Universiteit Utrecht

Faculty of Humanities
Version September 2014

PLAGIARISM RULES AWARENESS STATEMENT

Fraud and Plagiarism
Scientific integrity is the foundation of academic life. Utrecht University considers any form of scientific deception to be an extremely serious infraction. Utrecht University therefore expects every student to be aware of, and to abide by, the norms and values regarding scientific integrity.

The most important forms of deception that affect this integrity are fraud and plagiarism. Plagiarism is the copying of another person's work without proper acknowledgement, and it is a form of fraud. The following is a detailed explanation of what is considered to be fraud and plagiarism, with a few concrete examples. Please note that this is not a comprehensive list!

If fraud or plagiarism is detected, the study programme's Examination Committee may decide to impose sanctions. The most serious sanction that the committee can impose is to submit a request to the Executive Board of the University to expel the student from the study programme.

Plagiarism
Plagiarism is the copying of another person's documents, ideas or lines of thought and presenting it as one's own work. You must always accurately indicate from whom you obtained ideas and insights, and you must constantly be aware of the difference between citing, paraphrasing and plagiarising. Students and staff must be very careful in citing sources; this concerns not only printed sources, but also information obtained from the Internet.

The following issues will always be considered to be plagiarism:

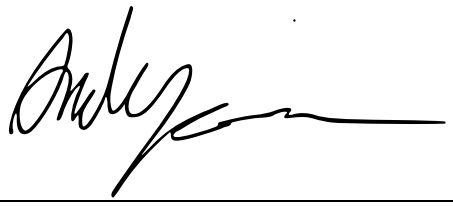
- cutting and pasting text from digital sources, such as an encyclopaedia or digital periodicals, without quotation marks and footnotes;
- cutting and pasting text from the Internet without quotation marks and footnotes;
- copying printed materials, such as books, magazines or encyclopaedias, without quotation marks or footnotes;
- including a translation of one of the sources named above without quotation marks or footnotes;
- paraphrasing (parts of) the texts listed above without proper references: paraphrasing must be marked as such, by expressly mentioning the original author in the text or in a footnote, so that you do not give the impression that it is your own idea;
- copying sound, video or test materials from others without references, and presenting it as one's own work;
- submitting work done previously by the student without reference to the original paper, and presenting it as original work done in the context of the course, without the express permission of the course lecturer;
- copying the work of another student and presenting it as one's own work. If this is done with the consent of the other student, then he or she is also complicit in the plagiarism;
- when one of the authors of a group paper commits plagiarism, then the other co-authors are also complicit in plagiarism if they could or should have known that the person was committing plagiarism;
- submitting papers acquired from a commercial institution, such as an Internet site with summaries or papers, that were written by another person, whether or not that other person received payment for the work.

The rules for plagiarism also apply to rough drafts of papers or (parts of) theses sent to a lecturer for feedback, to the extent that submitting rough drafts for feedback is mentioned in the course handbook or the thesis regulations.
The Education and Examination Regulations (Article 5.15) describe the formal procedure in case of suspicion of fraud and/or plagiarism, and the sanctions that can be imposed.

Ignorance of these rules is not an excuse. Each individual is responsible for their own behaviour. Utrecht University assumes that each student or staff member knows what fraud and plagiarism

Universiteit Utrecht

entail. For its part, Utrecht University works to ensure that students are informed of the principles of scientific practice, which are taught as early as possible in the curriculum, and that students are informed of the institution's criteria for fraud and plagiarism, so that every student knows which norms they must abide by.

I hereby declare that I have read and understood the above.
Name: Anders Holmgaard Johansen Student number: 6492819
Date and signature: 15/12/2019 

Submit this form to your supervisor when you begin writing your Bachelor's final paper or your Master's thesis.

Failure to submit or sign this form does not mean that no sanctions can be imposed if it appears that plagiarism has been committed in the paper.

Universiteit Utrecht

Master thesis

Moving fast and breaking things? Facebook's Lobbying of the European Union's General Data Protection Directive

Keywords: EU Interest Groups, Lobbying, Data Privacy, Facebook, Theory of Access

Anders Holmgaard Johansen
6492819

Supervisor: Dr. Lorena de Vita

MA International Relations in Historical Perspective
Utrecht University
December 15, 2019.

