UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

‘We have updated our privacy policy’

An analysis of the suitability of Privacy Policies, as End User License Agreements, to provide transparency as required in the General Data Protection Regulation.

Sofia Eriksson

Supervisor
Kristoffer Schollin

Examiner
Ulf Petrusson

Department of Law
Master of Laws Programme
Master Thesis
30 ECTS
Autumn 2018

Abstract

The General Data Protection Regulation presents transparency as a tool for data subjects to become informed and in control of their privacy through their personal information. Within this thesis the possibility of providing transparency for data subjects, as required within GDPR, is questioned based on the suitability of using privacy policies formed as End User License Agreements (EULAs) as the tool providing transparency. Privacy policies as EULAs are argued to not be suitable for providing the adequate transparency, identified as required in order to meet the demands of the regulation, due to the issues inherent in the structure of EULAs as liability waivers, often with diffuse and ambiguous language as well as the fact that they are often not even read by the users. It is further argued that the structure and format of privacy policies need to diverge from the current form of EULAs and develop into more suitable forms enabling the data subject to easily comprehend the information aimed to be provided through the transparency requirement in the GDPR.

Abbreviations

AI	Artificial Intelligence
Article 29 WP	Article 29 Data Protection Working Party
CNIL	The National Commission of Informatics and Liberty
CSR	Corporate Social and Environmental Responsibility
DPA	Data Protection Authority
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
EULA	End User License Agreement
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
OECD	Organization for Economic Co-operation and Development
PETs	Privacy Enhancing Tools

Abstract

Abbreviations

Table of Contents

1. Introduction

1.1 Transparency in the Privacy Context

The answer to two simple questions can serve as an explanation to the general perception of the privacy context. Firstly, how many privacy policies, regulating the use of your personal information, have you read, word for word, in the last year? If your answer is more than a handful it is likely due to curiosity, a specific work-task or because you are writing a thesis like this one. Secondly, how many privacy policies, by entering into a service, have you agreed to in the last year? Simply think about the number of times you have ordered something online and the amount will quickly add on. Collection of personal information is done through almost all services used by an individual, from using social media to ordering products through web-shops or simply by shopping for groceries with a members-card. The companies collecting the information, in order to tell us what to purchase next or even to let you know when you are pregnant,[1] conduct the usage of this information. The awareness and participation of the individuals presenting this opportunity, by surrendering personal information, is however not as intentional, which is reflected through the answers to the two initial questions. The privacy context is a field where possibilities to use personal information constantly evolve, it is also largely left undisturbed by the enablers, the individuals.

With the new General Data Protection Regulation (the GDPR), enforced by the European Union (EU), fairly ambitious goals are set in regards to the protection of individuals privacy and the ambition of enabling a prospering market for data.[2] These two aims are to be accomplished through specific demands on how companies, acting within the market, communicates to, and thereby generates transparency for, individuals, creating '*informed natural persons'*. [3] This transparency is to be reached through information provided, from companies to the individuals, regarding the usage of their personal information collected as data.[4] Thus, transparency is to function as a tool for individuals to control their personal information. The information regarding the use of personal data, that is to be provided between companies and data subjects using their services, is today most frequently presented through a company's privacy policy.

Despite the day-to-day occurrences with privacy policies for individuals using online services the general perception and fact remains that they are simply not read, some studies arguing that

[1] Larsson, Ledendal. (2017) Personuppgifter som betalningsmedel, p. 20. For instance Target recommended pregnancy related products based on patterns viewed through data, to a, not publicly known, pregnant teenage girl.
[2] The GDPR, recital 1, 2, 3.
[3] The GDPR, recital 39; Individuals will be used as synonym with *data subjects* as well as *users* through this thesis and includes all natural persons as framed to be protected in the GDPR, *on the protection of natural persons*.
[4] The GDPR, recital 26 and article 4 (1) specifies what is included in the term *personal data*. Henceforth used collectively with *personal information*.

they are even seldomly opened by the expected reader.[5] With the emphasis of the regulation being placed on transparency, the ability to reach said aim perceives to be a challenge if the information lacks the ability to reach the data subject when presented in an unopened privacy policy.

The GDPR does not set specific limits or provisions on how the information aimed to provide transparency should be presented to the data subject in terms of method or structure. Although most companies provide the information in privacy policies separated from the Terms and Conditions, or similar End User License Agreements (EULAs), as desired by the GDPR,[6] the structure of the privacy policies and EULAs are in many aspects alike. An EULA has as its primary goal to regulate how the user of a service can de facto use the service, thus create a binding agreement. In a similar way a privacy policy regulates how the data subject's personal information will be collected and processed. They are consequently both contracts regulating actions towards or by the company, therefore also sharing the formal portrayed structure of a contract. This thesis will therefore discuss privacy policies as being structured in the form of EULAs throughout.

Since the GDPR places no emphasis on the specific method of providing privacy information, the use of privacy policies in the form of EULAs remain valid as long as the provisions in the regulation are followed concerning the content and time frame demanded for providing the information.[7] The idea of EULAs, as a format, being sufficient for reaching the transparency required by the GDPR, is questioned in the following presentation due to the mentioned common perception and numerous studies showing that data subjects tend to never read the attached agreements, including privacy policies, when entering into services and applications online. With the new regulation putting more emphasis on control through the *informed data subject,*[8] a conflict is created if the data subject refrain from even reading the information and thus remains uninformed. It can therefore be questioned if EULAs can constitute the most efficient way of providing information and if it is even a suitable method within a regulation that aims for transparency between provider and user through information.

The structure of privacy policies has long been viewed as difficult and diffuse, hence in need of a change.[9] The new regulation, the GDPR, offers guidance on what minimum information should be provided as well as additional requirements on what content to provide to the data

[5] Bakos, Marotta-Wurgler and Trossen (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014): p. 33.
[6] The GDPR, recital 70, article 21 (4).
[7] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.14 (24); Article 29 WP, Guidelines on consent under Regulation 2016/679, p. 13, 3.3.2.
[8] The GDPR, recital 60.
[9] E.g. see, OECD (2006), "Making Privacy Notices Simple: An OECD Report and Recommendations", *OECD Digital Economy Papers*, No. 120, OECD Publishing.

subjects.[10] How to best give insight into the privacy and data collection-conundrum and to render control to the data subjects is also a part of the general privacy debate.[11] However, providing the right content to inform the data subjects is not sufficient as long as the information tool available or used cannot provide information in a way that renders adequate transparency.[12]

1.2 Adequate Transparency

The GDPR have enforced transparency as a key component of the privacy legislation through increased demands on transparency of information. The transparency demanded is thus aiming at creating an informed data subject. The previous discussions, within the privacy debate, concerning providing information for transparency reasons, has mainly centred on acquiring consent. More specifically regarding how to make sure that the consent is based on an informed choice.[13] Bechmann has claimed that the consent provided based on information in an EULAs is a '*non-informed blind consent'* due to the lack of understanding amongst data subjects in regards to what they consent to.[14]

Solove explains it in terms of '*The problem of the Uninformed Individual'*.[15] Both of these phrases aims at catching the inherent problem with giving valid consent in an uninformed situation and form the previous focal point for discussing transparency within privacy legislations. This criticism of the privacy legislation can be argued to be addressed with the demand of transparency, creating informed data subjects in all aspects of data collection, not only through consent.

The broad implementation of transparency in the GDPR, through an increase of transparency in terms of information generally and as mentioned not only when collection is based on consent, aspires to inform the data subjects and thus generate considered actions. The issue of data subjects being uninformed should therefore be solved by the general information requirement of transparency in the GDPR. With increased transparency requirements, the responsibility shifts to the data subject and allows them to make informed, comprehensible choices based on transparent information about the usage of their data. This is further highlighted through the demand on '*informed consent'*.[16]

[10] The GDPR, article 13,14.
[11] Datatilsynet, The Great Data Race – How commercial utilization of personal data challenges privacy, p. 46.
[12] See 1.2 below for a definition of adequate transparency.
[13] The idea of *informed choice* is also known as *transparency and choice* or *notice and consent* as a form of regulating transparency. For explanation see Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011): p. 34.
[14] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014).
[15] Solove. 'Introduction: Privacy Self-Management and the Consent Dilemma.', *126 Harvard Law Review*, (2013): p. 1883, section A.,1.
[16] Article 29 WP, Guidelines on consent under Regulation 2016/679, p.13 (3.3.1).

The informed consent is hence dependent on the transparency to provide information and create comprehensible knowledge for the user to be able to provide consent.

However, issues have been acknowledged regarding transparency and what it entails and possible negative effects, e.g. information overload.[17] In order to understand the purpose of the requirement, the components and abilities of transparency will be discussed throughout, emphasizing that complete transparency in itself is not the solution to uninformed data subjects.[18] Thus, it is necessary to provide comprehensible information through transparency in order to reach this informed consent, and an informed user when collection is based on another legal foundation, steering away from creating a blind, non-informed consent. The transparency sought within the GDPR will therefore be phrased as '*adequate transparency'*.[19] It will hence be further evaluated if this adequate transparency can be reached through the transparency provisions of the regulation and the customary form of delivering privacy policies as EULAs. The phrase therefore aims at the balance between too much information and too little transparency, enabling the user to comprehend enough to make a deliberate choice to use the service, or to consent, or not. The phrase will also be used to separate the general idea of transparency, as will be evident in the privacy legislation discourse and in previous legislation, from the one aimed to be created through the GDPR.

1.3 Purpose and Research Question

The purpose of this thesis is thus to evaluate if the functionality and form of privacy policies as EULAs are suitable for providing the data subject with the information and transparency required by the GDPR and thereby render adequate transparency for the users to control their personal information and make deliberate choices.

The purpose will be discussed and reached in three steps. Starting with *the demands of transparency placed on the agreement*, viewing what and by which means the regulation aims at generating, as formulated in this thesis, adequate transparency. Secondly, *the agreement presented to the data subject*, how the transparency is shown and provided in privacy policies which will be done by determining and viewing necessary functional criteria needed within the agreements in order for them to have the possibility of providing adequate transparency. Finally, *the functionality in practice* through the comprehensibility by the data subjects, which will be based on the two previous steps, will be addressed.

[17] E.g. Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014); see section 4.1 below.
[18] Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011): p. 36. Where Nissenbaum argues that transparency not solution in itself.
[19] This phrase is created by the author with the aim of framing the transparency as interpreted through the GDPR in this thesis.

1.3.1 Research Question

Can privacy policies, in the form of end user license agreements, generate adequate transparency to meet the demands of the GDPR?

As will be evident in the results below there is also a need to address these additional questions,

What possible adjustments can be made to the existing formal structure of privacy policies in order to reach transparency?

And within this,

Can any examples of privacy policies considered to be 'best practice' in providing transparency, be found?

1.4 Theoretical Framework and Method

1.4.1 Theoretical Framework

The privacy discourse is closely connected to the rapid evolvement of the possibilities of use of data. With this there are subsequently questions raised regarding the ability of companies, using the data, being able to inform the data subject in an adequate and transparent way in order to reach informed data subjects and gain informed consent. The reoccurring theme within the discourse of privacy legislation is therefore also the balance between controller and data subject, and the probability of keeping the data subject up to speed in regards to the usage of their personal data through privacy policies in form of EULAs.

Within the discourse of privacy legislation, scholars have continuously pressed on the construction of privacy legislation as being reliant on the data subjects active participation, to constitute an insufficient form for regulating privacy.[20] Adjoining debates on the technical evolution around data and the possibilities that has been created through this evolvement have added to the discussion on how, as well as if, privacy should be regulated at all.[21]

[20] Rauhofer. 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?' *European Data Protection Law Review,* vol. 1, no.1 (2015): p.14 f.; Solove. 'Introduction: Privacy Self-Management and the Consent Dilemma.', 126 Harvard Law Review, (2013), *the consent dilemma*.

[21] E.g. see Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011): p. 34. Explained as the paradigm of regulation through notice and consent with the free market.

The criticism on how privacy legislation is constructed today can be seen through Bechmann's argument that a blind eye was turned, by the legislator, towards the tendencies of data subjects actions online, when constructing the demands on transparency in the GDPR.[22]

The perception of the privacy legislation being that it is both demanding and at the same time empowering, through the requirement on the data subject to participate. This construction has been argued to be a naïve ideal which have been further supported by the research portraying the lack of ability for data subjects to access the black box of data collection,[23] and comprehend enough of the collection, processing, aggregation and use to thereafter act purposefully through a consequence and impact analysis. Additionally, the debate has also focused on the data subject's lack of interest in participating in a self-management legislation with major corporations as opponents. The unwillingness has further been argued to lead to the data subjects simply giving consent unknowingly, in order to access the service, leading to a non-informed consent culture.[24]

The theories mentioned are all concerning the issue of creating an effective, self-management, privacy legislation due to the unwillingness of participation shown by the data subjects. These prevalent issues will here be collectedly phrased as *actively uninformed data subjects*,[25] with the opposing objective being *informed data subjects*.

It is therefore within this setting, concluding that the legislation demands action from an unwilling data subject that is unable to comprehend what they are supposed to be in control of and decide over, that this thesis will evaluate the transparency requirement within the new regulation, the GDPR. The suitability of privacy policies as EULAs is to be evaluated from the paradox created in the theoretical setting of how privacy legislation is constructed and functioning. The functionality will be discussed in relation to the corporations, as collectors, ability to provide information on the collection of the object, the data, to the provider, the individual data subject and by this generate adequate transparency.

1.4.2 Method

The basis for the research method will be the legal requirements within the GDPR, this since it is necessary to clearly adhere to the requirements in order to answer the research question of whether the execution, in form of privacy policies, adheres to the goal of transparency implemented by the increased transparency requirements.

---

[22] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 35.
[23] Pasquale. *The Black Box Society*, p.9f.
[24] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p.21, 34.
[25] Also phrased as *uninformed* throughout.

Additionally, the GDPR, despite its territorial limitations, is a wide spanning regulation. The globalization and possibility to access different markets through the internet have enabled companies to act with little physical limitation. It is thus likely that the GDPR will have a global impact due to its applicability on not only the privacy policies prevailing from companies based in the EU but also on the global actors present on the EU market.[26] The discussion will consequently not be limited to an European perspective on how privacy is discussed and construed but rather a global one in order to include the likely impact of the GDPR.[27]

Therefore, the regulation of topic, the GDPR, will be discussed through its own regulatory setting in the EU and its member states as well as from the perspective of the US. This since both the EU privacy legislation and the US privacy legislation have been part of the debates held by scholars, organizations and government agencies regarding privacy and privacy policies for decades.[28] This does, however, not mean that the thesis aims at being a comparative discussion from these areas but rather that the subject and questions at hand are not conformed to a national issue in its essence and thereby neither is this thesis limited to a national perspective.

