information might be disclosed by the companies holding them.[198] In response to such concerns, the Proposed Regulation has introduced some changes on the way consent currently works under the Directive.

The first change relates to the very definition of 'consent'. According to Art.4(8) of the Proposed Regulation, consent means "any freely given specific, informed and *explicit* indication…" (emphasis added) The main change from Art.2(h) of the Directive is that consent now, by definition, should be explicit. If we can take a lesson from the use of the term under Art.8 of the Directive in relation to sensitive data, it increases the threshold. By so doing, the Proposed Regulation avoids the distinction between 'unambiguous' and 'explicit' consent that, under the Directive, pertain to ordinary personal data and that of sensitive data, respectively.[199] Under the Regulation, as it stands now, consent can only be given by an affirmative action, including by ticking boxes.[200]

The other substantial change introduced is to be found under Art.7 of the Proposed Regulation. The provision made it clear that the burden of proving that consent is given rests with data controllers. In addition, it has clearly recognized the right of data subjects to withdraw one's consent at any time.[201] It also codified the highly accepted opinion that when there is a significant imbalance between the position of the data subject and the controller, consent won't be the appropriate mechanism to process personal data. Even if the data processing in the context of employment and public law areas are mentioned as instances, this provision may potentially have a restricting effect on the use of consent as a ground for personal data processing.

Lastly, under Art.18(2), data subjects have a right to demand the transmit of their personal data to another controller, if, among others, processing by the first controller was based on

[198] Erobarometer 2011
[199] Proposed Regulation, Articles 6(a) and 9(2(a))
[200] Ibid, recital 25
[201] See Also Art.17 (1(b), where withdrawal of consent triggering the right to be forgotten and erasure.

their consent. This provision might have a particular relevance to SNSs so that data subjects can change services based upon their consideration without inconvenience.

In a form of conclusion, what can be said in general is that consent is and indeed has been playing an important role in the conception of the data protection law in Europe, as the Working Party has also confirmed.[202] The Proposed Regulation is also following a suit. What stands out in the proposal is its details and a general higher threshold of consent by including 'explicit' as an part of the definition. It appears that with the kind of strict implementation envisaged in the Proposed Regulation, coupled with a higher and uniform consent requirement, the role of consent can be diminished in effect.

[202] WP187

4 Do Facebook's Data Processing Practices comply with the Requirements of Consent Under the Directive? an Assessment

Facebook, a giant internet based service, is known for the processing of massive personal data from its users. As the main justification for the validity of such processing is the consent of the users, it is imperative to assess if the required kind of consent is indeed being secured, the standard being the Directive. In this chapter, therefore, the service provider is briefly introduced and the applicability of the Directive to the service provider's European operations established. Following that, the chapter examines the functioning and some major privacy challenges in the operations of Fabcebook. Lastly, it renders the assessment in light of the particular elements of consent as discussed in the second chapter.

4.1 Facebook Introduced

Founded in 2004 with a mission to 'give people the power to share and make the world more open and connected', Facebook has, as of September 30, 2014, 1.35 Billion monthly active users, with more that 82% of users being outside the US and Canada.[203] It remains the most popular social networking service worldwide. In Europe, it leads the market in 17 of 25 countries,[204] and according to a study conducted in 2012, Facebook is said to add 15.3 billion Euros to the European market.[205] Compared to Twitter, another popular SNSs, it has five times the number of monthly active users and enjoyed over ten times in revenue in the second quarter of 2014, amassing 2.91 billion dollars in revenue.[206] Tsaoussi identified three features that give Facebook its popularity, namely:

> a) Users can exchange messages, including automatic notifications when they update their profile,
> (b) They can join common interest user groups (organized by workplace, school, or college, or other characteristics, and

[203] Facebook, Newesroom, 2014
[204] Edwards (2013) p.2
[205] Facebook Newsroom (2012)
[206] Twitter v Facebook (2014)

(c) Build "Applications" which allow users to personalize their profiles and perform other tasks.[207]

Beyond these organizational configurations, privacy relevant choices at its initial stages are also regarded to have given Facebook a plus over competitors. Ellison and boyd, for instance, suggested that Facebook gave the possibility for users to decide who, in their network, can view different aspects of their profiles unlike, say, LinkedIn that controls what a viewer can see depending on the type of their account or MySpace that only provided a 'public' or 'friends only' options.[208] Particularly, unlike other SNSs of the time, Facebook "did not initially allow users to make any of their content broadly accessible."[209] The possibility of more privacy control was, thus, an advantage for Facebook from early on. This model remains at the center of Facebook even today, but works in a complicated way.