Word count 14.260

Universiteit Utrecht

Abstract

This thesis sets out to investigate to what extent the social media company Facebook influenced the General Data Protection Regulation (GDPR) of the European Union between 2012 and 2016.

Facebook is one of the biggest and most distrusted technology platforms in the World. Multiple times, private data gathered from the platform has been used to meddle with elections or referendums, affecting international relations and democracy. For this reason, it is important to investigate how Facebook participated in the democratic process of shaping a regulation, which limited its business significantly, namely the GDPR.

The purpose of the thesis is two-fold. Firstly, it will enlighten a lay man's audience on the European lobbying process, which can seem secretive and corrupt. Secondly, it will add to the academic literature on EU interest groups, since a study about the influence of data regulation by specific technology companies has never before been conducted.

The thesis will apply multiple acknowledged theories in order to establish a framework, which allows for a trustworthy conclusion. Central to the research are Pieter Bouwen's Theory of Access and Heike Klüver's focus on the aggregated goods of coalitions. In addition, the thesis applies two widely acknowledged methodological approaches, measuring influence. These are as follows: *the assessment of attributed influence*, which relies on interviews with central actors of the legislative process and *the assessment of preference attainment,* which compares Facebook's initial ideals of influence to the final outcome of the GDPR.

The thesis arrives at the conclusion that Facebook on the very salient issue of consent was able to influence the GDPR significantly. Overall, however, Facebook had a modest influence on the GDPR due to the company's lack of information supply, citizen support and coalition work. To that end, the thesis ultimately concludes that politicians of the Western world are increasingly acting as guardians of data privacy.

Table of contents

Introduction

Through the past five decades, the Internet has undergone a major evolution. From its use as a military experiment during the Cold War to its transformation into a civilian utility (Naughton 2016). Today, 4.39 billion humans around the world are connected to the Internet (Hootsuite 2019). But as the Internet has proved its success of connecting people, an obstacle has occurred regarding privacy and data protection, affecting ultimately the future of democracy. Today, internet companies to a large extent monetize personal information, leaving users with an abundance of free services, but little control over how their personal data is processed and used for commercial purposes. Thus, the Internet has turned into a multi-Trillion dollar industry fed by user data freely given away, often without the user's informed consent.

With the rise of the commercialisation of personal data, the Internet's most powerful corporate actors have become an increasing factor within international relations, attempting to influence how data protection regulation is performed by nation states.

The present thesis will attempt to illuminate how one of the most criticised corporate actors, the social media company Facebook, has attempted to influence international data protection regulation, namely the General Data Protection Regulation (GDPR) in the European Union.

Facebook is a relevant case study because it has evolved with the rise of the Internet from being a small social network connecting American university students in 2004 to becoming the world's largest social media platform with 2.45 Billion monthly users in 2019 (Constine 2019). However, during the same 15 year timeframe, Facebook's handling of personal data has proved to corrode democracy, enabling political players to target and influence certain voters extremely effectively with the use of Facebook's detailed personal data (Hern 2018a). Thus, From a societal perspective, Facebook has indeed lived up to its initial slogan: "Move fast and break things."

Facebook has breached data protection legislation since its founding in 2004 by Cambridge University student Mark Zuckerberg. Already in 2005, researchers found that "Facebook does not take adequate steps to protect user privacy" (Jones & Soltren 2005 p 1). Several breaches surfaced in the following years (McCarthy 2008, Sengupta 2011, King 2013), before Facebook's malpractice finally gained world-wide attention when a whistleblower revealed that the political consulting firm Cambridge Analytica had illegally obtained up to 87 million datasets from Facebook users (Rosenberg 2018). Cambridge Analytica had played a central role in the

campaign of the Republican presidential candidate Donald Trump who surprisingly won the American presidential race in 2016. The firm also ran the succesful "Leave" campaign during the Brexit referendum, which led the United Kingdom to leave the European Union (Hern 2018b). These examples and others (see Stevenson 2018) establish that the use of Facebook's platform on the political stage can disrupt international relations within and beyond the field of European governance.