In order to answer the research question, the method will include studying sociological, legal and economic factors impacting the possibility to provide adequate transparency for data subjects. Both economic aspects, in regards to the market created on data and the cost of time, as well as sociological aspects through moral and behaviouristic discussions is prevalent when addressing privacy issues. Since privacy has evolved to impact both the economy as well as the social demeanours of individuals these factors are highly relevant and crucial to include when presenting a discourse evaluating the legal tools within privacy legislation.

In order to evaluate the demands created through the transparency requirement within the GDPR, the legislation will be viewed through the replaced directive,[29] the initial recitals of the GDPR as well as with the guidelines provided by the Article 29 Working Party (Article 29 WP)[30] for interpretation of the regulation. The regulation will thus be interpreted literally and from the aim of the legislation as well as from an economic and sociological approach in relation to the transparency requirement.

[26] The GDPR, article 3.
[27] Chen, 'Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them', *the New York Times* (2018).
[28] The OECD formed their guidelines in the 1970s with the FTC quickly following with the adoption of the their FIPPs steering privacy regulation; McDonald and Cranor. 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* vol. 4, no. 3 (2008): p. 546.
[29] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Henceforth Directive 95/46/EC.
[30] Now the European Data Protection Board (EDPB), the documents referred to was concluded whilst named the Article 29 WP they will be referred to as such throughout the thesis.

This in order to reach a clear picture of what the GDPR actually requires e.g. in regards to providing transparent information in a '*concise, easily accessible and easy to understand, and (…) clear and plain language*'[31] way.

In order to tie the legal frame together with the socio-economic incentives steering the data subjects, privacy policies as a tool will be evaluated from a functionality aspect presented in a taxonomy. The privacy policies structure as EULAs and their functionality will be evaluated from criteria selected based on their perceived ability to enable adequate transparency. The criteria have been chosen based on the demands set out in the GDPR along with the recommendations provided by the Article 29 WP for providing transparency as well as the privacy debate in relation to the regulations. The privacy policies have been read from the aspect of each criteria and evaluated as meeting the criteria or not, in order to present an overview on how they comply with the features enabling adequate transparency. Furthermore, the criteria have been discussed in order to show the difficulty of providing a specific measure of what is necessary in order to generate adequate transparency. The taxonomy will also function as a guide to further discussions on how the privacy policies function as an instrument in complying with the demand in the GDPR of providing the data subject with adequate transparency.

The findings in these three sections will be incorporated in the discussion on the suitability of privacy policies for providing adequate transparency and the assessment on possible alterations that would create more transparency in privacy policies used today.

1.5 Material

In relation to the GDPR and the demand for transparency, the main source of materials used for this thesis is the legislation, The General Data Protection Regulation (the GDPR). [32] The GDPR is complemented with the Article 29 Data Protection Working Party Guidelines and the EU Handbook on Privacy.[33] Guidance for elaboration on the requirements have been found in the discussions from the EU Commission and Parliament leading up to the implementation of the regulation.[34]

[31] The GDPR, recital 58.
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation).
[33] Article 29 WP, Guidelines on transparency under Regulation 2016/679; Article 29 WP, Guidelines on consent under Regulation 2016/679; EU Publications, Handbook on European data protection law, 2018 edition.
[34] E.g. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling; European Commission - Press release, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.

Additionally, in order to conduct the evaluation of the functionality of privacy policies, in providing adequate transparency, eight policies have been selected and studied from a set of specific criteria. The selected privacy policies are all derived from corporations with an strong global coverage as well as a with businesses dependent on information in different variations, these chosen companies are: Apple, eBay, Google, Microsoft, Netflix, Spotify, TripAdvisor and Twitter. The criteria are further questioned and evaluated in their own regards but also to some extent on how they impact one another.[35]

The discussion and analysis in relation to the regulation, the privacy policies and the outcome of these, have been held in relation to articles and reports by legal scholars as well as governmental actors globally. The publications have been chosen to reflect the legal impact and considerations needed when discussing privacy as legal phenomena and its strong connection to the surrounding areas of society.

1.6 Restrictions

Since the subject of privacy is connected to various different aspects, both legal and within sociological and economic disciplines, as well as to information and surveillance, the restrictions of this thesis are aspired to be clearly emphasized. The focus of discussion will be strictly on the legal transparency requirements presented in the GDPR from a consumer perspective, i.e. the individuals who access and use the services regulated through the privacy policies.

Additionally, the discussion presented will be based on the perception and accessibility that these data subjects can assimilate through the privacy policies. Therefore, focus will be placed on the GDPR recitals and articles addressing transparency and the discussion revolving transparency through information held within the regulation and by scholars with focus on the format of the presented privacy policies.

When analysing the companies' agreements, the only aspect of discussion will be the privacy policies, therefore disregarding the terms of services and other similar agreements that may also be provided. Since the discussion on suitability revolves around the use of the EULAs as a structure for presenting the privacy policies there will be some overlap between the use of the abbreviation EULA and privacy policies. EULAs will be used when discussing the structure of the text, hence when addressing the document, its appearance and function. Privacy policies will be used when discussing the inherent function and aim of said text, additionally when simply discussing a specific privacy policy. When considering EULAs in this thesis they are therefore perceived to be used for regulating privacy issues as privacy policies.

[35] See chapter 3.

Within this thesis, the perception will be that privacy policies and EULAs are structured coherently and no further separation of content or definition in regards to the two phrases will be made.[36]

Furthermore, focus will not be to discuss the obligations the GDPR places on a company per se, rather in the setting of what the data subject can expect in terms of transparency through the GDPR. The regulation demands placed on companies collecting information not connected directly to the data subject, e.g. the need to provide documentation to Data protection officers and provide a contact person, falls outside of the scope of this thesis. So does also the articles within the GDPR not demanding nor connecting to the transparency requirement and therefore not contributing to the discussion of adequate transparency for the data subjects.

Questions regarding the legislators, enforcers or company's role in relation to transparency and privacy policies is thus only mentioned when necessary to address the data subjects understanding or interpretation.

1.6.1 Adjoining Research

The new privacy regulation, the GDPR, have prior to its enforcement, as well as since, been a popular subject for legal scholars both in terms of lawyers consulting companies as well as academics regarding implementation and the rights of the data subject. There has been a broad span of issues up for debate, many of them relating to the currency traded and regulated through the regulation, data.[37] Furthermore, sociological discussions regarding how the data subjects act and become informed have been subject to several studies linked with behavioural aspects of who reads the EULAs as will be seen throughout.[38]

Despite the occurrence of research regarding information and transparency, it has been conducted on a general level regarding privacy legislation issues, such as the validity of consent, and not specifically focused on the possibility rendered by the GDPR to provide transparency through privacy policies as EULAs. The research regarding information and transparency in relation to the data subject have functioned as guidance in conducting the following discussion.[39]

[36] See section 1.1 above for the view on EULAs and privacy policies similarities.
[37] E.g. Larsson, Ledendal. (2017) Personuppgifter som betalningsmedel.
[38] E.g. Bakos, Marotta-Wurgler and Trossen (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014); Forbrukerrådet, 250,000 words of app terms and conditions, May 2016.
[39] E.g. Löfgren, E., 'Samtycket enligt den allmänna dataskyddsförordningen, Personuppgiftsansvarigas ansvar och registrerade personers rätt till öppenhet och självbestämmande'; Larsson, S., 'DATA/TRUST: Tillitsbaserad personuppgiftshantering i den digitala ekonomin', Handelsrådet, research projekt 2018-2020; Larsson, Ledendal. (2017) Personuppgifter som betalningsmedel.

1.7 Disposition

Chapter two aims at presenting the legal framework regulating transparency from both consent and comprehensibility as the legal ground for processing but also the connection to trust and information. With this chapter the possibilities and aim found in the regulation will be lifted in order to further understand the practical application of the regulation in privacy policies as EULAs.

Chapter three further shows how the privacy policies are structured as EULAs and to what degree and aspect they can meet the requirements of providing the data subjects with information and transparency. These discussion will be based on the chosen criteria and their functionality of enabling adequate transparency.

Chapter four will address the challenges that are connected with informing data subjects through privacy policies as EULAs and specifically how these challenges are connected to transparency.

Chapter five discusses the suitability for adequate transparency to be given through privacy policies as EULAs and responds to the first research question based on the presentation within previous three chapters.

Chapter six concludes the possibility of privacy policies as EULAs meeting the goal of transparency, as put forwards by the GDPR, discussing the two subsequent research questions from possible solutions and adaptions to the contract form as well as from identified 'best practice'.

Chapter seven then concludes the discussions presented in chapter four to six in order to determine the possibility of privacy policies as EULAs reaching an adequate transparency for the data subject in accordance with the GDPR.

2. The GDPR and the Transparency Demands

2.1 Introduction

The enforcement of the GDPR, by the EU, was acknowledged and discussed by not only regulators, enforcers and companies but also by individuals. As May 25th 2018 approached, individuals within the EU had their mailboxes flooded with emails from companies that they were frequently in touch with as well as companies that they seemingly had never heard of. The content of the emails were more or less unanimously, '*we have updated our privacy policy*'.

This wave of emails responded to the urgent demand within the regulation to deliver transparency on how the company handle the personal data they had collected at one time or another and to provide transparency through informing the data subject about the fact that the company had information on the data subject. The effect of the enhanced demand of transparency through information in the GDPR was at once evident.[40]

Amongst the data subjects receiving information about updated policies, it appeared that many of them lacked knowledge about the fact that the company even had information about them.[41] This fact is also an argument in favour of the theory of data subjects being uninformed.[42] Another noted effect of the red flag in mailboxes, signalling updated privacy policies, was the lack of companies actually going through the trouble of informing how the policy, on handling personal information from the data subjects, had changed. Instead most companies referred to the privacy policy for the data subject to read, available at their website. At the best of times the privacy policy was added as a link to the information email. The requirement of informing data subjects about changes have thus been incorporated in the taxonomy and will be discussed in relation to reaching adequate transparency in chapter three and four.[43]

The following section aims at elaborating and clarifying the enhancements that generated the flood of mails from companies. This will entail how information and transparency are required within the regulation and what effects it aspires to have on creating an informed data subject. Initially a brief summary of how transparency in the previous regulation, the EU Data Protection Directive 95/46/EC (the directive), relates to the replacing regulation, will be provided in order to grasp the context of the enhancement. Thereafter transparency in the GDPR will be discussed from the concept of consent, comprehensibility, trust, information formulation, content and access.

2.1.1 Background of Transparency

The directive[44] is the predecessor to the GDPR and was adopted by the EU in 1995. The directive had, as with all directives, a more lenient demand on uniformity between member states aiming for harmonization, resulting in each member state adopting individual data protection laws.[45] However, the specific laws in the member states were to adhere to the two-folded perspective of preserving rights of individuals and enable free economic movement, as

[40]The GDPR, article 12-14; Kelion, L., 'How to handle the flood of GDPR privacy updates', *BBC* (2018); Chen, 'Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them', *the New York Times* (2018).
[41] Companies now asking for consent to continue sending emails despite never receiving explicit permission in the first place. Hern, A., 'Most GDPR emails unnecessary and some illegal, say experts', *The Guardian* (2018).
[42] Solove. 'Introduction: Privacy Self-Management and the Consent Dilemma.', *126 Harvard Law Review*, (2013):p. 1883, section A.,1.
[43] See taxonomy, 3.5 Analyzing the Privacy Policies; 4 Challenges of Informing Data Subjects through EULAs, 4.4 Ignorant Data Subjects and the Privacy Paradox.
[44] Directive 95/46/EC.
[45] In Sweden Personuppgiftslag (1998:204).

it constituted the overall harmonization goal within the directive.[46] This foundation of protection of personal data remain in the GDPR and is most evidently seen in the demand for transparency, which will be elaborated below. Furthermore, the recitals of the directive remain intact and applicable in the interpretation of the new regulation, the GDPR. Additionally they contain the function of explaining in what context the new regulation was established from.[47]

Unlike the previous directive, which also demanded data subjects to consent to certain collection of information, the GDPR has a stricter requirement on consent, that it is informed. Thus, through its direct applicability to all companies collecting data within the EU it ensures the information to be equal to all data subjects through the demands it put forward on transparency and information.[48] It is however, not only the applicability that has increased, also the types of information necessary to provide and the demands on when to do so has expanded and through this the transparency demand is strengthened.[49]

The most notable enhancement of transparency can be connected to the flooded mailboxes, unlike the directive, the GDPR demands not only that the information is provided at the time of the collection but also that a minimum set of what information is to be provided. These two requirements result in the fact that changes, concerning how a company collects or uses personal information, i.e. changes in their privacy policy, requires the company to inform affected data subjects, hence, all data subjects that the company have any information about. [50] The novel requirement of specific information to be provided to the data subject resulted in the updating of most companies privacy policies and subsequently, in flooded mailboxes for the individuals.[51]

The privacy debate has, as briefly mentioned in the introductory chapter, been ongoing globally.[52] Therefore, although the GDPR derives most recently from the previous EU legislation, the directive, the European legislation has a lot of common traits with the global privacy discourse. The discourse originates from the OECD guidelines,[53] the FTC principles, FIPPs[54] and still prevailing in the idea of Privacy Enhancing Technologies (PETs) as privacy enhancing tools.[55]

[46] Directive 95/46/EC, recital 7, article 1.
[47] The GDPR, recital (9).
[48] The GDPR, article 3.
[49] The demand to inform about the data subjects rights, when to inform the data subject, inform the data subject about who the collector is are all new features of the EU privacy legislation.
[50] The GDPR, article 12-14.
[51] The GDPR, article 12-14; see also section 2.6.
[52] See 1.4.2 Method, footnote 28.
[53] The OECD Privacy Framework, 2013.
[54] FIPPs are still prevalent in the US legislation of privacy, see FTC report, (2012) Privacy in an Era of Rapid Change, Recommendations for businesses and policymakers: p. 3.
[55] The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, November 2017.

Although these historical and still current, guiding principles are not the focal point of this thesis, they form the foundation for the privacy discourse held today and can thus also be linked to the discussion on transparency as will be seen in the discussion of the suitability of privacy policies as EULAs below.

With this short background of the European privacy legislation within the directive and its evolvement to the GDPR, the specific enhancements requiring transparency and information will be discussed in depth starting with the relationship between transparency and trust.