When users open a Facebook account, they are required to provide demographic data such as their name, age, study, gender, relationship status and so forth. It also encourages them to provide their address, telephone number, occupation, photographs, work places, places lived in, life events, interest and other details.[210] Having provided the data, users are asked to agree on Facebook's terms of use, which details relationship between Facebook and users, including the way Facebook uses users data. Thus, the accumulation of extensive personal data begins from the very outset. With time, Facebook introduced many features and with that came more data. Among others, status updating and photo/video sharing that is also immediately sent out to 'friends' (the News Feed feature); a chronicled display of a user's history of Facebook activity in their Facebook 'Walls' (the Timeline), private messaging, 'likes' and 'interests' have all been a source of immense data for the platform. As can be seen from the list of items under 'Accessing your Facebook Data'[211] at least 69 sets of data are stored with Facebook.

Facebook, as many other SNSs, has been instrumental in serving the public in many ways, be it in education, social relationship, the promotion and creation of business and in helping organize political movements. However, as Facebook's main revenue is dependent on users' personal data, privacy concerns and, indeed, incidents are rife. Given its reach and the ever growing sophistication, it is rational to think that its privacy related practices would have a

[207] Tsaoussi (2011) pp.1-2
[208] Boyd and Ellison (2008) p. 213
[209] Boyd and Hargittai (2010) p.3
[210] ibid p.2
[211] Facebook at https://www.facebook.com/help/405183566203254 (last accessed on January 10, 2015)

considerable implication, not only on the over a billion users, but also on the regulatory system of SNSs in general.

4.2 The Application of the Directive on Facebook

The DPD mainly works by imposing certain obligations on data controllers and providing corresponding rights to data subjects to manage their personal data, where consent features predominantly. As per Art.2(d) of the DPD, a data controller is one who decides the purpose and means of the processing. SNSs are by definition controllers, simply because they are the ones who, mainly through the setup and organization of their services, decide the purpose of the processing, which usually is "to allow users to engage in social networking so that advertisers can use information posted on user profiles to better target their ads."[212] As discussed above, Facebook qualifies as a controller.

The other important condition for the application of the Directive over Facebook would be if the latter processes personal data as discussed in chapter three. As highlighted above, both 'processing' and 'personal data' are defined broadly. Besides, it is clear that much of what Facebook users provide while opening an account or through their posts and tagging is plain personal data and even some would qualify as sensitive. As Facebook operates with users data, including by registration, storage and transferring to third parties, the processing of personal data is easily satisfied.

Still, the fact that Facebook makes personal data anonymous when providing it to advertisers cannot be a defense,[213] at least for three reasons. First, for anonymisation to happen, Facebook needs to have personal data acquired as per the dp laws. Second, the processes of anonymisation itself can be very well considered as a 'further processing' and thus requiring a specific consent or other ground, as we have seen is necessary. Third, given all the means available to Facebook, it is easy to link the data back to an identifiable person.

The last and important point to consider so as to establish the applicability of the Directive on Facebook pertains to its scope of application under Art.4. Accordingly, the Directive governs processing of personal data 'carried out in the context of activities of the establishment of the controller' on the Member States and to processing of personal data for which purpose the controller 'makes use of an equipment, automated or otherwise, situated on the territory.'

[212] Garrie et al (2010) p.131
[213] Roosendaal (2010) p.9

Arguably, the operations of Facebook, at least, in relation to users from Europe, fall under the Directive on both counts.

In relation to the first criteria under Art.4 (a), the relevant question is if Facebooks offices in Europe qualifies as an 'establishment' and if processing of personal data from Europe is done, wherever that might be, in the context of the activities of the offices. In this regard, Facebook has not been open in relation to its operation in Europe. For instance, it is reported that "information about the exact nature of the activities of the Facebook offices located in Europe and, most important, whether they are involved in data processing is very difficult to obtain."[214] Facebook does not also reply individual questions about its operations.

However, on its own admission, it appears that it has establishments in Europe. Facebook opened an office in London in 2007. A year later, it announced that it has opened an international headquarter in Dublin, Ireland. The Office is described by Facebook as the center of international operations and provides 'a range of online technical, sales, and operations support to Facebook's users and customers across Europe, the Middle East and Africa."[215] Further, the Statement is treated as an agreement between Facebook Ireland Limited and Facebook users residing outside the US and Canada,[216] signaling that this Dublin office works as an independent entity. Given the wide interpretation of an 'establishment', this becomes a clear case that Facebook Ireland falls within its ambit. Hence, processing of personal data from Europe, that would be carried out in relation to the activities of the Dublin office, among others, would be subject to the Directive.