The Cambridge Analytica Scandal led to a worldwide lack of trust in Facebook and user confidence in the company plunged by 66 percent (Weisbaum 2018). In addition, prominent American politicians and even Facebook's own co-founder call for a break-up of the company due to its growing monopoly of social interaction on the Internet (Lecher 2019, Shelby 2019). Facebook's CEO, Mark Zuckerberg has admitted to some of the company's misdeeds and recently settled with American authorities to pay a record-breaking $5 Billion fine, which critics deem a symbolic "speeding ticket" (Sherr 2019). In addition, Mark Zuckerberg's continued power in the company has attracted wide criticism. For instance by Harvard scholar Shoshana Zuboff who characterised Mark Zuckerberg as:

> *"One man at Facebook who does not enjoy the legitimacy of the vote, democratic oversight, or the demands of shareholder governance exercises control over an increasingly universal means of social connection along with the information concealed in its networks."* (Zuboff 2018, p 156)

In light of Facebook's many breaches of data protection regulation and its widely criticised power in affecting democracy and international relations, it is important to assess which reservations Facebook maintained towards the GDPR which is deemed "the most comprehensive and forward looking piece of legislation to address the challenges facing data protection in the digital age" (Zarsky 2017, p 995). The GDPR marked a major leap in European data protection policy as it regulated data protection by unprecedented measures. It was proposed by the European Commission in 2012 with the objective of implementing a single set of data protection rules across the 28 European member states, replacing the outdated Data Protection Directive of 1995. More than five years of intense negotiations followed and the regulative intentions prompted a counter reaction among corporations. Since 2011, Facebook has increased its European lobby budget nineteen-fold and now ranks in the top among lobby spenders in the EU

(Lobbyfacts 2019). By taking a glance behind the scenes of this secretive tech lobby, this thesis aims to shed a light on Facebook's lobbying of the GDPR by answering the question:

To what extent did the General Data Protection Regulation shift towards Facebook's ideals during the legislative process from 2012 to 2016?

The thesis will investigate Facebook's interests when influencing the GDPR. It will do so by drawing in central theories and methods from the literature of EU interest groups. It will analyse Facebook's "access goods" drawing on Bouwen's (2002) theory of access and draw in Klüver's (2013) theory of aggregated goods, attained by lobbying in coalition.
A study on Facebook's EU lobbying has never been conducted before, thus this thesis will allow the reader hitherto unprecedented insights into Facebook's efforts with regards to influencing the GDPR. The thesis places additional bricks in the puzzle of corporate lobbying of data privacy regulation and corporate lobbbying in general. It does so by conducting interviews with actors central to the legislative process in addition to analysing primary sources used in the lobbying process. In combination, these methods will help assess whether the GDPR shifted towards Facebook's ideals during the legislative process. The research is strictly focused on Facebook and the GDPR, but can help answer the question of whether the general public can trust the technology giants which to a growing extent control public discussions. Thus, the answer to this question is relevant for society as a whole. The conclusion also places itself central to the general question of whether the Internet is still in its initial state of creativity, excitement, and hopefulness. Or whether it, as theorized by Tim Wu (2010), like all other technologies in their time of grandeur has been captured by corporate interests with the connivance of governments.

Methodology

> *"Influence is to the study of decision-making what force is to the study of motion."*
> (March 1955, p 432)

Influence is defined as the ability of an actor to shape a political decision in line with the actor's preferences (Dür 2008). When allowed influence, these actors are important in the process of designing and implementing policies in the European Union. They are a source of societal representation in political decisions and are sometimes even seen as a central indicator of the EU's democratic legitimacy (Greenwood 2007). Thus, in order to understand who is successful in influencing in the European political processes, the study of interest groups is a pivotal phenomenon to observe and explain (Coen & Richardson 2009).

The past 15 years, European scholarship on interest groups has become increasingly based on empirical and systematic research, sophisticated methodological techniques and consistent theoretical approaches. However it remains a niche field of interest among academic sholars (Beyers, 2008). This is most likely due to the fact that although the question of influence is central to the study of interest groups and public policy, the complexity of analysing and operationalising influence is deterring scholars from doing so (Klüver 2013). Measuring influence is challenging because it moves through multiple channels. It can be exercised trough "direct lobbying" (Hansen, 1991) of policy-makers. But also by "outside lobbying" (Kollman, 1998), aimed at influencing public opinion, or by influencing the selection of decision-makers in the EU institutions (Fordham & McKeown 2003). And finally, some groups exert "structural power" (Bernhagen & Bräuninger 2005). Many businesses wield this power when deciding whether or not to invest in areas which are to be affected by certain policies.