2.2 Transparency and Trust

Building trust between the data subject and the controller is an inherent goal articulated by the GDPR. Already when a new reformed privacy legislation was proposed by the European Commission in early 2012, an emphasis on building trust was apparent in the press release from EU Justice Commissioner, Viviane Reding:

"The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses."[56]

The citation further shows the prominence of the question of trust as well as the shifted focus towards the individual and the need for the data subjects to "*be better informed"*. [57]

Trust is inherently connected to the transparency requirement in the GDPR through the idea of transparency generating trust. The idea has been described by the European Parliament:

"…considers that it is crucial that transparency and the proper provision of information to the audiences concerned are key to building public trust and to the protection of individual rights".[58]

This summarizes that there is a need for understanding transparency, in the way it is being prompted in the GDPR, as well as in revolving discussions regarding privacy legislation and data collection, through the idea of generating trust. The generation of trust through transparency is motivated by the idea that creating a more open and transparent setting will

[56] European Commission - Press release, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Brussels, 25 January 2012.
[57] European Commission - Press release, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Brussels, 25 January 2012.
[58] European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)), (2018/C 263/10).

enable privacy for the individual by generating control to the data subject.[59] In order to comprehend how transparency is to function and yield trust, information needs to be incorporated into the perception of transparency. The information provided between controller and data subject is therefore creating transparency and privacy at the same time. The idea of transparency consequently centres on the data subject having a clear enough view of the personal information handled or used by the controller in order to create a transparent relationship to build trust.[60]

The perception that transparency creates trust is not questioned within the regulation or by the drafters, it is rather presented as a self-evident fact. This presentation of transparency generating trust will be challenged in section 4.5 where the aim will be to show that transparency can also hinder trust. Regardless of the possibility for transparency to create trust, in order to reach transparency there is a need to provide information. The aim to create better informed data subjects through the GDPR can thus be seen through the enhanced demand on informed consent.

2.3 Transparency and Consent

The view of individuals as autonomous legal subjects demand that the legislation allows for the data subject to surrender a right in favour of other benefits through consent. An illustration of this need can be seen in the health sector. How privacy regulation is handled within different health facilitators that are accumulating personal medical information, is mainly and historically dependent on the consent provided by individual patients for collection and storage of their health information. [61] As data processing have evolved and the possibilities with data increased, the unequal information balance between collector and data subject have been prominent in the relation between state and individual as well as within employments.[62] Thus challenging the collection based on consent between uneven parties. This imbalance is further evident with the growth of many of the companies today handling personal information as a part of their day-to-day work. This challenge is therefore also acknowledged in the new regulation in relation to providing valid consent.[63]

2.3.1 Informed Consent and Free Choice

The GDPR has responded to these evolvements, as well as the need for data subjects to be given self-control, by enhancing the demands of how to provide consent to a controller for processing

[59] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.5, (4), '*The concept of transparency in the GDPR is user-centric rather than legalistic*'.
[60] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.1 introduction (2).
[61] Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011): p. 33.
[62] Pasquale. *The Black Box Society*, p. 3, 42.
[63] Article 29 WP, Guidelines on consent under Regulation 2016/679, p. 5, 3.1.

information from a data subject, especially when the processing has no imminent necessity in order for the company to provide their services. This enhancement is presented through the demand of informed consent.[64] Since the consent needs to be informed there is a subsequent need for the company to be transparent, this is clear in relation to cases where the transparency requirement towards the data subject is directly linked to situations where consent is the legal basis provided for processing. E.g. the requirement of informing the data subject of the possibility to withdraw consent constitutes a need for the company to be transparent.[65]

However, there are also demands on what the phrasing 'informed' entails to be provided, by the controller when asking for consent, in order to conclude that the information is being transparent for the data subject. The demands on providing consent now includes that the consent needs to be based on a '*free choice*'.[66] Many of the online actors today demand consent from the data subject for collecting, processing and using personal data in order to grant the data subject access to the service. This requirement of consent creates an ultimatum in the form of a take-it or leave-it scenario created for users wanting to access the service but not at the cost of their personal information. Consent that is provided in a settings where the option of not providing consent prohibits the data subject from access can also be strongly questioned in regards to the demanded free choice and it being freely given, where it is arguable that consent cannot be given of free choice if there is not actual choice.[67]

2.3.2 Forced Consent

The issue of privacy policies demanding consent in order for the service to function left many users of social media applications without an actual choice as the GDPR entered into force. With the new regulation, the social media applications demanded a new, freely given consent to be provided by the users, if not given, the service was rendered useless. This was directly reported to Data Protection Authorities (DPA) in the EU member states France, Belgium, Germany and Austria with the claim of companies using 'forced consent' towards the data subjects.[68] Arguing from the GDPR regulation on consent along with the recitals exemplifying freely given consent,[69] and the Article 29 WP Guidelines on consent, the argumentation renders that this take-it or leave-it approach goes against the provisions of 'free consent' as set out in the GDPR.[70] These complaints can however be further problematized. If a service is existing on the idea of sharing personal information between users, the usefulness of the service would not be satisfactory to the data subjects if rendered unable to collect personal information based

[64] The GDPR, article 6; Article 29 WP, Guidelines on consent under Regulation 2016/679, p.13 (3.3.1).
[65] The GDPR, article 7.3.
[66] The GDPR, recital 42.
[67] Which has also been argued by NOYB – European Center for Digital Rights, update on filed privacy complaints.
[68] NOYB – European Center for Digital Rights, update on filed privacy complaints.
[69] The GDPR, recital 39, 42 and 43.
[70] See e.g. the complaint launched in France, NOYB – European Center for Digital Rights, privacy complaints.

on consent. Therefore, the argumentation of forced consent cannot be applied to all services since it is the feature of sharing information that is sought by the data subjects when entering the service. The prohibition of these types of services requiring consent can also be argued to be in direct violation to the aim of the regulation rendering informed data subjects and free data movement since it will hinder companies' evolvement due to stagnating data movement if consent cannot be provided.[71] It is therefore of necessity to see the transparency rendering relevant information as the objective within the regulation and not the prohibition of data collection, this since the second would directly hinder a prospering market.

The consent as formulated in the GDPR is therefore a legal basis for collecting and processing personal information that requires an increased level of information and transparency, also rendering the need for the data subject to make an informed and active choice whether to provide consent or not. This can therefore be argued to be where the demand for adequate transparency is most evidently needed.

2.4 Transparency and Comprehensibility

Since the collection of personal data can be done on other legal grounds than consent the discussion on transparency is not only limited to consent as a legal basis for collection but evident throughout the legislation and thus also when processing occurs on one of the other foundations. [72] As described by the Article 29 WP the demand on transparency is not narrowed to one feature but spans over all aspects of data collection regulated in the GDPR.[73] It is therefore necessary to address transparency generally as an aid for comprehensibility of the data subject regarding the information provided concerning the collection of their personal data.

By transparent information the data subject can be provided with insight regarding the basis for collection, e.g. for the fulfilment of a contract, as well as how this information is protected, anonymized, shared and so on. The data subject can then actively choose whether or not to use the service rendered, based on how the personal information provided is handled and possible effects of the collection for the data subject. Thereby creating the control, aimed for within the regulation, for the data subject.[74]

This way of shifting control to the data subject, by placing it as an informed choice to participate or not, also shift liability towards the data subjects. As long as they have had the possibility to become informed they have also actively chosen, regardless of what ground it is based on

[71] The GDPR, recital 3.
[72] The GDPR, article 6.
[73] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.1, introduction (1).
[74] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.5 (4).

legally and not only in the case of consent.[75] This could then be seen as rendering an enhanced burden for data subjects to be informed, however this can be argued to be balanced towards the companies' liability by the GDPR requiring the transparency and information to be given to the data subjects.

The transparency requirement will henceforth be discussed in regards to the purpose of reaching comprehensibility for the data subject both when based on explicit consent and when agreeing to a privacy policy EULA that justifies collection on one of the other legal foundations. How the enhancement of transparency is stipulated throughout the legislation and applicable regardless of legal ground for processing will be elaborated through the view of how transparency and information is connected.

2.5 Transparency through Information Formulation, Medium and Format

2.5.1 Article 12 Transparent Information

There is no clarification in the GDPR, of what is included in the meaning of transparency other than an amplification of what is aimed to be achieved with transparency. One of these amplifications can be found in recital 39 concluding that transparency aims at achieving *informed natural persons*.[76] This reflects back to necessity of information to create transparency as mentioned above.[77]

There are however clear demands on information and what information should be provided in the regulation. Article 12 adheres to the division of the GDPR addressing "*Rights of the data subject*" and the article constitute the first right, requiring the controller to provide the data subject with transparent information.[78] The article provides a broad scope of the information that is to be provided to the data subject. The components set out under article 12 will hereafter be addressed and discussed from their practical meaning in regards to enabling transparency.

2.5.2 Concise and Transparent

The first section demands that the information that is to be provided is done so in a "*concise, transparent, intelligible and easily accessible*" way.[79] Within this, several aspects can be observed on how the information is to be delivered to the data subject.[80] The requirement of *concise and transparent* information aims at avoiding the data subject to be overwhelmed with

[75] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 32.
[76] The GDPR, recital 39.
[77] In section 2.2.
[78] The GDPR, article 12(1).
[79] The GDPR, article 12(1).
[80] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (8).

the information provided, so called, information fatigue.[81] The request for transparency is limited to relevant information through the requirement of concise information in order to avoid the information being to exhaustive and thereby limiting the possibility of the data subject to fathom the information necessary to generate transparency. This requirement also entails the actual place for providing the information to the data subject, preferably distinctly separate from other contracts and in an easy to find model. This is further recommended to be presented in way so that the data subject can grasp the overall context of the information regarding processing.[82] Such as in an online setting where the technology can provide layers of information.[83]

2.5.3 Easily Accessible and Intelligible

That the information is provided in a concise manner is further connected to the demand of *easily accessible*, the data subject should not, in the first place, need to search in order to find the EULA containing the privacy policy no more than the data subject should need to actively search for specific information within it. The transparency requirements thereby include the demand of a simple way for the data subject to be informed.[84]

As for the need for the information to be *intelligible*, this constitutes a demand for the information to be presented so that it can be understandable by the data subject.[85] This can be a difficult balance as the information is also establishing a contract and thus consideration needs to be made in regards to possible formalities in different jurisdiction for the contract to have the legal ramifications wanted.[86] In order to balance the difficulty concerning what needs to be provided for the privacy policy as an EULA to function both as the legal contract it is, as well as an information provider, the GDPR has stipulated that the information need to render an awareness of the collection for the data subjects. Thus, there should be no direct hindrance by the regulation to include the legal settings wanted to avoid legal implications within the EULA as long as the possible impact for the individual is also made clear in relation to the data subject.[87]

2.5.4 Clear and Plain Language

However, the possible implications for the data subject from the collection cannot be presented in an overly legal or obstructing language, as the second feature of article 12 calls for '*clear*

[81] See more in section 4.1, formulations such as information overload are also apparent in the discourse.
[82] The GDPR, article 12 (7).
[83] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (8); see also chapter three, 3.4.4.
[84] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.8, (11).
[85] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (9).
[86] E.g. what needs to be fulfilled for a contract to be legally binding.
[87] The GDPR, article 5.1, recital 39, Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (10).

and plain language'. This aspect is fairly elaborated within the EU through other legislations, guidelines as well as 'best practice' regarding how to provide written information in the sought way.[88] In the relation of EULAs and data subjects understanding of the content and obligations within, the writing should be done in clear language avoiding vague formulations. For instance, formulations upon which the interpretation can be dependent on numerous factors are discouraged.[89]

2.5.5 Method of Providing Information

The final aspect of article 12 in relation to the transparency of privacy policies as EULAs is through what medium the information is provided to the data subjects. There is a presumption of it being provided in writing, which is also the most frequent way privacy policies are presented, although often in an online settings. The provision of written presentation, is in no way established to legally limit the means of the presentation method selected for providing information. The article should rather be considered as opening up for other techniques to be chosen as a method of complementing the presentation to the data subject if they are deemed more suitable in order to reach transparency.[90]

It is therefore up to the arena of the collector, on which the data subject accesses the service, and thereby where they are presented with the information and expected to comprehend the privacy policy as an EULA, that will determine the limitations of form. As long as the chosen form is selected in the interest of reaching better transparency and not factually functioning as a hindrance to the data subject's transparency.[91]

2.6 Transparency through Information Content and Time of Delivery

2.6.1 Article 13 and 14 Information to be Provided

After having laid out the general structure for how the communication to data subjects should be presented, the GDPR becomes more specific in the requirement on transparency through what information is to be provided. In articles 13 and 14, the demand on information content and time for providing the information set out points that are forming the minimum content needed to be available to the data subject in order to ensure transparency.[92] The direct requirement for the collector to provide the data subject with specific information is a novel addition in the GDPR in relation to the previous directive.[93] The added specification thus aims

[88] European Commission, How to Write Clearly by the (2011); Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Article 5; GDPR, recital 42 in relation to consent.
[89] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.8-9, (12).
[90] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.11-12, (17-19).
[91] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.11-12, (17-19), p. 14, (24).
[92] The GDPR, article 13, 14.
[93] Ledendal, Larsson, Wernberg. *Offentlighet i det digitala samhället*, p. 293.

to enhance the transparency by creating a lower limit on what constitutes a necessity for the data subject to be informed about. In addition to this lower limit of content, the GDPR also provides a time frame for when the information should be given, creating an assurance that the information is actually given to the data subject.[94]

The two articles adhere to two separate reasons for a collector to have collected the data subjects personal information in the first place. Article 13 responds to when a collector has gathered information directly from the data subject and article 14 regards the occurrence of when a collector as a third party, receives information through another collector about said data subject. Article 13 therefore concludes what information a data subject is entitled to, by a controller who have collected information directly from the data subject whereas article 14 responds to the information to be provided in the situation where the collection has occurred from a different party and not directly from the data subject.[95]

2.6.2 Collection Directly from the Data Subject

When a data subject, through using a service, agrees to a privacy policy EULA and thus submits their allowance for collection of their personal data, regardless of on what ground, this is first and foremost a situation of direct collection as regulated in article 13. It is also this occurrence that forms the basis of the research question, *Can privacy policies, in the form of end user license agreements, generate adequate transparency to meet the demands of the GDPR?*. This since it is through the privacy policies as EULAs that the data subjects agree to the collection and this agreement is presented at the time of entering a service. This further falls in line with the overall idea of when the data subject should be notified through the information and thus reach a level of transparency before agreeing to the policies, at the time of the wanted collection.[96]

The information categories that needs to be provided are explicitly mentioned as six categories of information: identity, contact details, purpose, legitimate interests when based on consent, recipients and intended transfer of data.[97] Furthermore, information regarding the rights of the subject, found in the GDPR chapter three, to '*ensure fair and transparent processing*' is also mandatory information.[98] Thus, transparency is covered in all areas of the privacy policy as an EULA, its form, content, when it is to be disclosed as well as how it legally can aid the data subject in further scenarios.

[94] The GDPR, article 13 (1), article 14 (3) a-c.
[95] The GDPR, article 13 (1), article 14 (3) a-c.
[96] The GDPR, article 13(1) '*at the time when personal data are obtained*'.
[97] The GDPR, article 13.
[98] The GDPR, article 13(2)b.