This said, in its recent amendment of the Data Use Policy, Facebook has made it clear that Facebook Ireland Limited has been established and registered in Ireland as a private limited company and is the data controller responsible for the personal data of people outside the US and Canada.[217] Thus, Art.4(1(c) of the Directive would not be appropriate to our case as it deals with a scenario where the controller is not established in the EU.

[214] Kuczerawy (2010) p.75-85
[215] Facebook Newsroom (2012)
[216]Statement of Rights and Responsibilities, Art.19(1)
[217] Facebook, Data Use Policy

4.3 Facebook Basics and Some Privacy Concerns

Lilian Edwards would advise us that one way of understanding data protection issues in SNSs is to see their revenue source and business models.[218] Writers Enders et al classified the revenue models of SNSs into three major categories, i.e., advertising, subscription and transaction.[219] Advertising, in turn, can take two forms, namely affiliate models and banner advertising.[220] In the first model, an SNS steers traffic to an affiliate website and charges for the referral, and in the latter, advertisement is displayed on the SNSs.[221] Facebook mainly relies on advertisement as its main source of revenue. For instance in its statement on June 18, 2013, Facebook declared that it has over 1 million active advertisers.[222] Marketers and advertisers select target audience and Facebook, using its sophisticated mining technology and immense personal data of users, provide the targeted group. It is right here that the extent and quality/accuracy of personal data becomes very crucial for Facebook to strive, as the payment from the advertisers depends on, usually, the number of clicks, which in turn depends on the accuracy of selection. As the then EU Commissioner Meglena Kuneva Is quoted as saying in 2009, personal data is, as with Facebook, the "new oil of the internet and the new currency of the digital world."[223] As such, the privacy concerns of Facebook operations have, mainly, bean related to how it acquires the extensive personal data it processes and how it treats it afterwards.

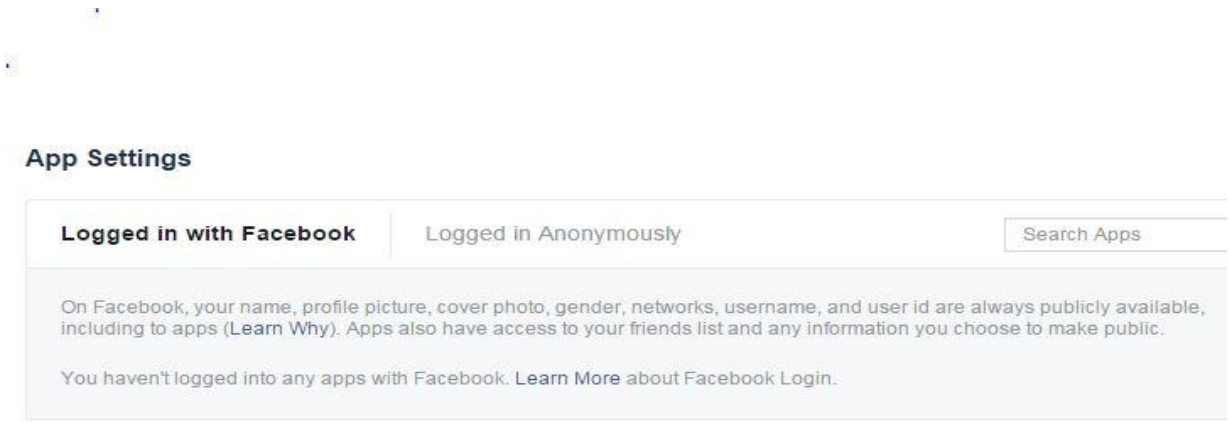
Many incidents have brought Facebook privacy issues into spotlight and takes different dimensions. The consequences of privacy lapses as well vary from simple discomfort and surprises to embarrassment and frustration; from reputational damage to identity theft; from loss of job and school disciplinary measures to suicides. Obviously, some features of the service infringe data protection principles more than others. Following are some of Facebook services that have been steering privacy related controversies.