It is important to include these facets when drawing conclusions on interest group influence. It is therefore highly necessary to diversify the use of methods and triangulate the findings in order to attain a balanced and trustworthy result. Triangulation is explained by Denzin (1970) as using "multiple observers, theoretical perspectives, sources of data and methodologies" (p 310). According to Dür (2008), the combination of different methods could provide a solution to aspects that cannot be tackled in studies relying on only one method. This research will thus attempt to triangulate the findings by combining two central methods. Firstly *assessing the degree of preference attainment* will be operationalised when analysing original lobby documents

and comparing them to the final outcome of the GDPR. Secondly, the method of *attributed influence* will assess Facebook's influence by way of interviewing central actors in the legislative process. The findings of these methods are analysed combining two theories, namely the approach of Heike Klüver (2013) emphasizing the importance of aggregated goods in coalitions, and the approach of Pieter Bouwen (2002) who coined the term "access goods," focusing on the trading of information in exchange for influence. In combination, these theories and methods serve to establish an argument, which is triangulated and observed from different perspectives. In the following, I will describe in brief the methods used in forming the analysis.

Assessing attributed influence

The method of assessing attributed influence draws on self-evaluation of interest groups or on the assessment of experts. It has several advantages, since it is simple and can be applied to almost all cases. Here, direct questions can be asked regarding the provision of information by lobbyists to politicians and the provision of influence in return. Using this method, it is possible to confirm or deny the transfers of information and influence. As it was done in the case of Pappi & Henning's (1991) network analysis of the organization of influence on the EU's Common Agricultural Policy. Interviewees may for example be asked to "rate to which extent you provided expert knowledge during the legislative process" in order to clarify this transfer of information. *Assessing attributed influence* requires the establishment of an interview setting with central actors in the legislative process who have deep knowledge within it. This could be lobbyists, experts or politicians. In the present study, four interviews with actors central to Facebook's lobbying efforts have been conducted. The interviewees were given the questions beforehand and due to the probability of providing sensitive information, the identities of the interviewees were anonymised.

The interviewees are:

1. A Senior Advisor to the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE)
2. A former chair of a Facebook-supported lobby association.
3. A former high-ranked Facebook representative at the Brussels office.
4. An independent expert of information technology lobbying.

The four interviewees have different characteristics and are therefore split into two groups:

"Lobbyists from Facebook or in association with Facebook" and "Experts embedded in the law making process." As it is common practice for the preparation of interviews, a list of questions were designed for the two groups of interviewees with specific topics to be covered. The questions were designed to help answer the research question, focusing on the supply and demand of information, citizen support and the use of lobby coalitions. Three of the interviews were held in the form of semi-structured interviews. This gives interviewees a certain amount of leeway when replying. It opens to the possibility of asking clarifying questions and the questions do not always have to be asked in the exact way outlined in the interview guide (Bryman 2012). The remaining interviewee, interviewee 4, preferred to submit a self-completion questionnaire. This is a quicker method of interviewing, which has its advantages and disadvantages as it eliminates both interviewer bias and the opportunity to ask clarifying questions (Bryman 2012).

To attain the optimum answers, an effort was made not to ask leading questions or use words that might offend or trigger the interviewee. The questions also attempt to camouflage highly academic glossary, which could damage the interviewee's perception and absorbtion of the question and thereby provide a weak answer. As a main rule, all the questions asked have a similar wording. However, they are designed differently, based on the expertise of the interviewee.

The method of assessing attributed influence has several drawbacks. The most important being that the methodology assesses perceived influence rather than actual influence (Klüver 2013). Evaluation and self-evaluation is a highly subjective assessment which can be problematic. When an expert is asked to give an assessment of a group's influence, the assessment may unconsciously be shaped by specific, prominent cases. At other times, experts may simply explain the findings reported in academic studies using other methods. Doing so, they may simply duplicate the problems of these methods. Interviews may also lead to reificaitions of widely accepted beliefs, resulting in few new findings (Dür 2008). In addition, interviewees might exaggerate their influence in order to signal success to their members. This is most commonly found within interest groups, which are dependent on memberships, like worker's unions or NGOs. Other groups, like Facebook, can afford to remain subtle and understate their influence in order to gain more access or avoid the creation of counterlobbies or a bad public reputation. At the same time, corporations are often very closed organisations negligent to disclose their strategies. Overall, interview situations face pertinent problems like deficient respondent recollec-

tion or interviewer bias. Due to the pitfalls of the methodological approach of *assessing attributed influence*, this method will be used in order to fill the voids of information which the method of *assessing preference attainment* does not cover.