2.7 Transparency through Access and Portability

As mentioned in regards to information content, the rights of the data subject needs to be included in the information provided to the data subject, a demand that should be considered in relation to the idea of rendering the data subject with control through the GDPR. These rights are, when being presented to the data subjects, a part of information transparency and can in some cases also be seen to render transparency by their functions. The rights most closely connected to providing transparency is the right to access and data portability.[99]

The right of access for the data subjects, places a demand on a company to, upon request, investigate and respond to the data subjects request on whether the company has any information collected relating to the data subject. If this request is responded affirmatively the GDPR further require that the collector need to convey the content of that information to the data subject.[100] This possibility rendered to the data subject further allows for the right of data portability, which empowers the data subject by enabling them to demand companies that have collected information from the said data subject, based on consent or contract, to provide this information to the data subject.[101]

The data subjects control of the information is further ensured by demanding the information to be delivered '*in a structured, commonly used and machine-readable format'*.[102] This requirement aims to function as a measure to hinder the controller to provide obscure information, meaningless for the data subject and thereby eliminating the comprehensibility needed for transparency.[103]

The aforementioned requirement enables the data subjects to own its information by placing a need for the company to be transparent and collaborative in regards to the subject's information. Thus in the longer perspective allowing for the data subject to be able to take part in the data economy without losing their personal information once shared.[104] The data portability right has also been argued to constitute a form of transparency rendering control for the data subjects in allowing them to ensure that the information is correct.[105]

[99] The GDPR, article 20, article 15.
[100] The GDPR, article 15.
[101] The GDPR, article 20.
[102] The GDPR, article 20 (1).
[103] Article 29 WP, Guidelines on the right to data portability, p.18, - *How to deal with a large or complex personal data collection?*.
[104] Article 29 WP, Guidelines on the right to data portability, p.4.
[105] Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: p. 15 (26).

These two rights of the data subject constitute factual actions to ensure that transparency can be demanded directly by the data subject. This will therefore be argued to be a transparency possibility directly empowering the data subject and not dependent on the information provided by the collector in the privacy policies.

2.8 Discussion

This overview of the transparency requirements within the GDPR have aimed to show that the demands on companies to inform and remain transparent are needed at all times when there is a collection of data from a data subject, directly and indirectly. Transparency has been shown to come both in the form of liability on the company conducting the collecting and processing, as well as a right of the subject to ensure that they are provided with information. Therefore, the aim with the regulation can be considered to create the adequate transparency in order for data subjects to gain insight into the effects of the collection. Thereby avoiding that the information provided is too diffuse to generate adequate transparency and comprehension for the data subjects. When solemnly viewing the transparency requirements within the GDPR the idea of adequate transparency can thus be argued to counteract the actively uninformed data subjects that have been prevalent in the privacy discourse.

There is a clear emphasis, within the transparency requirements, on mechanisms believed to enable the data subject to be made aware of the collection of personal data, such as the demand on the company to provide the legal basis for collecting to the data subject. In this regard, transparency is not a legal aim on its own but a demand in order to reach the legal aspects of informing the data subject.[106] This is thus the framework creating the legal basis upon which transparency is to be ensured for the data subjects. After having analysed the regulation from the perspective of providing transparency through information the practical application can be argued to be fairly straight forward. However, the result of how transparency is actually provided will be discussed in connection to the companies' privacy policies. How this transparency takes its practical form will be presented in the following chapter by considering specific criteria placed on privacy policies to measure if they can reach adequate transparency as prescribed through the demands put forth by the GDPR.

[106] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.5, (4).

3. A Taxonomy of the Functional Criteria Present in Privacy Policies

3.1 Introduction

This section will be devoted towards scrutinizing the documents that are actually transmitting the demanded transparency to the data subject, namely company's privacy policies in the form of End User License Agreement. As initially concluded the privacy policies are in this thesis considered being the main concern to reach the required transparency seen in the GDPR and therefore they are also the main object when evaluating the possibility to generate adequate transparency. How the privacy policies function and are structured, from their appearance to the data subjects, to their compatibility with the functional criteria chosen will provide the basis for this discussion regarding how the legal legislation is translated in reality and thus presented to the data subject.

The focus is therefore to elaborate and evaluate the practical functionality of privacy policies in the form of EULAs in providing adequate transparency. It should be noted that the privacy policies chosen are all from companies who are active, in terms of subjected to the territorial scope of the GDPR[107], if not based within the EU. Additionally, all of the privacy policies have all been amended in close relation to the enforcement of the GDPR, indicating that they were adjusted with new information as exemplified in the background of the GDPR.[108] First a clarification of the structure and function of the documents, EULA, forming the basis for this taxonomy will be provided.

3.2 Privacy Policies as Legal Documents

With many of the daily activities taking place in an online setting through social media, web-shops as well as through information seeking services, the most frequent contact with privacy policies is therefore also through these online channels. When individuals are participating in the online community they are continuously asked to agree to the activity conducted. This agreement, or consent to participate is usually submitted when checking a box for agreement and use of the service. The box is complemented with a statement obliging the user not only to participate but also to have read and understood said company's privacy policy as well as other terms of service. These boxes, asking for active participation, have become such a frequent interference in the daily life of data subjects that studies have been done on how much time it would take to read all of the attached agreements.

[107] The GDPR, article 3.
[108] Microsoft amended their document again in October 2018.

The average privacy policy and terms of service, attached to the agreement box, resulted in a 37 hour long session if read word by word.[109]

3.2.1 The Creepy Line

These privacy policies are however not merely policies, they create an agreement between the user of the company's provided services and the company itself. The legal functionality, in the company's perspective, is therefore not mainly to provide fair information to the data subject, but to fulfil the legal requirements in relation to data collection and remain liability free. The need to comply with the demands on transparency might not always be in the company's inherent interest.[110] The foundation of data provided through the data subjects participation is today highly valued and thus desired by companies. If data subjects became more hesitant to share their information it would render a direct effect in terms of costs for companies. This especially with data having evolved into a currency,[111] and something that is possible to build businesses on. Therefore the main interest is more likely to be granted as much data as possible from the data subject and remain liability free by having collected this information on legal terms. This interest was mentioned by the previous CEO of Google, Eric Schmidt, who, in 2010, phrased it as '*There is what I call the creepy line. The Google policy on a lot of things is to get right up to the creepy line and not cross it.'*[112]

This creepy line can be connected to the phenomena of '*function creep'*.[113] It is through the quotation portrayed as evident that there is a line of what collection can be conducted and when the collection is beyond that line, creepy. Function creep does however, show us that the creepy line is apt to be pushed further by expansion and argumentation of what falls within the line. Rendering that the interest of collection as much information as possible in relation to the creepy line, is not a safe guard for the data subjects. Rather the creepy line can be argued to be constructed of what CEOs of companies like Google can motivate to fall within the line.[114]

---

[109] Norwegian study with an estimated average of 33 apps, Forbrukerrådet, 250,000 words of app terms and conditions, May 2016; McDonald and Cranor. 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* vol. 4, no. 3 (2008): p.565. The time spend for American Internet user estimated to be 201 hours annually with the cost calculated to 3,534 dollars per person and year.

[110] Zuiderveen Borgesius. 'Behavioural Science and the Regulation of Privacy on the Internet' in *Nudging and the Law - What can EU Law learn from Behavioural Sciences?, ed.* Alemanno and Sibony (Hart Publishing, 2015): p. 30. On diverging interest of policy makers and companies.

[111] Larsson, Ledendal. (2017) Personuppgifter som betalningsmedel, p. 16-23.

[112] Saint, *Business Insider*, Eric Schmidt: Googles policy is to 'get right up to the creepy line and not cross it' October 2010.

[113] Dictionary, 'function creep', '*Gradual widening of the use of a technology or system beyond the purpose for which it was originally intended'*.

[114] See also section 5.5 below.

It should be noted that Googles view on privacy has been forced, in some way by legal actions, to adapt since then.[115] This legal aspect of privacy policies will be further seen through the chosen functional criteria below.

3.3 Functional Criteria Enabling Adequate Transparency

The functional criteria selected for this taxonomy have been chosen, in part, from the demands required by the GDPR, as evolved in the previous chapter regarding article 12.[116] Furthermore, the Norwegian Consumer Council,[117] have through their work with consumer protection and consumer legislation viewed privacy policies from the perspective of consumers and accessibility. This work has generated into recommendations for creating comprehensible privacy policies from a consumer perspective. The recommendations have also been considered when formulating these criteria for functionality in this taxonomy.[118]

Each of these criteria constitute one end of a line with an opposing function, i.e. short is the opposite of lengthy. In order to exemplify this balance, the criteria chosen are explained in relation to the opposite characteristic that can be concluded to hinder transparency in terms of practical function instead of enabling adequate transparency. There are however, at least not in this thesis, a clear formula stipulating the perfect balance of these criteria for providing adequate transparency. A privacy policy can therefore be lengthy in regards to another shorter privacy policy but still provide a higher degree of adequate transparency for the data subject due to the language used. Hence each privacy policy needs to be measured in relation to their inherent criteria in order to make a fair adjustment. This taxonomy therefore aims to construct a guide for evaluating a specific privacy policy.

This assessment and the table taxonomy creates a snapshot of the chosen EULAs, simply answering if they fulfil the criteria or not. They have not been individually assessed to determine if they reach adequate transparency or not, but will be discussed from an overreaching perspective exemplifying different aspects of the criteria. General conclusions as a universal truth should therefore be avoided based on the following presentation. The structure and criteria used are rather to be observed and perceived as a tool in the event of evaluating privacy policies as EULAs.

[115] Letter to Google from CNIL on behalf of the EU data protection authorities.
[116] See section 2.5, Transparency through information formulation, medium and format.
[117] Forbrukerrådet, 250,000 words of app terms and conditions, May 2016.
[118] Forbrukerrådet, 250,000 words of app terms and conditions, May 2016.

The aim with this section is also to identify the challenges with this balance of transparency in order to create a foundation upon which the discussion on suitability and possibility of EULAs to provide adequate transparency to data subjects can be based. Consequently, the purpose is to present an objective view of the criteria in relation to the demand from the GDPR discussed above.

3.4 Taxonomy Criteria

The following criteria have been chosen for their ability to aid adequate transparency. They are first and foremost discussed as transparency enablers in the perspective of the GDPR requirements, the article 29 WP guidelines and by scholars in the privacy discussion. The criteria will be presented and motivated from their functionality and further problematized from the criteria opposite, that instead hinders adequate transparency. Thereafter an overview of the selected privacy policies will be presented in relation to how they respond to the criteria set out. Note that no balancing will be done in the taxonomy, they either adhere to the requirement or not.

3.4.1 Short and Concise

Meeting the criteria of short and concise can be a challenge as privacy policy are demanded to incorporate specific information in order to increase transparency.[119] This is therefore argued to be where the balance of providing information to reach transparency is most evidently an issue. Measuring this requirement as a functional feature is this not necessarily about length in terms of pages, or screens, but rather resonates to whether the privacy policy keeps to the point, avoids unnecessary wording and avoids repetition. Due to the difficulty in measuring this without studying the impact of the reader's comprehensibility of each privacy policy, this feature will not be measured as a criteria but simply shown in printed pages, thereby rendering the possibility to further discuss if the fulfilment of the below explained criteria have an effect on the factual length. The pages included in the table refers to the number of pages first visible to the reader and within parentheses to the number of pages when a 'expand all' feature is present and used.

All of the following criteria can therefore in some sense be argued to adhere to generating a short and concise privacy policy and thereby enabling adequate transparency for the data subjects.

[119] See section 2.6.1 above.

3.4.2 Common Language

The requirement to provide privacy policies that are written in a common language connects to the rights of the data subject specified in the GDPR, specifically the demand of clear and plain language.[120] In relation to transparency, common language connects to a demand on understandable language for the data subject, who is the considered user of the service.[121] Therefore the demand of common language is not merely an objective demand obliging the use of a specific vocabulary. Although the demand does entail that the privacy policy is to use language that are customary used by the society, it also involves the adaptability of the text to the thought group of data subjects as consumers. A social media forum will therefore require a privacy policy to be written in a language that adapts to the wide span of vocabulary existing between teenagers and professors. With many social fora today aiming to adhere to a large and widespread audience it is in the interest of the privacy policy to be as simplistically written as possible in order to provide the needed information to a wide target group.[122]

3.4.3 Legalistic and Technical Language

Since what constitutes common language can be difficult to measure given the, often, extensive span of data subjects with access to a certain service, it can be viewed by the opposing criteria, legalistic and technical language. This can however vary on the same basis as common language, hence specific phrases have been selected.

The following legal terms selected are based on legal terms from the GDPR, *personal information, sensitive data (*including *sensitive personal information* and similar phrasings*), natural person* and *third party (affiliate* included*).* The following technical terms have been chosen due to their relevance in regards to how the data is used, *algorithm*, *cookies* (including the phrasing *similar technologies,*) *unique identifiers, device token, pixel tag, plug-ins, data encryption* and *application data cache*. The occurrence of technical and legal terms, without explanation either in the form of layers or directly, will function as an indication that a privacy policy is not written in a common language. The possibility to cover all legal and technical terms present in privacy policies is in this thesis limited and the aim is merely to give an indication of how well the policy responds to the common language requirement since no guidance has been given in the regulation or the guidelines on how this should be evaluated.

[120] The GDPR, article 12 (1).
[121] See section 2.5, Transparency through information formulation, medium and format.
[122] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 7 (9), p.9-10, (13).

3.4.4 Headings

The practical function of using headings and section in the privacy policies can, in relation to transparency, constitute a visual aid. It does however also have a comprehensibility advantage, allowing for the data subject to get a quicker overview of the content presented and thereby also be able to easier grasp the different parts of a privacy policy.[123] In regards to the issue of privacy policies being long and hard to comprehend the headings thus serve as a counterbalance towards this issue. Allowing for said data subject to choose what deems necessary to read is therefore argued to provide a higher degree of adequate transparency.

At the other end of headings and structure is a formless text, creating less possibilities for the data subject to achieve an overview of the content and thereby demanding the data subject to find the information sought by going through the entirety of the privacy policy. This creates inaccessibility rendering many data subjects to refrain from reading at all. Therefore, a privacy policy structured with headings will not require the data subject to choose between reading it all or none of it since it can easily get an overview by seeing all sections through headings.

3.4.5 Layers

The use of headings is closely connected to the use of layers in the online context. By dividing the text into sections or headings to guide the data subject they will also be enabled to easily move between the different sections through layers connecting the data subject from an overview to wanted specific heading.[124]

Allowing for layers also allows for the aspect of providing a shorter, summarized overview of the policy with the layer function leading the data subject to a longer version, more technically or legally explained version or to a glossary where such is deemed necessary. The possibilities with layers in an online setting are many, and should be used.[125] A good example of this is Google's privacy policy, which have adapted layers in order to provide explanations to certain words as will be seen in the next section.[126] The Article 29 WP has also lifted the combination of other electronic functions when using a layered approach, in order to better ensure that the information reaches the reader, such as pop-up notices (also known as just-in-time notice).[127]

[123] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p 7. (8).
[124] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 19 (35); EU Publications, Handbook on European data protection law, 2018 edition, p. 215.
[125] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 19 (35); This can also be done as Microsoft and eBay have chosen with a shorter and an expanded version.
[126] Google LLC Privacy Policy.
[127] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 12. (18).