4.3.1 Third Party Applications

Facebook allows third parties to develop applications, such as games, using its platform, as regulated under the 'Facebook Platform Policies'. Accordingly, Facebook allows application

[218] Edwards (2013) p.3
[219] Enders et al (2008) p.205
[220] Ibid
[221] Ibid, p.206
[222] Facebook Newsroom 2013
[223] Kuneva (2009) , Speech

developers to access personal data of its users, upon certain conditions. Among these conditions are that applications have their own privacy policy and that they obtain users' consent before using their data.[224] It also includes that they can use 'friend data (including friends list) in the person's experience' in their application.[225] Strictly personal data that Facebook has, nonetheless, labeled as 'public' are also available to apps, arguably in contradiction to the minimality principles of data protection. When users install some of these applications, they need to give their consent for the app to access their data. However, in some of them, the terms are not easily accessible or are not to be found as the Irish Audit Report on Facebook revealed in 2011.[226] In those cases, the legitimacy of processing is questionable on many grounds. Besides, some 'terms of use' do not inform users of the purpose of the vast access that the applications require from users, who have to either chose to accept it in its totality or not access the service. I have also observed that a great deal of apps are by default public, meaning anyone online can see that a user has installed the app. It is also bewildering wherefrom Facebook acquires a mandate to allow the applications to use friends' data as the screenshot below shows.



It is obvious that such third party applications can be held accountable as controllers. That being true, Facebook is facilitating the infringements. It is less likely that Facebook plays by the rules against the third party applications as it charges them 30% of their revenues for using the platform.[227] Such applications have been a subject of complaints in Ireland, the US and Canada, among others.[228] The finding of the Norwegian Consumer Council that many

[224] Facebook Platform Policy, 2 (1)
[225] Ibid (3(3)
[226] Irish Audit (2011) p.91
[227] Mahmood (2013) p.61
[228] Irish Audit (2011) pp.87ff

Facebook users are not aware as to the existence of these applications also strengthens a doubt if an informed consent is given for their access to personal data.

4.3.2 Timeline

In December 2011, Facebook introduced the timeline, which if effect is an orderly display of users Facebook history. Some of the difficulties that came with the introduction of timeline are spelt out as follows[229]: i) hiding mutual friends by users became impossible; ii) it is no more possible to limit the public view of cover photos and iii) specific time when friends were added and pages liked can be seen. These all have serious implications, for instance, on security of users. As a new feature, depriving users of controlling their accessibility is a significant data protection issue.

4.3.3 The 'Like' Button

Another feature introduced in 2010, the 'Like' button, according to Facebook, is a social plug in that web sites can use, where a click means sharing them on Facebook.[230] The system is tested for its efficacy in increasing traffic to sites and has been very popular among businesses.[231] If the one clicking is a Facebook user, the activity is reported in his/her News Feed to his/her friends. Moreover, when a logged in Facebook user visits a site with the 'Like' button, she/he is presented with "personalised content based on what their friends have liked, recommended, or commented upon on the site."[232] It is argued that such data gives Facebook an excellent clue on the preferences and interests of its users. It is difficult if such data that Facebook gets can be justified by consenting to the Statements given its far reaching effect.

4.3.4 The Changing Default Privacy Setting

One of the challenges of relying on consent as a justifying ground for the processing of personal data is that the prerequisites that data subjects read, understand and make an informed decision has been, in many ways, challenged. Thus, low rate of privacy policy reading and understanding is well documented.[233] In addition, even if users have a chance to control the accessibility of their data using the privacy setting that SNSs usually provide, for

[229] Mahmood, p.55
[230] "Like Button for the Web (2010)
[231] Roosendaal (2011) p.5
[232] Irish Audit (2011) p.81
[233] Custers et al (2013) p.440

different reasons, it might not be as used expected. For instance, in the UK, a research showed that more than half of SNSs users left their setting on default,[234] thus at the mercy of the respective SNSs. The reasons include difficulty in operating the system and frequent changes in the part of the SNSs.[235] As a result, user-friendly default setting serves as a safeguard instead of totally relying on consent, as the Working Party stressed.[236] This was also emphasized by the Council of Europe, where lack of privacy-friendly default settings was found to be one of the threats of the right to private life attributable to SNSs.[237]

Against this requirement, Facebook fares bad as, with successive changes in its setting, more personal data is rendered public.[238] As Facebook default setting stands at early January of 2015, the following can be observed. While future posts (status/photo/video/shared content) are visible to 'friends' and timeline posts are possible by 'friends'; tags review before it is posted on Facebook is set to 'off' and 'friends of friends' can see posts users are tagged in their timeline, resulting in less protection. However, there has been an encouraging development as well. For instance, the default setting of Facebook as outlined by the Irish report on Facebook in 2011, shows that status updates and posts were set to 'public'.[239]

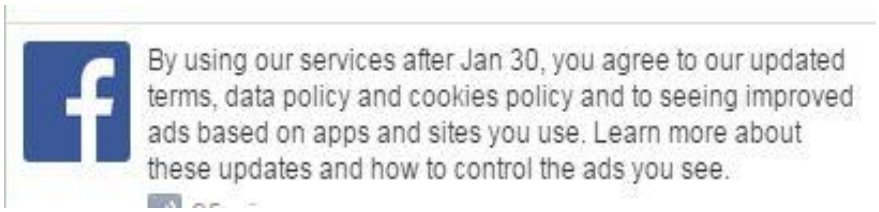
Surprisingly, 'life events' posts, including users' health and wellness are set as 'public', as are all 'likes', thus visible to, i.e., 'anyone on or off Facebook'. What is more, apps, plug ins, and instant personalization are, by default 'enabled'. However, unlike the situation prior to 2011, there are no more selected partner sites, upon users first visit, provide a personalized experience until they are turned off. In addition, the 'take a privacy tour,' prompt for new users is also encouraging.