Assessing the degree of preference attainment

The approach of *assessing preference attainment* assesses the degree to which a certain group was successful in attaining its preferences towards a certain law. The method is widely considered the most effective when measuring influence (Klüver 2013). Assessing the degree of preference attainment is operationalised by comparing the final outcome of a legislative process with the policy preferences of an interest group. The analysis concludes that Facebook's overall preference towards influencing the GDPR was to weaken the GDPR's restrictions the collection of private data. When comparing this document to the final GDPR it is possible to assess whether the GDPR was shifted towards Facebook's ideal points. The document analysed is Facebook's submitted recommendations on the opinion of the Internal Market and Consumer Committee (IMCO) in response to the European Commission's draft proposal of the GDPR in 2012. The document is obtained through the platform Lobbyplag.eu, which has gathered and published thousands of lobby documents connected to the GDPR. The analysed document can be found in the appendix. The recommendations are very detailed and reveal the exact passages Facebook wanted changed. The recommendations are also in line with Facebook's general recommendations submitted to the European Commission and therefore highly credible. Comparing successful and unsuccessful recommendations gives a good impression of the success of Facebook when lobbying the European Institutions with regard to GDPR.

The approach of *assesing preference attainment* is effective for many reasons. Most importantly, the method can detect influence even if nothing visible happens, for example because all lobbying is secret or because structural power is at work. It also provides an objective measurement of influence and can be applied to most cases (Dür 2008). However, *assessing the degree of preference attainment* also brings with it several drawbacks. Although it is an advantage that the method can consider all channels of influence, it is at the same time problematic that it does not make it clear through which channels influence is exerted. Furthermore, the method does not account for alternative explanations like coincidences or luck involved in the implementation of preferences in policy output. This means that if the GDPR turns out to reflect Facebook's ideal policy preference, it cannot necessarily be attributed to Facebook's lobbying activities

(Klüver 2013). This method therefore cannot guarantee that a certain interest group was behind a certain change, since other groups could have suggested the same change. For this reason, the main question of this thesis does not attempt to find out how exactly Facebook changed the GDPR, but rather whether, and to what extent, the GDPR changed towards Facebook's ideals. Since the method does assess whether the law was changed in the direction of the ideals of a certain interest group it can help clarify whether Facebook was successful.

Another weak spot of this metod is the difficulty of knowing the salience of Facebook's issues. If a group for example is successful on 20 percent of issues and unsuccessful on 80 percent of issues, a quick analysis would suggest that the group had little influence. However, it could be that the group is successful on the issues which are salient to it and unsuccessful with regards to those that are not salient to it. In that case, a succes rate of 20 percent on one salient issue should be considered quite influential. Keeping salient issues in mind is therefore crucial when measuring influence (Dür 2008).

The Evolution of Privacy Regulation

> *"That the individual shall have full protection in person and in property is a principle as old as common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."* (Warren & Brandeis, 1890, p 193)

When the GDPR was proposed in 2012, it was lobbied extensively by American technology companies like Facebook. To understand why this happened, it is important to understand the clash between European and American values in data privacy. This requires a glance back in the history of privacy regulation.

During the past 130 years, technological advancements have rendered privacy regulation a matter in constant state of flux. The quote above was coined in reaction to the flourishing American news industry with easy access to *"instantaneous photographs"* (Warren & Brandeis, 1890, p 195) and it paved the way for the regulation of non-physical privacy intrusions and thereby personal data (Kramer 1990).

Later, the quick rise of computers opened hitherto unimaginable doors to data processing and data regulation. In 1980, The Organization of Economic Cooperation and Development (OECD) issued eight guidelines focusing on data collection, consent and accountability (OECD Recommendations 1980), but The Council of Europe already then stressed the need for protecting the individual, rather than securing economic development (Kraus 1993).