Another way of using layers to enable adequate transparency for users is through the layers used in Twitters privacy policy, directing the reader to where they can amend the settings for the service in relation to different aspects of information.[128]

As with the demand for headings, the opposite of a layered structure is the lack of it, in a formless text. In the example of Twitter's layers guiding the data subject to the specific place where they can control their personal information, the lack of guidance in relation to impact connected to these amendments can also be argued to hinder transparency. This structure will require that the data subject to first find the needed information about a specific part of the collection and then after finding out that they can steer this use, need to search for where this is placed in order to amend it. Therefore the guidance that Twitter's layers deliver should be provided with the explanations found in Google's layers and vice versa for optimal usage for data subjects.

3.4.6 Explanation

With the legalistic background and aim of EULAs as liability disclaimers, they tend to be written by people within a legal profession, as compliance officers, corporate lawyers or lawyers hired solemnly for the completion of privacy compliance within a company. Regardless, the privacy policies encountered by data subjects compile of many both legal and technical terms, as the use of data has grown all the more technically advanced and the possible ways of usage have increased. The understanding of the data subject can therefore be hindered merely on specific words used to describe the usage of the data as shown by the criterion, common language. As seen in Google's privacy policy, an explanatory help for these types of formulations can be adopted.[129] They comprise of another layered version allowing for the reader to press on words and formulations of legal or technical matter and view an elaborated explanation of the meaning. These tools create an aid for the data subjects not familiar with the specific language and at the same time limit the policy in regards to length and inaccessibility to those who are already familiar with the terminology. However, the need for the data subject to be immediately informed about the possible impact of the collected need to be considered when using these explanatory layers, so that clear language is not substituted with explanations.[130]

[128] Twitter Inc. Privacy Policy.
[129] Google LLC Privacy Policy.
[130] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 19 (36).

If explanatory tools connected with layers, are used, a balance can be created that would allow for the needed formulations responding to the agreements liability function to be provided. This without creating a disadvantage towards the data subjects not familiar with the technical or legal formulations used. This balance of providing information then functions as an equalizer in regards to information, thus creating a more adequate transparency between parties.

3.4.6 Clear Formulations

Staying on topic when providing the information needed, in order to ensure that the data subjects can comprehend the information, is strongly connected with the initially mentioned criterion of providing a short and concise privacy policy agreements. Adapting and using clear formulations should therefore be the intention in all communication between controller and data subject in order to provide transparency. Ambiguous formulations often lead to lengthy and complex text since the main issue or goal of the text tends to be circled around and left unanswered within other formulations.

Providing clear formulations in texts is especially challenging when it is connected to legal and technical matters. The risk of oversimplifying and thus rendering the information dishonest or non-informative is prominent, rendering in that the goal of providing transparency through clear formulations is not met. In order to avoid this there have been previous studies done on what phrasings and words are considered as vague or ambiguous in the context of privacy policies.[131] In this thesis the scope will however remain narrowed towards the guidance in the relevant regulation, the GDPR.[132]

3.4.7 Ambiguous Words

In order to measure this criterion in regards to its functionality, each privacy policy has been searched for the words specifically noted, by the Article 29 WP, to be avoided in order to provide a clear policy. These worlds constitute '*may'*, '*might'*, '*some'*, '*often'*, and '*possible'*.[133] The occurrence of these words in the privacy policies without a clearly needed context is thus creating ambiguous meaning which renders that the policies do not comply with the clear formulation functionality.[134] The aggregated number of occurrences of these words in each privacy policy respectively will be presented to view the amount of occurrences where clear formulations are hindered.

[131] See e.g. Reidenberg, Bhatia, Breaux, and Norton. 'Ambiguity in Privacy Policies and the Impact of Regulation.' *Journal of Legal Studies, Forthcoming, Fordham Law Legal Studies Research Paper* No. 2715164 (2016): p. 6.
[132] The GDPR, recital 42; Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 8-9 (12).
[133] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p 9. (13).
[134] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p 8f. (12).

This is hence the only criterion indicating a scale, besides the amount of pages. However, like the others, the criterion of clear formulations have also been marked as does or does not in the taxonomy below.

3.5 Analysing the Privacy Policies

The above criteria have been viewed from the perspective of the set of privacy policies selected in order to construct an overview of how the criteria are occurring in practice. Thereby being able to estimate the possibility of privacy policies functioning as a tool enabling adequate transparency to the data subjects. As have been mentioned in relation to each criteria some of them are less suitable for objective measurements and have therefore been amended in order to function as a comparative, factual criteria.

As mentioned in the introduction the selected companies are: Apple, eBay, Google, Microsoft, Netflix, Spotify, TripAdvisor and Twitter.[135] Like many companies today, these have a business model requiring the company to collect and process data in order to function. Some of them require it for providing the service, i.e. companies delivering products require the contact information of the ordering part in order to ship the produce. Others collect it in order to further evolve the service, such as in order to give specific recommendations of similar movies based on the content provided by selecting a movie. In one way or another these companies service collects and uses data, rendering in the user having to agree to a privacy policy stipulating how this data is collected and used.

Companies mainly focusing on data collection for targeted advertisement, i.e. companies who have privacy policies for what is collected when a data subject simply visits their website, is left outside the scope since it often requires a more deliberate action by the data subject to even access the EULA containing the privacy policy. The privacy policies chosen are therefore policies that data subjects agree to by accessing and creating an account within the service in the first place. The privacy policies have been collected from the respective company's website on the 5th of November 2018.

3.5.1 Actively Informing

The possibility for the data subjects to remain informed if all of the above criteria are met and thereby generates adequate transparency, requires the data subject to become informed of any changes.

[135] See section 1.5 for selection of companies; see the bibliography, privacy policies, for the companies privacy policies in full text.

Refraining from informing the data subject about changes or simply encourage the data subject to check for updates on a continuous basis is not enough to adhere to the demand of fairness within transparency.[136] Therefore an additional criterion will be seen in the table below, stating if the company guarantees to actively inform the data subject when amendments have been enforced in the privacy policy.[137]

3.5.2 Online Setting

In order to fairly evaluate the privacy policies in relation to the criteria, they have been observed in the online setting, allowing for features such as layers and headings to function properly. The number of pages, as mentioned under short and concise, has been counted in the 'print' mode, generating how many printed pages the privacy policy would require, the privacy policies with numbers in parentheses signify the expanded version of the privacy policy. The clear formulations criterion is complemented with a number stating the total use of words signalling unclear formulations as mentioned in 3.4.7, if the policy have an expand function presenting a longer view, the longer version have been selected. The following table presents an overview of the findings in the selected privacy policies.

3.6 Taxonomy Table

Criteria ---------- Company	Short and concise	Common language	Headings	Layers	Explanations	Clear formulations	Actively inform in event of change
Apple	8 pages	No	Yes	Yes	No	No (70)	Yes
eBay	3 (13) pages	No	Yes	Yes	No	No (53)	Yes
Google	27 pages	Yes through explanations	Yes	Yes	Yes	No (75)	Yes
Microsoft	3 (24) pages	No	Yes	Yes	Yes	No (190)	Yes
Netflix	9 pages	No	Yes	No	No	No (35)	Yes
Spotify	9 pages	No	Yes	Yes	No	No (35)	Yes
TripAdvisor	5 pages	No	Yes	No	No	No (60)	Yes
Twitter	12 pages	No	Yes	Yes	Yes	No (44)	Yes

[136] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.17 (29).
[137] See also 2.1, Introduction.

3.7 Discussion

Having viewed the privacy policies from the factual criteria one can draw the conclusion that they are in some degree in line with the ideas behind the enabling criteria, such as headings. The execution, however, is not coherent between the different companies providing the privacy policies, rendering different strengths and weaknesses apparent in the different policies. It can also be interpreted that the importance of certain features is unevenly viewed between the companies, or perhaps the guidance drawn from the GDPR and the Article 29 WP have been interpreted differently if consulted at all, resulting in inconsistencies. Regardless, they are lacking coherency and the emphasis between criteria is diverging.

Although there are companies who, in sections of their privacy policy, responds to the above stipulated criteria satisfactory, there is no company who is completely fulfilling in regards to comprehensibility of how the data is actually used as seen through the requirement of clear formulations. This requirement is by far the most elaborated and straight forward in regards to guidance from the GDPR and the Article 29 WP with specific words shown as rendering ambiguity in the formulations and thus hindering comprehensibility of the data subject. Despite this, within the 107 pages viewed the words collectively appear in 562 instances. It can also be noted that TripAdvisor with the shortest privacy policy in number of pages still manages to use unclear words 12 times per page. There can within this, limited study, not be concluded that a shorter privacy policy will render clearer formulations.

Regarding the length of the privacy policies, functioning as a respondent to the criteria of short and concise, the privacy policy with the, by far, lengthiest privacy policy, Google with 27 pages, is also the only one responding positively to five of the six other criteria. Showing the above stipulated fact, in section 3.3, that a lengthy privacy policy can still exceed a shorter one in regards to comprehensibility.

This analysis does, despite the objective features of the requirements, contain subjective elements and should therefore be remembered to not try to make claims on the comprehensibility of all data subjects coming into contact with these privacy policies. The aim with this is therefore simply to conclude that the guidance on how to provide adequate transparency rendering comprehensibility for the data subjects does not assert that there is a uniform interpretation of these recommendations nor that comprehensibility is guaranteed. They simply render a lower threshold for companies to reside upon when choosing information and presentation.

4. Challenges of Informing Data Subjects through EULAs

The criteria lifted in the taxonomy have clarified the ideal features of privacy policies, provided in the form of EULAs, in order to reach adequate transparency. However as have been touched upon, there are challenges within the criteria as they are used in the structure of EULAs. Although the criteria constitutes aims within the legislation, the challenges to follow are not solemnly based on the requirements in the legislation but rather the effects that can be created when the criteria appear in privacy policies as EULAs. The first three challenges are related to the factual effect of the design of the information content to be rendering informed data subjects, the end user license agreement form of privacy policies. Thereafter certain challenges in relation to the data subject as the receiver of the information, will be regarded.

4.1 Information Fatigue

There is an unanimous view in debates regarding EULAs on them being too lengthy. As can be seen in the taxonomy table, the agreements are not contained to one or two printable pages. The length of the agreements vary between the selected privacy policies for the taxonomy with a difference of up to five times the length of the shortest compared to the lengthiest privacy policy analysed.[138] The discourse around the issue of length is, as mentioned in relation to the demands of transparency within the GDPR, related to the possibility for the data subject to grasp the content.[139] However, it is not solemnly a specific EULAs length that is problematic in relation to information fatigue. It is the accumulation of numerous privacy policies collectively, these EULAs are also multiplied in seemingly endless variations due to the massive impact of companies providing different services in each data subject's day to day life. As mentioned, studies have been done concerning the actual time reading EULAs consume along with the cost this creates for the data subjects in order to exemplify just how time consuming it would be to read each specific EULA.[140] This creates the condition phrased by several scholars as information-overload or information fatigue. [141]

The requirement of transparency can thus simply not be interpreted as a need for more detail and longer agreements since the possibility for the data subject to comprehend and acquire the needed information declines and hinders transparency as the length adds on. The structure of the privacy policies as EULAs can therefore be perceived to enable lengthy and elaborated agreements. This issue of requiring information to be provided to the subjects and at the same

[138] See 3.6 taxonomy table. TripAdvisor of 5 pages in relation to Google's 27 pages.
[139] See 2.5.2, information-fatigue/overload.
[140] Forbrukerrådet, 250,000 words of app terms and conditions, May 2016; McDonald and Cranor. 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* vol. 4, no. 3 (2008).
[141] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014); see footnote 109.

time remaining transparent has been discussed and explained as the transparency paradox.[142] The element of simply adding more information to the current structure is therefore not desired without amending the structure of privacy policies which the information is presented in. Different presentation variations of privacy information could increase the amount and appropriateness of the information incorporated and at the same time produce a more transparent view for the data subject. The possibility of amendments to steer clear of information fatigue and how these could be done will be further discussed in chapter six.

4.2 Comprehensibility and Intelligibility

Adjoining to the challenges with lengthy privacy policies as EULAs and information fatigue is the content of the information being incomprehensible. In this regard the comprehensibility of the data subject is dependent on numerous factors, e.g. the usage of specific unclear words as shown in the taxonomy. This hinders the possibility for the data subject to efficiently evaluate the information they are provided with. Unclear or ambiguous formulations can therefore undo information being provided in the first place. In this regard the privacy policies being formulated as legal documents disclaiming liability as agreements, EULAs, function in an aesthetical way as hindering comprehensibility. On a general basis most individuals are not used to being faced with reading and comprehending legal documents such as contracts and agreements on a day-to-day basis. The data subjects thus lack the comfortability in reading documents like EULAs. This creates a challenge in regards to using these documents for the function of specifically delivering adequate transparency to data subjects.

4.2.1 Transparency Through Right of Access and Portability

As exemplified when viewing the different transparency enablers prominent in the GDPR, the right of access and data portability have the possibility of not only empowering the data subjects with the factual control of their data but also to increase transparency of content.[143] This is however dependent on the form of the data that is provided.[144]

In order to reach an adequate transparency for the data subject it would therefore be reasonable to argue that the way that the data is provided for portability also fulfils the general demand on how information is to be provided to the data subject, i.e. '*concise, transparent, intelligible and easily accessible'* and in *' clear and plain language'*.[145] The demand in the GDPR, article 20, is clearly directed at the usage of data portability to enable the data subject to reclaim and

[142] Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011); Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 30.
[143] The GDPR, article 15, 20; Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: p. 15, (26).
[144] See 2.7, transparency through access and portability.
[145] The GDPR, article 12; see also chapter 2.

redistribute the information between companies. Although this is an important part of rendering control to the data subject, the usefulness of data portability has no effect if the comprehensibility of what the information the data carries or can be used for, is limited or obsolete to the data subjects, as discussed in relation to the transparency requirement in the GDPR.[146] Therefore, the technical use of data needs to be describe to the data subject in a way rendering comprehensibility, challenging the information provider to explain technical functions in clear way and at the same time render enough information for the data subject to comprehend the possibilities and consequences with the technical use of their personal information provided.