As can be seen from the descriptions of the current default setting, there are some positive developments. However, the use of 'friends of friends' and the fact that health and family related posts are set to 'public' does not go in line with the minimal visibility that user-friendly settings demand.

[234] Edwards (2013) p.14
[235] Ibid, p.13
[236] WP163
[237] Joergensen (2014) P.4
[238] Edwards (2013) pp.15-16
[239] Irish Audit (2011) p.33

4.4 Facebook's Statement of Rights and Responsibilities and Data Use Policy

As the opening of the Statement reads, 'by using or accessing Facebook' users agree to the Statement, as updated from time to time in accordance with Section 14.' Supplementing this, Art.14(3) reads, 'your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms' and thereby gives Facebook an important leverage. The Changes may be posted on 'Facebook Site Governance Page', which only has some three million followers. Many times, what Facebook does is give a notice to users like in the screen shot herein below.



The Statement govern the relation between Facebook and users, applications developers, page administrators, advertisers, and sites using Facebook plug ins, with each referred to further information linked. Much of the Statement being on the responsibility of the other parties, users' issues of privacy are governed at first, though not fully. Thus, section 1 refers users to read the 'data use policy' concerning how Facebook collets and uses personal data with section 2(4) telling or warning users as to the effect of publishing content as 'public'.

Under the data use policy, the sources of information that Facebook collets include information required for registration; information shared by users as public and via friends adds, page or website likes, and some data that are treated as made public by definition, i.e. name, profile pictures, cover photos, gender, networks, username and User ID. Some reasons are given as to why these are treated as such, but only towards the end. The other sources of data being friends of users, the last source, presented in a condensed and ill structured paragraph, includes information from: running Facebook (messages, looking at others' timeline), 'time and location data from posts; visits to games and sites with Facebook platform and plug ins, and from advertising sites and affiliates. It is also vaguely provided that it may also be collected from 'click on, view or otherwise interact with *things (*emphasis added))'

Concerning the purposes for which Facebook uses users' data, it provides both a general and some instances of the purposes of using users' data. Thus, it can be used "in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use." Among the particular purposes mentioned, they include: helping people see and find things that you do and share, keeping Facebook safe and secure; to protect Facebook's and other rights, measuring or understanding the effectiveness of ads you and delivering them; for internal operations, including troubleshooting, data analysis, testing, research and service improvement. Sharing with others is also indirectly provided with some conditions like by 'by telling you about it in this policy'. Besides, towards the end, it is provided that Facebook may 'allow service providers to access information so they can help us provide services.' It is very important to note that 'information' is defined very broadly and circularly under the Statement as facts or other information about you, including actions taken by users and non-users who interact with Facebook (Art.18(3)).

Duration wise, Facebook stores data 'for as long as it is necessary to provide products and services to you and others'. The presentation of both the Statement and the data use policy is okay, excepting for certain parts. However, finding the terms and the data use policy is a bit tricky. For instance, it cannot be simply glanced from the timeline page.

From the above presentation, many important data protection relevant observations can be made. Below, I limit the discussion into consent related requirements under the Directive.

4.5. Do Facebook Operations Satisfy the Consent Threshold under the Directive ?

As discussed under the second chapter, for consent to justify the processing of personal data, it needs to be informed, given freely and informed. In addition, the way it is given should be unambiguous or, for sensitive data, explicit. At this juncture, It should be noted that these traits of consent, as envisaged in the Directive, are not easily susceptible for a meaningful measurement. Keeping this inherent challenge in mind, the opinions of the WP29, among others, provide important guides on general indicators of what 'informed' 'specific' or 'freely given' means in different circumstances. We should, therefore, use them, as appropriate.

To begin with the requirement that consent be 'freely given', the kind of consent that Facebook users give does not seem to satisfy the threshold. For consent to be considered as freely given, for instance, data subjects should have a real choice, where denying consent should not result in inability to access. This is far from the way Facebook, and indeed many SNSs, work. Users can only join Facebook by accepting its terms that include the data use policy. Frequent updates that Facebook introduces from time to time also do not give users a chance to deny consent without quitting the service completely. Quitting the service is not a choice *per se* as it means losing a social network that users have built, may be for free, for years.