The breakthrough of the Internet as a commodity in the 90's brought with it a surge in technology enterprises. The collection of personal information in computer databases rapidly accelerated and soon fueled a billion dollar industry devoted to aggregating personal data. Hundreds of companies now gathered personal data in order to create databases for rent to marketers to target potential customers (Solove, 2001). In 1995, this development led the newly rebranded European Union to pass the Data Protection Directive (95/46/EC). The directive set a new direction for the member states, which was much stricter than data privacy in USA. The difference was later explained by Law Professor Joel Reidenberg (2001):

> *"The United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights."* (p 730)

With the Data Protection Directive (95/46/EC), Western Europe took an “omnibus” approach to privacy with one directive covering all situations of data processing, while the USA took a “sectoral” approach, implementing specific privacy laws in specific sectors. This distinction, according to White (1997), was made because the USA dominated the technology business and feared that restrictions on the free flow of information could damage its economy. Thus American companies and lobby organisations have always wielded structural power when it comes to technology lobbying. However, in Europe there was already then a consensus of data privacy being a basic fundamental right. This is shown in the Charter of Fundamental Rights of The European Union (CFR) in 2000 and in the Treaty of the Functioning of The European Union (TFEU) in 2007, establishing that “everyone has the right to the protection of personal data concerning them” (TFEU art. 16, 1). The cooperation between European Member States on finding the right balance between individual privacy rights and the needs of organizations to process personal data opened a political opportunity for the global change in future legislations (Newman 2011). This became apparent on January 25 2012 as the European Commission proposed a replaced of the Data Protection Directive (95/46/EC) called The General Data Protection Regulation (GDPR). After years of intense lobbying, especially from the American technology sector, the GDPR was adopted on April 14th 2016 and put into force on May 25 2018.
The GDPR put in place strict data privacy laws and has been called "the most comprehensive and forward looking piece of legislation to address the challenges facing data protection in the digital age" (Zarsky 2017 p 995). In order to understand the analysis of this thesis, the most important points of the GDPR are explained in the following:

Consent

- The person whose data is processed must give consent to the processing of data for specific purposes. This consent can be withdrawn (GDPR art. 1)

Record-keeping

- Data controllers must be able to prove compliance at any given time (GDPR art. 7)

Data Protection Officer

- Data controllers with more than 250 employees must hire a Data Protection Officer to supervise and ensure compliance with the GDPR and act as an intermedi-

ary between the controller and the member state's Data Protection Authority. (*GDPR* art. 37)

Data Subject Rights

- The GDPR establishes that EU residents have multiple rights, most importantly:
  - The right to access the personal data being processed (GDPR art. 15)
  - The right to rectify inaccurate data (GDPR art. 16)
  - The right to restrict data processing under certain circumstances (GDPR art. 18)
  - The right to object to processing personal data (GDPR art. 21)
  - The right not to be subject to a decision which produces legal effects based solely on automated data processing (GDPR art. 22)
  - The right to erasure also known as the 'right to be forgotten' (GDPR art. 17)
  - The right to transfer one's personal data to another controller. Also called the Right to Data Portability (GDPR art. 20)

Breaches

- Any breaches of data have to be reported to the relevant authorities within 72 hours of the incident (GDPR art. 85).

Fines

- In the case of non-compliance, fines can be issued of up to €20 Million or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (GDPR art. 83).

Initially, the GDPR generated strong reactions among companies who process personal data internationally. It has been reported that the world's 500 biggest corporations spent a total of $7.8B to comply with GDPR (Kahn 2018). However, recently the GDPR has inspired countries like Brazil, Japan, South Korea, India and even the American state of California, which is home to technology companies such as Facebook, to draft similar data privacy regulations (Palmer 2019). Glancing to recent data breaches and public sentiment, scholars believe that compliance with the GDPR could provide a competitive advantage in the future (Voss & Houser 2019). In that case, privacy regulation will have evolved from a very specific move against a sensational-

ist press to a ubiquitous basic right acknowledged and complied with by most of the Western world.

Influencing the European Union

This chapter will dive deeper into the corridors of the European Union where the GDPR was shaped and influenced. It will assess how the different institutions work and how they are lobbied in order to understand how Facebook influenced the GDPR.