4.3 Impact Analysis

As a consequence of the challenges with information fatigue and lack of comprehensibility an additional challenge with privacy policies as EULAs becomes evident, the difficulty for the data subject to make an accurate impact analysis based on the information given. Although not a challenge independent to EULAs as such, the inability to read all information and comprehend it makes it impossible to thereafter make an adequate analysis of how the collection of data could affect the individual. Therefore, any decision made regarding allowing collection or not, based on lengthy and diffuse EULAs are made without the data subject having been able to conduct a proper impact analysis. The data subject has then little to no insight into how the impact of agreeing to the collection can inflict consequences not immediately made visible.[147]

This need for the data subject to be able to conduct an impact analysis has been addressed in the guidelines connected to the transparency requirement as well as directly in the GDPR emphasizing that the data subject "*should be made aware of risks…in relation to the processing of personal data"*.[148] This further adheres to the idea of empowering the data subject to even out the imbalance between the provider of information and the receiver, thus aiming to uphold the principle of fairness.[149] The requirement that the information provided should be clear enough to found the basis for an impact analysis is therefore a requirement within the GDPR and directly necessary in order to provide adequate transparency for data subjects.[150]

4.4 Ignorant Data Subjects and the Privacy Paradox

The theory of a 'blind, non-informed consent' being created by privacy legislation is concluded by Bechmann based on her own as well as a number of other studies showing the low percentage

[146] Article 29 WP, Guidelines on the right to data portability, p.18, - *How to deal with a large or complex personal data collection?*.
[147] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (10), p. 22, (41). In regards to the possibilities of profiling.
[148] The GDPR, recital 39; Article 29 WP, Guidelines on transparency under Regulation 2016/679, p. 7, (10).
[149] The GDPR, article 13 (2); Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.17, (29).
[150] The GDPR, article 5.1; Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.7, (10).

of data subjects that actually read the privacy policies addressed to them. The fact that these data subjects, despite not reading the privacy policies, still accepts the terms when entering into the service or application thus creates the blind and non-informed data subjects.[151] The uninformed users are shown not only in relation privacy policies as argued in this thesis, but are a general consequence of the form of EULAs, further supported by the statistic on how many users that agree to software license agreements actually reads them, not even reaching a percentage.[152]

4.4.1 Privacy Paradox

In contrast to the perception of data subjects being uninformed and unwilling to be informed, there are studies done within the EU, indicating that there is an apparent and, in some regards, increasing concern amongst data subjects in relation to data privacy. The concern generally relates to the protection and control that data subjects perceive to have when considering their personal information that is collected through internet usage.[153] Hence there is a clear conflict created between data subjects disregarding the information available and the concern they have regarding the usage which has been described as *the Privacy Paradox*.[154] The paradox constitutes a challenge when it comes to achieving the task of informing data subjects that are actively choosing to stay uninformed, resulting in that the data subjects perceive a lack of control and concern, despite the actions taken to provide the users with information in order to reduce this issue. If the data subject wishes to be informed and in control only in theory but not in practice, creating privacy policies that render adequate transparency will not be sufficient. Thus, in order to actually provide adequate transparency, the hindrance of data subjects not wanting to be informed must also be solved.

4.4.2 Peer Pressure

An adjoining challenge in regards to the privacy paradox, is the creation of peer pressure discussed as a behavioural mechanism steering data subjects' willingness to access and read privacy policies. The idea being that the social networks present today form an integral part of society demanding individuals to participate in order to be a part of the societal group. This can be seen as an outflow of the 'forced-consent' issue, constituting that if the data subject does not accept the terms prevalent in the privacy policy regarding their data, they are unable to

[151] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 25 ff.
[152] 0.1-0.2 % read software license agreements. Bakos, Marotta-Wurgler and Trossen (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014): p, 3.
[153] European Commission, Special Eurobarometer 447, Online platforms: p. 74. 'Most are concerned about the data collected about them on the Internet'.
[154] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 29-30.

participate. This peer pressure, Bechmann argues, creates a case of 'social loafing' which is explained as the assumption that since everyone else participates in the online medium, the potential risks of letting the company collect the data subject's data are not properly evaluated and thereby lead to misinformed decisions.[155] Thereby exemplifying another issue connected to the lack of impact analysis conducted by the data subjects.[156]

4.4.3 Creating Active Data Subjects

The overall conclusion and consequence regarding ignorant data subjects is therefore that in order to reach adequate transparency, the data subjects are required to act in accordance with their concern. Creating engaged data subjects through a legislation can be done with different incentives. The GDPR does in a very modest way include the economic spectra of data, by creating rights as data portability the data subject has the control over the data and thereby the possibility to use it as an economic leverage. However, this would require that all individuals using a service demands more, financially or of the service, for providing the company with their data in order to impact the major data collections currently held within companies. There is also the possibility of creating fear within the individuals in order to engage them in the use of their data. As we have seen there are already a concern amongst data subjects on how their data is being used. This concern is still outweighed by the collective action of society in using the services. Providing for further legal actions, easily accessible for the data subject is a way of creating an awareness amongst individuals, if used and successful. The success rate of the rights given to the data subject through the GDPR would likely pave the way for further actions to create an aware and active data subject. Thus, steering away from the actively uninformed data subject portrayed today.

4.5 Transparency and Trust

With the GDPR explicitly claiming that the regulation will provide the data subjects with trust as seen in the discussion on transparency through the GDPR, there is as mentioned a presumption of transparency generating trust.[157] Since this idea is incorporated in the regulation, an attempt to define the connection between transparency and trust will be made by showing when the regulation and the practical function of privacy policies as EULAs enables this connection and when it hinders it.

The challenge of information fatigue will have a limiting effect on trust since the possibility for the data subject to comprehend what is being transparent can be argued to be a key element for

[155] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 27.
[156] See 4.3 above.
[157] The GDPR, recital 7; see also 2.2.

trust.[158] It has been shown that the need for the three initial challenges shown above, connected to the documents, to be solved is crucial for creating trust. This due to the fact that if the data subjects cannot assimilate the information in regards to scope, they are also hindered to comprehend. Thus also unable to predict possible impact and thereby unable make an informed choice. As has been touched upon, the risk assessment a data subject should be able to conduct when allowing collection of personal data can also be misinterpreted or not executed at all. They then fall in the challenge of becoming ignorant data subjects.[159]

However, ignorance can also be a component that generates trust. Solove has addressed one issue of transparency created, when a company displays all information available in relation to the collection, as a fake feeling of control for the data subject. The information provided with complete transparency can then create a feeling of being informed and thus in control for the data subjects. However, the limited comprehension of the data subject might invalidate the possibility of a risk assessment and the factual control and thereby the complete transparency renders a false trust for the data subjects.[160]

The relationship between transparency and trust is therefore prevalent as is stipulated in the GDPR, the idea of more transparency always being a positive impact on trust can however not be seen as evident. It is therefore of essence, in order for the GDPR to reach the aim of generating trust, that the transparency provided constitutes adequate transparency.

4.6 Conclusion

The issues of informing data subject, in an adequately transparent way, are not strictly limited to the use of privacy policies as EULAs as information format, but in many regards connected to the way data subjects are able to comprehend and absorb the information provided, as have been shown here. It is therefore necessary to discuss the suitability of privacy policies as EULAs from both the perspective of the information presented as a written agreement but also from the perspective of user friendliness to generate comprehensibility. This will be further addressed based on the discussion of privacy policies format as EULAs and their challenges in the following chapter, evaluating the suitability of providing adequate transparency in privacy policies as EULAs.

[158] Not forgetting the fact that the ignorant data subject accepts privacy policies despite being uniformed, as seen through the privacy paradox, section 4.4.
[159] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014): p. 34.
[160] Solove. 'Introduction: Privacy Self-Management and the Consent Dilemma.', *126 Harvard Law Review*, (2013): p. 1887. More generally, "people are more willing to take risks, and judge those risks as less severe, when they feel in control.".

5. EULAs Suitability in Providing Adequate Transparency

5.1 Introduction

As has been clarified through the discussion on transparency within the GDPR, the demand on transparency works as a user-centric feature rather than a legalistic requirement within the regulation.[161] The function of transparency is therefore responding to the aim of the GDPR being a regulation directed towards empowering the data subjects. The discussion of the demand for transparency clarifies a number of obstacles, as seen through the challenges of the EULAs as contract forms and information providers above. This chapter aim to further discuss whether the privacy policies as EULAs can function as a suitable mean in reaching an adequate transparency for users from the perspective of the challenges with providing transparency.

Therefore, the discussion will be based on the setting formed by the requirements framed in the GDPR of privacy policies being short and concise, written in common and clear language and the factual design presented in the taxonomy and the information providing capacity of the EULAs as seen within the challenges presented above.

Since the existence of privacy policies available, and in many cases unavoidable, today is immense and brought to the data subjects' attention on a near to daily basis there is no question that they are the main way of providing information regarding company's privacy conduct. Although the suitability of the format is questioned in this thesis, the view of privacy policies as the primary information providers is the direct opposite. The 2018 Handbook on European Data Protection Law deems privacy policies on websites as being one of the most efficient ways to provide information to data subjects.[162] The Handbook also exemplifies the appearance of a privacy policy taking up just about two pages. Based on the discussion of demands in the GDPR as well as the appearance of privacy policies, two important angles needs to be addressed in relation to this guidance. The first being why companies seemingly experience issues with providing a comprehensible privacy policy in terms of length and clarity. The second being that even if companies reached comprehensible privacy policies, can the EULAs format overcome the hindrance of ignorant data subjects.

5.2 The Form of End User License Agreements

The fact that EULAs are created to function as legal contract has been mentioned both initially as well as when viewing the selected privacy policies. [163] The functionality has thus created the

[161] See section 2.4; Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.5, (4).
[162] EU Publications, Handbook on European data protection law, 2018 edition: p. 213.
[163] Tene and Polonetsky. 'Big Data for All: Privacy and User Control in the Age of Analytics.', *Northwestern Journal of Technology and Intellectual Property* vol. 11, no. 5 (2013): p. 261, §56.

structure for privacy policies as they have developed within these agreements. The first perspective, the difficulty with reaching appropriate length and clarity, hindering companies from reaching adequate transparency through their privacy policies will be discussed and answered from the perspective of privacy policies being legal contracts.

The original form of EULAs was created by software companies providing different licenses for usage of their software, which also had as its goal to prevent unsolicited usage of their product by the customers, i.e. a contractual agreement in order to be able to retribute wrongful behaviour. [164] To provide the user with fair and adequate transparency of what data the company collected was therefore not a necessary part of the agreement. With increased demands put on awareness and practices around privacy, companies moved the privacy policy regarding data and personal information to its own document, with the form of EULAs intact. The privacy policies thus still function as a liability waiver, ensuring that the company remained guarded against legal repercussions. The origin of privacy policies as part of agreements regulating usages can therefore be seen as the reason for its historic length and legalistic language. Since agreements and contract are most commonly written by lawyers with the aim of legal safeguard there was no evident requirement for making the content understandable since the validity of the agreement remained for legal practitioners to dispute.

5.2.1 Extensive Collection

As the possibilities for data collection, aggregation and profiling increased, and are still increasing, with the online environment, the desire to collect more information than directly needed in order to provide the service, prevailed. In order to ensure a legal basis for this extensive collection, it could thus be done through a diffuse, lengthy and seldom read privacy policy. The possible function of collecting more information than necessary would then, by data subject accepting the privacy policy, be based on the consent to share information from the data subject, incorporated in the privacy policy.[165] The fact that they are seldom read is in some sense positive for a company that wishes to collect more information than directly necessary for the service and have the possibility to evolve the profitable usage of personal data. A privacy policy including this purpose could then, theoretically, safeguard against even, if read and understood, sceptic usages.

However, as the view on data privacy has become a more user-centric and an empowering legislation has been enforced, higher demands have also been places upon companies to act fairly against their user and consumers as seen through the discussion on the enhanced

[164] Tene and Polonetsky. 'Big Data for All: Privacy and User Control in the Age of Analytics.', *Northwestern Journal of Technology and Intellectual Property* vol. 11, no. 5 (2013): p. 261, §56.
[165] Datatilsynet, The Great Data Race – How commercial utilization of personal data challenges privacy, p. 43.

transparency demand.[166] The very limited transparency that has been historically prevalent in the agreements regulated through EULAs are therefore in need of reform in order to meet the adequate transparency needed to create informed data subjects.[167]

5.2.2 Suitability

The legal aim of EULAs are therefore not particularly suitable for providing the required transparency and information that is to be provided to data subjects through the new privacy regulation, the GDPR. This is further supported by the analysis presented in the taxonomy, showing that the selected companies all struggle to meet the 'clear formulations' requirement and use numerous formulations hindering clarity and thus also adequate transparency. Since the privacy policies needs to fulfil the requirements of the GDPR they still, in one regard, serve to ensure that the company remains liability free. At least in relation to providing the transparency and information demanded by the regulation. There is therefore a need to balance the origin of non-negotiated liability contracts that EULAs have been, with the communications aid to data subjects that privacy policies needs to become in order to remain liability free in relation to the GDPR.

5.3 The Usage of Data as a Hindrance of Comprehensibility

The complexity of data usage that has been created through the advancement of technology can furthermore be argued to hinder the EULAs possibility to provide adequate transparency due to the length and complexity of the information. This complexity evolves with the numerous ways of using data today, which is also quickly advancing with technologies such as AI and the value of data as currency.[168]

Companies collecting data through the usage of their services thus also aspires to maximise the value of the data collected in order to improve their user-experience and service. This also renders that the usage of the data changes at the same rapid speed as new possible usages develop. Data that was originally collected in order to render a service of recommending similar products will in the following step be used for marketing purposes on a different site than the one used by the data subject when the data was provided.[169]

Since the GDPR require that the data subject becomes informed at the time of collection the future possible or known usage must also be provided to the data subject when the data is first collected. For this the EULAs have the possibility of functioning well, providing the data

[166] See chapter 2.
[167] See chapter 3.
[168] Larsson, Ledendal. (2017) Personuppgifter som betalningsmedel, p.14-15.
[169] Compare Google when recommending guitar lessons in ads through Gmail based on the view of guitar tutorials on YouTube. This usage is known and exemplified in their privacy policy.

subject with a text explaining the current usage of the data by the company and what it will be used for going forward. This does require that the company knows what the forthcoming use will be and can simply in a short manner explain this to the data subject. However, if the EULAs were to cover all the theoretically possible future usage of that information at the same time, they would likely lose many of the other features necessary for adequate transparency as shown in the taxonomy. Most notably, the coverage of possible usages would render the information diffuse and unclear since the data subject would be left with several different scenarios and thereby the possible foreseeability will decrease. Additionally, the length would quickly escalate and the demand on the information to be given in a 'short and concise' manner would be difficult to achieve.

At what time information is provided can therefore be used to avoid the issue with too elusive and lengthy provisions regarding all usages by simply keeping the data subject updated and presented with an additional choice, as the possible usage evolves. This can be done with technical features such as notices. This possibility in form up pop-up notices will be further elaborated in the discussion regarding alterations in chapter six.