Concerning the specificity of the consent that Facebook users give as required by the Directive, I have observed the following. As discussed above, the application of specific consent implies that users are able to indicate their authorization to different purposes that their data can be used for. This possibility is nonexistent in the way Facebook terms are accepted. Users are provided with different purposes for which their data can be used, but do not have a means to indicate which purpose they are willing their data to be used for. In addition, expressions like that users' data can be used "in connection with the services and features we provide to you' is very generic and, thus, against the requirement. Maybe, the possibility of limiting audience, specially the recently added 'only me' option can be a way to show some level of preference, but not a substantial one. I would strongly expect Facebook to provide a separate possibility of consenting mainly in relation to the collection and sharing of personal data with third parties as this is where complaints abound.

The last element of consent being that it be informed, it has, mainly, to do with sufficiency and presentation of information in such a way that data subjects can understand the implication of giving a consent. The way the the statement and the data use policy are presented, at least in terms of layout and font usage, my general observation is positive. However, there are serious issues that need a due consideration. First, the Facebook terms (both the statement and the data use policy) are not readily accessible from many pages of a Facebook account. Second, the fact that the Statement contains provisions addressed to individual users and others, mainly corporate partners, could be a source of confusion, and it would have been better for users to have it separately. Thirdly, the provision in the data use policy pertaining to third party apps as sources of information is not clearly stipulated and is written in a condensed way. Generic purposes like for 'research' 'improvement' are also

against the requirement. Lastly, it should be noted that the frequent changes that Facebook does on its policies and settings might not reach users. It seems that a better way of communicating users on developments that affect their interest, for instance, through email as Facebook has it already, could help in this regard.

Moving to the ways of indicating consent, the Directive stipulates that there should be a clear indication of one's consent. Applying this to Facebook operations, even if it can be argued that potential users' indication of consent by clicking the 'Sign up' sign amounts to unambiguous action, Art. 14(3) of the statement is particularly problematic, as 'continued use' including for possible changes in the terms, is considered as signifying consent. As this is a simple inaction, we can read ambiguity in it and, therefore, short of the Directive requirement. As the threshold in this regard is set to increase in the proposed Regulation, it is hoped that Facebook would change such terms.

Similar problem is noticed in relation to the processing of sensitive data that the Directive requires to be given explicitly. To begin with, Facebook does not separate its set of data as sensitive or otherwise and treats them equally. Moreover, the fact that posts regarding 'life events' that include health, which is a sensitive data under Art.8(1) of the Directive, is shared to 'public' by default is a clear contravention of the Directive.

From the forgoing discussion, it can be deducted that Facebook has a long way to go to comply with the European rules. Most importantly, it needs to improve its handling of users' data in relation with its partners. Much is also needed in informing users, providing them with options of giving consent in relation to specific purposes and making the terms easily accessible to users. The higher threshold and enhanced enforcement mechanisms envisaged by the proposed Regulation is hoped to tame some of Facebook's privacy related operations.

5 Conclusion and Recommendations

Data protection law is an emerging area of law that aims at safeguarding personal data of individuals against excessive and unwarranted access and use. Originally introduced as a means to curb government surveillance, it found a higher relevance with the increase in computational prowess of modern technological tools, the computer and the internet being the principal ones. More recently, the emergence of social networking service has made the protection of data protection very important and yet complicated

In Europe, successive laws have been adopted in this regard. The relevant laws reveal that personal data is protected as a matter of human right as much as for its economic ends. In relation to the second purpose, the increasing importance of personal data in the growing internet based services coincides with the creation of a single market in Europe. The 1995 Directive, therefore, has a purpose of ensuring that personal data of European is protected as much as it concerns itself with ensuring unfettered flow of data within the Union.

A broad material scope of the Directive means that it applies on controllers established in Europe, those from outside Europe, but have an establishment in Europe in relation to which processing occurs; and to those with no establishment in the EU, but use some equipments in Europe to acquire data. The Directive mainly works by imposing certain requirements, in a form of dp principles, on controllers and puts data subjects in the other end of the equation with certain rights in relation to the processing of the data that identifies them, even indirectly. Thus, for a controller to justify a processing of personal data, there needs to be some solid ground(s) that the law stipulates, consent from data subjects being one of the justifications and is frequently in use. Other data principles also are there to mitigate excessive processing.

As important as it is for individuals to be able to have a decisive say on data identifying them through consent, it has also proved to suffer some limitations. Among other, it is difficult to tell there really is consent with all its traits and this can be manipulated by controllers. This is specially so with the popular social networking sites that rack immense data from their users. With a view to mitigate such problems, the Directive demands that consent be specific to a

certain purpose, informed and given freely. Besides, it demands that indication of consent be given clearly, leaving no doubt, as a validity requirement.

Facebook, a leading social networking service, strives mainly on personal data of users. Users give their consent during registration and the terms they consent to dictate for future changes too. Some of Facebook's features manifestly fall short of the Directive requirements. The fact that it does not enable users to separately consent for different purposes; its treatment of 'continued use' as giving consent; its similar treatment of data regardless of sensitiveness; easily inaccessible terms and changing default setting that leave important personal data as 'public'; and its complicated relationship with third party partners are some of the issues that trigger uneasiness when assessed against the consent related requirements of the Directive. Hence, they need a due consideration from both Facebook and regulators besides an increased assertiveness and awareness of users.

With a new legal regime with a broader scope; detailed rules; higher threshold of consent, and harnessed enforcement mechanisms looming, it is expected that consent of users will be used in a way that protects them better.

6 Reference Table

Legal Instruments

Convention for the Protection of Human Rights and Fundamental Freedoms

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.

Directive 95/46/EC of the European Parliament and of the Council 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 (L 281, 23 November 1995, 0031-0050)

Charter of Fundamental Rights of the European Union of the European Parliament, December7, 2000, O.J. C 364, 2000

Books and Book Chapters

Bygrave Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limit.* The Hague, (Kluwer Law International) 2002

Bygrave Lee and Dag Wiese Schartu, *Consent, Proportionality and Collective Power* in in Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? London (Springer) 2009

Bygrave Lee A, *Data Privacy Law: An International Perspective*, Oxford (Oxford university press) 2014

Backman Christel, *Regulating Privacy: Vocabularies of Motive in Legislating Right of Access to Criminal Records in Sweden*, in Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds) Computers, Privacy and Data Protection: an Element of Choice, London (Springer) 2011

Brownsword Roger *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? London (Springer) 2009

Edwards, Lilian, *Privacy and Data Protection Online: The Laws Don't Work* ? in Lilian Edwards and Walden (eds) in L Edwards, C Waelde (ed) "Law and the Internet" (Third Edition, Oxford, Hart Publishing, 2009) pp.443-288

Fuster Gloria Gonzalez, The *Emergence of Personal Data Protection as a Fundamental Right of the EU*, New York (Springer) 2014

Hert P. De and S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* in Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? London (Springer) 2009

Leenes Ronald and Isabelle Oomen, *The Role of Citizens: What Can Dutch, Flemish and EnglishStudents Teach Us About Privacy*? In Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? Springer, 2009

Kuczerawy, A. (2010) *Applicable data protection law in a relationship between EU users and no Social Networking Site*' in M. Bezzi et al. (Eds.): Privacy and Identity (IFIP AICT 2010), pp. 75–85

Mahmod, Shah, *Online Social Networks: Privacy Threats and Defenses*, in Security and Privacy Preserving in Social Networks, (ed) Richard Chbeir and Al Bouna (2013), Springer

Nouwt Sjaak, *Towards a Common European Approach to Data Protection: ACritical Analysis of Data Protection Perspectives of the Council of Europe and the European Union* in Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? London (Springer) 2009

Rouvroy Antoinette and Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in Serge Gutwirth, Yves Poullet, Paul De Hert, ·C´ ecile de Terwangne and Sjaak Nouwt (eds) Reinventing Data Protection? London (Springer) 2009

Solove, D.J.. The digital person. Technology and privacy in the information age. New York (New York University Press). 2004

Solove, Daniel J. Understanding Privacy. Cambridge (Harvard University Press) 2008

Swire, P, and Robert Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Data Directive, Washington, (Bookings Institution Press) 1998

Purtova Nadezhda, *Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Information, and Ambient Intelligence* in Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds) Computers, Privacy and Data Protection: an Element of Choice London (Springer) 2011

Articles

boyd D, N Ellison, *Social Network Sites: Definition, History, and Scholarship'* Journal of Computer-Mediated Communication, Vol. 13(1) (2007)

Bergkamp Lucas, Hunton, and Williams, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, Computer Law and Security Report, Vol.18, No.1 (2002)

Bygrave, Lee, *The Place of Privacy in Data Protection*, Computer Law & Security Report, Vol.17 (2001)

Bygrave Lee. *Privacy and Data Protection in an International Perspective*. In: Scandinavian Studies in Law Vol. 56 (2010)