5.4 Users Being Unwilling Recipients

The second angle to address responds to the data subject's perception of the privacy policies. Since the suitability of EULAs providing adequate transparency also depends on this perspective a short discussion will be devoted to what the data subjects actually want and how they act. As has been made clear through this thesis, simultaneously as the awareness of data collection and usage as well as privacy legislation have developed so has the demand for more transparency and control by data subjects.[170] The purpose of the GDPR being an empowerment tool for individuals responds to this awareness and demand, but as has been argued throughout, the action of the data subjects is not coherent with these thoughts.

The underlying issue for this thesis, includes the perception that few data subjects read the privacy policies presented to them. Through the studies present in this thesis so far, along with numerous more in different perspectives, it can at the very least be established that the number of data subjects not reading privacy policies massively precedes the amount who does.[171] This social behaviour is the most notable hindrance to provide adequate transparency but is not necessarily linked to the form of EULAs. However, if the assumption is made that this lack of

[170] European Commission, Special Eurobarometer 447, Online platforms: p. 74. 'Most are concerned about the data collected about them on the Internet'.
[171] Bakos, Marotta-Wurgler and Trossen (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014); Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011); Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies 11, no.* 1 (2014): p. 35.

interest depends on the privacy policy format, this could be linked to the previous, and still current, purpose of EULAs as agreements to be written and argued by legal professionals. That purpose would then strengthen the distance of data subjects since it is seen as not aimed for their comprehension. Another aspect that in part presents the previous view of data subjects regarding privacy policies as lacking relevance, can be found in the knowledge about the privacy policies aim. A study conducted in the US worryingly concluded that 57% of the respondents believed that the existence of a privacy policy by a company in itself safeguarded them from having the company share the data collected.[172] However, this study was conducted over a decade ago and the knowledge of privacy legislation is likely to have increased amongst individuals and within society at large.

Nevertheless, functions such as opt-out possibilities which can allow for the data subject to be in control of how they surrender their data, are seldom used, indicating that the behaviour of data subjects might not be entirely steered by the form of privacy policies but rather the pursued usage of a service. The primary focus is then being on the original purpose of the visit, such as a purchase or a service which deters the data subjects focus from finding out how privacy is handled rendering users to simply accept in order to continue with the main purpose.[173]

One aspect that could possibly resolve the issue of unwilling data subject is the idea of Privacy Enhancing Tools (PETs) that allows for an assessment of the privacy policies by the data subject. The possibility to use PETs to evaluate and control privacy policies would, leaving the evaluation easy to see for data subjects, then render that data subject can at any time gain adequate transparency and that it is therefore enough to uphold the standards regulated in the GDPR.[174] The potential of this will be further elaborated in the discussion on amendments in chapter six.

As mentioned above the suitability of privacy policies as EULAs and the possible solutions to the identified challenges must include the perspective of the unwilling data subject in order to reach an informed data subject.

5.5 Issues Regarding Consent

Given the above difficulties of providing information to data subjects, solutions and arguments such as Nissenbaum's regarding the malfunction of user consent needs to be evaluated. Not only the difficulty with length and technicality of the EULA structure but the unwillingness and lack of comprehensibility amongst data subjects render that including consent as a part of the

[172] Turow, Joseph. 'Americans and Online Privacy: The System is Broken.', A report from The Annenberg Public Policy Center of the University of Pennsylvania. June 2003, p. 3.
[173] Datatilsynet, The Great Data Race – How commercial utilization of personal data challenges privacy, p. 40.
[174] The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, November 2017, *remote audit of enforcement*.

privacy policy will render non-informed consent. Hence data subjects can give their consent without the consent being based on actual knowledge. Nissenbaum point to this uneven structure of information between company and data user as the foundation for changing collection and usage of personal information based on consent completely. Instead of consent based on information, a contextual concept is provided, based on the idea that what personal information should be allowed to be collected will be based on from what context it is provided.[175] This is however a method that has been argued to open up for the issue of regulating how to limit the information collection, specifically how to decide where one context end and the following begins.[176] It can therefore generate function creep, expanding the use of the personal information by the company, bit by bit.[177] Although the collection based on consent have been questioned and can be argued to be shallow, the issues of non-informed and too unspecific consent have been addressed and believed to be amended throughout the GDPR with the evolved requirements of valid consent.[178] In regards to hindering function creep the requirement on specific consent is aimed to prohibit the broadening of the original data collection purpose.[179]

Therefore, if the adequate transparency for data subjects can be reached through the GDPR this would limit the issues with consent since the data subject would be informed and thus capable through transparency to make a valid choice on whether to consent or not, to the proposed collection. The GDPRs enhancement on consent can therefore be argued to be dependent on the function of providing transparency as it is required in the legislation.

5.6 Conclusion

"Users are not the experts in privacy and security, it's actually Google", "Google should be telling users what's wrong, we should point out the anomalies, and guide users through their settings."[180]

With this quote the suitability of EULAs for providing adequate transparency to the data subjects can be summarized. They are not, in the form of lengthy, complex, legal agreements, suitable, given the lack of knowledge, insight and interest amongst the data subjects, to provide adequate transparency. The companies thus need to change their privacy policies from legal

[175] Joergensen, 'The unbearable lightness of user consent.' *Internet policy Review*, 3, no.4. (2014): p.8f.; Nissenbaum, 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011); Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, no. 1 (2014).
[176] Bechmann, 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies 11, no.* 1 (2014): p. 30.
[177] See also section 3.2.1 above on the problems regarding function creep.
[178] The GDPR, recital 32, 42, 43, article 4 (10), article 6, 1(a), article 7.
[179] Article 29 WP, Guidelines on consent under Regulation 2016/679, p. 11-12.
[180] Kim Guemmy, Product management lead for Google account security, in Newman, H., L., 'The Privacy Battle to Save Google From Itself', *Wired*.

and technical documents and create an actual tool for users in order to create willing and informed data-subjects.

These tools need to be persistent and simple enough for the data subject to, not only comprehend but be willing to participate by actively controlling their data. Since the discussion has elaborated on the difficulty in balancing the historically strong legal regulating function of EULAs with the new, through legal measures, required transparency, the structure and form of privacy policies need to be more clearly detached from the function of legal documents. This due to the most prominent hindrances are, as have been discussed, linked to original function of EULAs. It can therefore be argued that if the companies does not manage to adapt their privacy policies to the adequate transparency demanded, the previous function of the agreements as ensuring that the companies remain liability free will render that the companies become liable in relation to not meeting the new requirements of transparency in the GDPR. Thus, the previous function now renders incompatibility with the new regulation, demanding a change of the privacy policies structure.

The exclusion of legalistic language, lengthy ambiguous phrasings as well as the cover-all approach present in many privacy policies, will benefit the objectives of the GDPR and render more adequate transparency for users. How and if these alterations can be achieved within the privacy policies present today will be discussed in the following chapter.

6. Room for Alterations

6.1 Introduction

With the GDPR on its way to be enforced, companies attempted to update and adjust their privacy policies in order to meet the new demands, as seen in this thesis, not quite reaching the finishing line. This aim for adaption can be seen in the taxonomy where all privacy policies were amended in the month leading up to the implementation of the regulation.[181] Also evident in the discussion of the privacy policies selected for this thesis is that they are not providing adequate transparency in relation to the criteria despite the amendments made. Furthermore, already during the very first day of the GDPR being in force, the 'free consent' provision was argued to be breached.[182]

Since then, with the GDPR being well into the second half of its first year, some alterations to the privacy policies would be desired by now, however it is likely that most companies will

[181] May 2018. Microsoft having been amended once more in October 2018.
[182] NOYB – European Center for Digital Rights, update on filed privacy complaints.

remain seated waiting for legal rulings acting as guidance before amending their policies further. Therefore the few remarks to be made in this chapter will be strictly based on the findings in this thesis since there are not yet any case law available.[183]

As shown in the previous chapter there are several difficulties with providing adequate transparency to data subjects, steering clear of information fatigue and at the same time provide enough information for data subjects to be informed, conscious and in control of their data. But before addressing what can be done to balance these difficulties a short section will present what the GDPR actually rendered in terms of amended privacy policies.

A study comparing the largest online companies, to some extent the same companies subject to this thesis taxonomy, have been aimed at showing the privacy policies before and after the enforcement of GDPR in relation to word count, time it takes to read the policy and the grade level of reading required for understanding the content. The study surprisingly showed increased issues both in regards to the above mentioned issues of information fatigue with the words enhanced as well as time consumption and in some cases also the language skills required.[184]

Since most of the individuals that are considered to be data subjects today also fall into the definition of consumers,[185] the question of privacy policies as EULAs can be seen as in the same section as 'consumer-friendly and fair'-agreements fall into. This has led to a number of consumer agencies addressing the privacy policy agreements and their appearance.[186] These reviews and the concluding suggestions for improvements will therefore serve as a foundation for the discussion regarding possible measures to create a more adequate transparency through the privacy policies.

6.2 Potential Alterations

The Norwegian Consumer Council conducted a project in 2016, amplifying the need for more insight into the terms prevailing online, including the many privacy policies connected to apps. The project resulted in a set of suggestions for creating privacy policies that would render comprehensibility among users.[187] Some of these recommendations have been discussed in detail in regards to the EULAs functionality and with the guidelines provided by the Article 29 WP.[188]

[183] In relation to the questions discussed in this thesis regarding transparency.
[184] Sobers. 'The Average Reading Level of a Privacy Policy', *Varonis* (2018).
[185] Rhoen. 'Beyond consent: improving data protection through consumer protection law.' *Internet Policy Review*, vol. 5, no.1. (2016): Introduction.
[186] E.g. the Norwegian Forbrukarrådet.
[187] Forbrukerrådet, 250,000 words of app terms and conditions, May 2016.
[188] Such as, short and concise, common language, structure and headings.

However, the final suggestion put forwards by the Council to '*Adopt an industry standard*' has not been addressed so far and specifically relates to future alterations, it will therefore be given some attention.

6.2.1 Industry Standard

How information about data collection is provided to the data subjects through privacy policies can be seen as a custom that have evolved in relation to the evolvement of the collection and legislation. However, as we have seen above this custom does not portray in a uniform way in companies' privacy policies appearance nor information. The suggestion of an industry standard, as put forth by the Council aims at creating a coherence between privacy policies that avoids individual provisions for each company, thereby making it easier for the data subjects to relate to the information provided and build trust.[189] A similarity between the companies' privacy policies would enable an awareness for the data subject in relation to where to look for specific information and also be aware of what information they should be able to find when reading a privacy policy, even when they are provided from a previously unknown company. Companies with specific collections or usages of data could then simply provide the sections that differs from the standard in a clear and concise way. An industry standard can therefore contribute to decreasing the time it takes for data subjects to not only read but also become familiar and understand each company's different policy. Thus, also enabling fulfilment of the goal of short and concise privacy policies.

A report from the Office of the Privacy Commissioner of Canada written in November 2017, argues in the opposite direction, from an industry standard, to enable negotiation possibilities for consumers to avoid the take-it or leave-it approach apparent today. Although complete opposite from the Norwegian proposition they too argue that it would generate more trust if the data subjects had the possibility to impact the privacy policy faced with.[190] Given that one of the most prominent issues with privacy policies today constitutes the multitude of them apparent in each individual's life, the likeliness of data subjects actually using the negotiation possibility is here argued to be low. Even though the possibility might be expressed as desired, finding the time to negotiate the terms after first overcoming the obstacle of information fatigue and search for enough information to be able to comprehend what to negotiate towards, are not realistic scenarios. Creating privacy policies that can to each extent be fully negotiated by the data subject will therefore likely hinder adequate transparency to users.

However, a combination of an industry standard and negotiation in the form of selections can render enough familiarity and options for the data subject to be informed as well as in control.

[189] Forbrukerrådet, 250,000 words of app terms and conditions, May 2016.
[190] The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, November 2017.

Creating an industry standard privacy policy that also contains different alternatives specially directed to the company in question, of which the data subject could select to enable or not, the perceived control could also generate more trust without compromising the foundational insight provided through the industry standard.

6.2.2 Pop-up Notices

In relation to asking for specific consent, as required by the GDPR, this is already being done by a variation of the above mentioned alternatives. Through pop-up notices the data subject is being cautioned about the fact that within the service about to be entered, or within a specific feature of an application, consent in required since collection of personal data will occur. The idea of using alternative technical information methods for providing the data subject with informed transparency, is in theory, a way to be more transparent regarding the collection and usage of personal information. However, some of these practices have been a more apparent take-it or leave-it approach requiring a new consent from its users in order to continue using the service or application.[191] The applicability of this function in relation to the GDPR is yet to be determined as the complaints are still being processed.[192]

Although the function of pop-up notices is clearly questioned in relation to the data subjects possibility to deliver 'free consent' they have the possibility to enable a higher degree of adequate transparency. The usage of personal information acting as a hindrance for data subjects to comprehend could, to some extent, be combated through the use of pop-up notices.[193] Submitting a notice to the data subject as the usages of personal information evolves would enable different usages to progress as well as allow for the company to ask for renewed consent when needed. Perhaps this will require the possibility of the data subject to reject, without suffering consequences of limited usage. At the same time companies would ensure that they provide the information at the time of collection without burdening the original privacy policy with vague and lengthy elaborations on all possible future usages. If the type of usage that was informed about through the notice would evolve to become the foundational collection of the company, the privacy policy can simply be amended thereafter.

Although the use of pop-up notices can be argued to enhance the transparency and information provided to the data subject, a difficulty with this could be the interference they construe in the user experience of the service. The frequency of pop-up notices can create an irritation rendering the data subject to experience fatigue. Although not information fatigue in the sense of too much information, the same consequences can occur if the data subject is being subjected to multiple choices requiring action. Rendering in that the data subject simply accepts in order

[191] See 2.3 above.
[192] NOYB – European Center for Digital Rights, update on filed privacy complaints.
[193] See 5.3 above.

to continue to access the wanted service. The use of these pop-up information provisions has evolved and is currently used by e.g. Google and Facebook. The idea of providing the data subject with continuous information should however only be used when suitable.[194] This since there is a limit for the amount of pop-up notices enabling more adequate transparency for users and not creating fatigue, to be aware of when using them to provide the data subject with information.

6.2.3 Review System

The usage of PETs to allow for control of the privacy policies in relation to the GDPR have been argued to render the possibility of providing a stamp of approval in relation to companies' policies.[195] Thus generating a review system which could function as an incentive for the data subject to be informed about privacy policies.

The usefulness of this rendering adequate transparency for data subjects can however be strongly questioned. The theory of *informed minority* is based on the similar perspective of a few controlling data subjects that can and will prosecute bad terms and thus generate fair terms on a general basis for all data subjects. The effectivity on this is however limited due to the fact that the informed minority has not been shown to have an impact, rendering in the conclusion that it could be too little to matter.[196] The effectiveness of PETs would therefore be dependent on the active participation and realization of remote auditing which in relation to the unwilling data subject portrayed above, remains unlikely. The issue would then remain with creating informed data subjects.