Custers and et al, *Informed Consent in Social Media Use – The Gaps between User Expectations and EU Personal Data Protection Law*, Scripted Vol. 10, Issue 4 (2013)

Culnan M.J., '*Protecting Privacy online: Is self-regulation working?*' Journal of Public Policy Market, Vol. 19 (2000)

Daniel B and et al, *Data Protection: The Challenges Facing Social Networking*, 6 Internet Law & Management review Vol. 6 (2010)

Edwards, Lilian, Privacy, *Law, Code and Social Networking Sites*, Electroni copy available at Electronic copy available at: http://ssrn.com/abstract=2200163 (2013)

Enders Albrecht, Harald Hungenberg, Hans-Peter Denker, and Sabastian Mauch, *The Long Tail of Social Networking: Revenue Models of Social Networking Sites*, European Management Journal, Vol. 26 (2008)

Grimmelmann James, Saving Facebook, Iowa Law Review, Vol. 94 (2009)

Hon (2011) W Kuan, Christopher Millard and Ian Walden. *The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1*' (March 10, 2011) Queen Marry School of Law Legal Studies Research Paper No. 75/2011, <http://ssrn.com/abstract=1783577 (2014)

Hustinx, Peter J. *Data protection in the European Union* Privacy & Informatie 2 (2005)

Kokott Juliane and Christoph Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,* International Data Privacy Law, Vol. 3, No.4, 2013

Moerel (2011a) Lokke. *The Long arm of EU data protection Law: Does the Data protection directive apply to processing of personal data of EU citizens by websites worldwide?* In: International Data Privacy Law. Vol. 1. No. 1 (2011)

Moerel (2011b) Lokke. *Back to Basics: when does EU data protection law apply?* In: International Data Privacy Law. Vol. No. 2. (2011)

Romano Fabio Balducci, *The Right to the Protection of Personal Data: a New Fundamental Right of the European Union*, (2013) Electronic copy available at: http://ssrn.com/abstract=2330307

Roosendaal A, '*Facebook Tracks and Traces Everyone: Like This*!' Tilburg Law School research paper (2010) Electronic copy available at: http://ssrn.com/abstract=1717563,

Rubinstein Ira S. and Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, New York University School of Law Public Law & Legal Theory Research Paper Series Working Paper No. 12-43 (August 2012) Electronic copy available at: Electronic copy available at: http://ssrn.com/abstract=2128146

Schwartz Paul M. *European Data Protection Law and Restrictions on International Data Flows*, Iowa Law Review Vol. 80 1(995)

Tucker Catherine, *Social Networks, Personalized Advertising and Privacy Controls* (2014) Electronic copy available at: http://ssrn.com/abstract=1694319

Other Documents

Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 Final. Available http://www.europarl.europa.eu/registre/docsautres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf

Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data* adopted 20 June 2007 (WP136)

Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor'* adopted on 16 February 2010 (WP169)

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

Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent* adopted on 13 July 2011 (WP187)

Article 29 Data Protection Working Party *Opinion 05/2014 on Anonymisation Techniques* Adopted on 10 April 2014 (WP216)

Internet Sources

Tsaoussi Aspasia, *Facebook, Privacy and the Challenges of Protecting Minors on Social Networking Sites,* A paper presented in the 4th International Conference on Information Law (Thessaloniki, 20th & 21st May 2011) Available at http://ssrn.com/abstract=1878035

European Commission, Progress on EU data protection reform now irreversible following European Parliament vote, March 12, 2014, available at http://europarapid/press/release-MEMO-14-60_en.htm

Media Bistro, Twitter v Facebook: Key Stastics, Facts and Figures, available at http://www.mediabistro.com/alltwitter/twitter-vs-facebook-stats_b60825 (2014)

Kuneva Maglena (2009), 31 March Speech, available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/%20.

Irish Data Protection Commissioner, Facebook Ireland Ltd Report of Audit (2011) at http://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

Al Franken, Facebook's Proposed Privacy Plan Puts Users at Great Risk, available at http://www.huffingtonpost.com/al-franken/facebook-privacy-franken_b_834769.html

Facebook Developers, "Like Button" (2010) available at http://developers.facebook.com/docs/reference/plugins/like

Facebook Newsroom, Measuring Facebook's Economic Impact in Europe (2012), at http://newsroom.fb.com/news/2012/01/measuring-facebooks-economic-impact-in-europe/

Jammet Adrien, The Evolution of EU Law on the Protection of Personal Data, Centre for European Law and Legal Studies (CELLS) Online Papers (2014) available at Electronic copy available at: http://ssrn.com/abstract=2501417