6.2.4 Privacy Policies as a Competitive Edge

Finally, to achieve the possible amendments to the structure of privacy policies and create a more adequate transparency for users, the participation of the companies will be fundamental. Enabling companies to see privacy protection and thus the effective and functioning privacy policies as a competitive edge has been noted by the European Data Protection Supervisor (EDPS) as one way that would increase privacy protection.[197] Creating privacy policies that meet the demands in the GDPR would therefore be an incentive for companies to create adequate transparency through the policies in order to be validated as user friendly.

---

[194] Article 29 WP, Guidelines on transparency under Regulation 2016/679, p.21 (39); Schaub. 'Nobody reads privacy policies – here's how to fix that.' *The Conversation.* (2017).
[195] The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, November 2017, *trust mark*.
[196] Bakos, Marotta-Wurgler and Trossen (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014): p.2, 5ff.
[197] Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: p. 34, (75).

As noted by the EDPS, there has been similar demands that have rendered competitiveness on the market in form of the corporate social and environmental responsibility (CSR). The idea thus being that if consumers rate and chose their social media platform, online service providers and similar functions provided by companies, based on the privacy policy in place it will become financially profitable to be transparent and create adequate information for users and thus also profitable for companies.[198] Within this aspect, the view of auditing through PETs and a review system can be argued to fill a function, allowing for the data subject to quickly create a perception about the privacy policies within a previous unknown company. However, the idea of transparency as a market advantage falls short in the perspective of the massive amount of services collecting data, these services can be argued to be to a very limited extent interchangeable and thus creating little room for selecting another service if one does not measure up to the transparency required.

To conclude, besides the overall ambition of reaching the requirements within the GDPR, there are two identified ways of amending the privacy policies in order to reach a better suitability. The first being the adoption of an industry standard with suitable, pop-up notices for creating an adaptive and informative functionality for the data subject. The second way being to rely on the adaption of companies' privacy policies to the demands of the GDPR and having the formality of this adaption be evaluated through a reviewing data subject. In regards to the overall challenges, the first amendment will be likely to have a better chance of reaching adequate transparency since it calls for a complete re-evaluation of the form when creating an industry standard, hence not having to be dependent on the action of data subjects to provide critique.

6.3 Current 'Best Practice' in Privacy Policies

Based on the challenges with privacy policies occurring and the possible alterations presented above, it can be concluded that the presentations of privacy policies, within the form of EULAs, vary in how well they generate adequate transparency. Despite the many guidelines and variations in how to provide information, the best practice often occur in sections of a privacy policy, no one adapting them in full.

An aspect constituting a best practice amongst providing adequate transparency for data subjects can be identified in companies creating a bullet-list of options. This function is most frequently appearing when consent is asked for different collections and usages for marketing purposes. Since these lists are made directly visible and lifted out from the general document containing the privacy policy, they become accessible to the data subject which creates a higher degree of transparency as well as better informed data subjects. There are however limitations

[198] Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: p. 34, (75).

to this practice. If all possible selections of usage were placed in this order so that the data subject needed to address them individually, it would probably be more time consuming than today, when data subjects are expected to read the entire policy. The practice might generate an actual choice and selection not present today but it is despite this not to be aimed for in regards to all information prevailing in the privacy policies. That bullet-lists are used in regards to marketing is most likely due to the immediate impact and implication of marketing, apparent for the data subject. Agreeing to a privacy policy containing provisions that will allow for the company to conduct direct marketing to the data subject has a direct effect in the form of the marketing correspondence following and is therefore an evident choice rendering the data subject to feel in control.

A next step on what could be provided through the bullet-list method, should be the more elusive part of the privacy policies addressing how and when sharing information with affiliations and third parties take place. However, this is a more controversial question due to the lack of insight into the process of sharing given to the data subject, through the black box society. If these actions were lifted out of the privacy policy as a direct and clear choice for the data subject, transparency would be increased and information would be clearer whether the company shares personal information or not. The eagerness of companies to disclose the precise measure of how they share data is, as have been discussed, not evident in the privacy policies analysed and most likely not something companies are willing to highlight further.

Additionally, the function of layers, as occurring in six out of the eight privacy policies considered should also be noted as considered a best practice. Layers can be and are, as discussed, used in different extension and for different reasons such as navigation or explanations and this needs to be kept in mind when aspiring for a best practice. With the comprehension of the data subject as the main priority the usage of layers for navigations should constitute a minimum threshold and thereby not reach the level of best practice. Evolving the use of layers in order to further provide the data subject with the information best needed at different times should therefore be a priority.

7. Concluding Remarks

Through the increased information and transparency demands within the GDPR, the functionality and issues with the criteria in the current structure of privacy policies as EULAs and their actual function have been analysed and discussed. This discussion further demonstrates that the data subjects are not provided with adequate transparency, regardless of the establishment of transparency and information provisions and criteria. Hence rendering the data subjects to remain actively uninformed. It has further been concluded that the form of the privacy policies need to be adapted in order to function as a transparency tool for the data subjects both in regards to comprehensibility, with the information provided, and accessibility in regards to the structure and custom of not accessing EULAs.

There is thus a need to further evaluate and reform the structure of providing information to data subjects in order to reach adequate transparency. While some changes are occurring with pop-up notices as well as layered approaches with explanations, the main obstacle remains the unwilling data subject. This could be solved by creating a practice with privacy policies that demands the data subject to be informed, rendering that they simply cannot remain uninformed. However, creating a regulation that aims to render control to the individual does not correspond to an execution of the regulation that forces transparency on the individual. This might not be desired nor possible to reach since it would have additional effects on the autonomy of individuals and their personal information, directly opposing the aim of the current regulation. Attempting to create an informed data subject is nevertheless the only way to fully render the adequate transparency necessary in order for the GDPR to be efficient in the aim of providing control to the data subject.

The application of the GDPR in privacy policies, in order to adhere to the requirements, has been shown to be insufficiently performed in the taxonomy and the challenges present within the structure of privacy policies as EULAs. Thereby facing the risk of generating a new form of blind, non-informed consent, with the result of an active but automatic data subject simply accepting what is necessary to reach the end goal. In order to avoid this, the adaption of privacy policies, to a more obvious and including format, through an industry standard as exemplified above, cannot be too forceful. Hence the goal is to interest the data subjects to participate instead of forcing them. If the interest of the data subjects shown in the studies above is concluded as misleading it might be time to further question if the area of data privacy can be left to the ignorant data subjects and instead leave the transparency and choice structure still part of privacy legislation today.

There are, as discussed, many possibilities of the GDPRs demand on transparency to function as a tool for the data subject. However, the practical use and function of privacy policies need to adapt to this view of transparency as a tool and adapt into a form engaging the data subjects

participation. It is however not desired to force the individuals to participate since this reinforces the current actively uninformed data subjects. To conclude, the informed data subjects sought in order for the adequate transparency, needed for the GDPR as a privacy legislation, to be effective needs to be created for the regulation to be effectively protecting individuals privacy.

Bibliography

Literature

Ledendal, Jonas, Larsson, Stefan, Wernberg, Joakim. *Offentlighet i det digitala samhället, vidareutnyttjande, sekretess och dataskydd*. Nordstedts juridik Karnov Group, 2018 (cit: Ledendal, Larsson, Wernberg. *Offentlighet i det digitala samhället*)

Pasquale, Frank. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge MA, USA: Harvard University Press, 2015 (cit: Pasquale. *The Black Box Society*)

Zuiderveen Borgesius, Frederik.'Behavioural Science and the Regulation of Privacy on the Internet'. In *Nudging and the Law - What can EU Law learn from Behavioural Sciences?*, edited by Alberto Alemanno and Anne-Lise Sibony, 179-209. Hart Publishing, 2015.

Reports

Datatilsynet, The Great Data Race – How commercial utilization of personal data challenges privacy, November 2015. https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf, accessed 16-10-2018.

FTC report, (2012) Privacy in an Era of Rapid Change, Recommendations for businesses and policymakers, p. 3. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, accessed 20-11-2018.

Larsson, Stefan, Ledendal, Jonas. Personuppgifter som betalningsmedel. (4 red.) Karlstad: Konsumentverket, 2017.

Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, The Office of the Privacy Commissioner of Canada, Privacy Enhancing Technologies – A Review of Tools and Techniques, November 2017. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711 , accessed 25-10-2018.

Turow, Joseph. 'Americans and Online Privacy: The System is Broken.', A report from The Annenberg Public Policy Center of the University of Pennsylvania. June 2003. http://repository.upenn.edu/asc_papers/401

Journal Articles

Bakos, Yannis, Marotta-Wurgler, Florencia and Trossen, David, R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, 43, no. 1(2014): 1-45. http://dx.doi.org/10.2139/ssrn.1443256

Bechmann, Anja. 'Non-informed consent cultures: Privacy policies and app contracts on Facebook.' *Journal of Media Business Studies* 11, *no.* 1 (2014): 21-38. https://doi.org/10.1080/16522354.2014.11073574

Joergensen, Rikke, F. 'The unbearable lightness of user consent.' *Internet policy Review*, 3, no.4. (2014) DOI: 10.14763/2014.4.330

McDonald, Aleecia. M. and Cranor, Lorrie. Faith. 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society* vol. 4, no. 3 (2008): 543-568. http://hdl.handle.net/1811/72839

Nissenbaum , Helen. 'A Contextual Approach to Privacy Online.' *Daedalus*, Vol. 140, no. 4, Protecting the Internet as a Public Commons, (2011) pp. 32-48. Published by: The MIT Press on behalf of American Academy of Arts & Sciences. https://doi.org/10.1162/DAED_a_00113

Rauhofer, Judith. 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?' *European Data Protection Law Review,* vol. 1, no.1 (2015): 5-15.

Reidenberg, Joel, R., Bhatia, Jaspreet, Breaux and Travis, Norton, Thomas. 'Ambiguity in Privacy Policies and the Impact of Regulation.' *Journal of Legal Studies, Forthcoming, Fordham Law Legal Studies Research Paper* No. 2715164 (2016): 29 pages. http://dx.doi.org/10.2139/ssrn.2715164

Rhoen, Michiel. 'Beyond consent: improving data protection through consumer protection law.' *Internet Policy Review,* vol. 5, no.1. (2016) DOI: 10.14763/2016.1.404 p.1.

Solove, Daniel, J. 'Introduction: Privacy Self-Management and the Consent Dilemma.', *126 Harvard Law Review*, (2013): 1880-1903.

Tene, Omer and Polonetsky, Jules. 'Big Data for All: Privacy and User Control in the Age of Analytics.', *Northwestern Journal of Technology and Intellectual Property* vol. 11, no. 5 (2013): 239-273. http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

EU Regulations

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

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.

European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)), (2018/C 263/10).

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation).

Guidelines and EU Statements

Article 29 Working Party, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018.

Article 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, as last Revised and adopted on 5 April 2017.

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018.

EU Publications, Handbook on European data protection law, 2018 edition.

European Commission - Press release, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Brussels, 25 January 2012.

European Commission, How to Write Clearly,(2011). https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5

European Commission, Special Eurobarometer 447, Online platforms, Report 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf

Letter to Google from CNIL on behalf of the EU data protection authorities https://www.cnil.fr/sites/default/files/typo/document/Courrier_Google_CE121115_27-02-2012-EN.pdf , accessed 05-11-2018

OECD (2006), "Making Privacy Notices Simple: An OECD Report and Recommendations", *OECD Digital Economy Papers*, No. 120, OECD Publishing. http://dx.doi.org/10.1787/231428216052

OECD Privacy Framework, 2013, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm, accessed 20-11-2018.

OECD webpage for privacy, http://oe.cd/privacy, accessed 20-11-2018.

Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf, accessed 05-11-2018.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010at the 1099th meeting of the Ministers' Deputies, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00, accessed 19-11-2018.

Online Sources

Chen, X., B., 'Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them', *the New York Times* (2018). https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html, accessed 07-11-2018.

Dictionary, 'function creep', https://www.dictionary.com/browse/function-creep, accessed 08-11-2018.

Forbrukerrådet, 250,000 words of app terms and conditions, May 2016. https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/ , accessed 26-10-2018.

Hern, A., 'Most GDPR emails unnecessary and some illegal, say experts', *The Guardian* (2018), https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts, accessed 07-11-2018.

Kelion, L., 'How to handle the flood of GDPR privacy updates', *BBC* (2018). https://www.bbc.com/news/technology-43907689, accessed 07-11-2018.

Larsson, S., 'DATA/TRUST: Tillitsbaserad personuppgiftshantering i den digitala ekonomin', Handelsrådet, research projekt 2018-2020. http://handelsradet.se/forskning-och-utveckling/forskningsprojekt/forskning-relevant-for-handelsnaringen-2018/data-trust/, accessed 03-12-2018.

Löfgren, E., 'Samtycket enligt den allmänna dataskyddsförordningen, Personuppgiftsansvarigas ansvar och registrerade personers rätt till öppenhet och självbestämmande', Master Thesis, Faculty of Law, Lund University (2017). http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8930852&fileOId=8933704, accessed 22-10-2018.

Newman, H., L., 'The Privacy Battle to Save Google From Itself', *Wired*. https://www.wired.com/story/google-privacy-data/ , accessed 29-10-2018.

NOYB – European Center for Digital Rights, update on filed privacy complaints, https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf, accessed 05-11-2018.

Saint, Nick, *Business Insider*, Eric Schmidt: Googles policy is to 'get right up to the creepy line and not cross it', October 2010. https://www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10?r=US&IR=T&IR=T, accessed 16-10-2018.

Schaub, Florian. 'Nobody reads privacy policies – here's how to fix that.' *The Conversation.* (2017). http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932, accessed 13-11-2018.

Sobers, R., 'The Average Reading Level of a Privacy Policy', *Varonis* (2018) https://www.varonis.com/blog/gdpr-privacy-policy/, accessed 07-11-2018.

Privacy Policies

All of the privacy policies were accessed on the 5th of November 2018.

Apple Inc.

https://www.apple.com/legal/privacy/en-ww/

eBay Inc.

https://www.ebay.co.uk/pages/help/policies/privacy-policy.html#summary

Google LLC

https://www.gstatic.com/policies/privacy/pdf/20180525/853e41a3/google_privacy_policy_en.pdf

Microsoft Corporation

https://privacy.microsoft.com/en-us/privacystatement#mainenterprisedeveloperproductsmodule

Netflix Inc.

https://help.netflix.com/legal/privacy

Spotify

https://www.spotify.com/uk/legal/privacy-policy/

TripAdvisor LLC

https://tripadvisor.mediaroom.com/UK-privacy-policy

Twitter Inc.

https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-page-gdpr/pdfs/PP_Q22018_April_EN.pdf

.