The structure of the European Union

The European Union we know today began to take shape in 1949 as the Council of Europe was founded in order to establish a peaceful conversation between the war-torn European nations. Two years later, The Six (Germany, France, Italy, the Netherlands, Belgium and Luxembourg) chose to cooperate within their profitable heavy industries and form the European Coal and Steel Community (ECSC). The idea of being able to move goods freely proved effective and more industries were included, forming the European Communities (EC) in 1967. This also led to several enlargement processes. Today, the EU is constituted by 28 member states. In 1992 the 'Treaty on European Union" (TEU) was signed in Maastricht, renaming the European Communities as the European Union (EU). With the Treaty of Amsterdam in 2001 the European Parliament's institutional power was strengthened. It was given legislative power in more political fields and the power to appoint the President of the Commission. After the Treaty of Lisbon in 2007, the EU took the legislative shape it has today. A bicameral legislature in which the Commission proposes legislation and the European Parliament passes legislation alongside the Council of Ministers was established. The Treaty of Lisbon also made the European Charter of Fundamental Rights legally binding. The Charter asserts among other rights that "Everyone has the right to the protection of personal data concerning him or her" (CFR Art. 8).

The EU distinguishes between five different types of legal acts, namely regulations, directives, decisions, recommendations and opinions. Regulations, directives and decisions are binding while the rest are not.

In the beginning of a legislative procedure, the European Commission has to submit a proposal to the European Parliament and the Council. In the first reading, the European Parliament votes to approve, reject or propose amendments to the Commission's proposal. These amendments

often appear as a result of the lobbying process. The text approved by the Parliament is then forwarded to the Council, which can decide to approve the Parliament's formulation and pass the act with the original wording or formulate its own position. If the Council does not approve the European Parliament's position, the three institutions hold trilogue meetings in which a common position is negotiated. If the institutions agree, the act is passed (Article 294 TFEU 2012).

For every proposal, The Parliament must appoint a MEP as Rapporteur. The Rapporteur is responsible for the Parliament's response to the proposal and is flanked by shadow rapporteurs from the responsible Committee. In the case of GDPR, the responsible committee was the Committee for Civil Liberties, Justice and Home Affairs (LIBE) and the responsible Rapporteur was Jan Albrecht, a MEP from the Green group in the European Parliament.

In the case of the GDPR, The European Commission put forward its proposal in January 2012. In March 2014, the European Parliament voted to support GDPR. After the Subsequent 21 months of negotiations, the Commission, The Council and the Parliament held trilogue meetings and reached agreement in April 2016.

The structure of EU lobbying

Lobbying is anything but a new phenomenon. However, it has only slowly entered the role it currently has in our vocabulary. The Oxford English Dictionary traces the word back to the 1640's. Here "lobbying" was exercised by Londoners standing in the lobby of the House of Commons where they could meet and speak their elected politicians. 200 years later, the word "lobbying" appeared on print for the first time in a local newspaper in 1830s Ohio, referring to an attempt to influence Ohio local politics (Sheidlower 2006).

Since then, lobbying has gained heightened attention in the public. Today, the act of lobbying is synonymous to "persuade" or "urge" and it is exercised by anyone who seeks to influence another person's opinion. However, in politics where lobbying has its roots, the verb has gained a bad reputation. It is often portrayed as a corrupt wrestling match between politicians and corporations. A match in which democracy often comes out as the loser. As a result, some professional lobbyists seek to escape the negative connotations by using different names, like: Lawy-

ers, Public Affairs or Public Relations consultants. And Civil Society groups and NGOs mostly prefer to label their lobbying "advocacy" (Transparency International 2015).
However, lobbying, or interest representation as it is also called, is an important part of the legislative process in the European Union. And it is much more complex than the aforementioned wrestling metaphor. In fact, representation of interests is enshrined in the laws of the European Union. In the Treaty on European Union, which entered into force following the Treaty of Lisbon of 2007, it is established that:

> "*The institutions shall, by appropriate means, give citizens and representative associations the opportunity to make known and publicly exchange their views in all areas of Union action."* (TEU, art 11 (1))

Thus, politicians are required to engage in dialogue with all stakeholders of society, making sure every voice is heard. Among academics there is a wide consensus that lobbying in the European Union is defined as Pieter Bouwen (2002) assesses: "an exchange relation between two groups of interdependent organizations" (p 368). Or as elaborated by Heike Klüver (2013): "an exchange relationship between interest groups and the European institutions in which influence is traded for information supply, citizen support, and economic power" (p 3). But lobbying is conceived in several ways. The interviewees of this paper, for instance, define lobbying as the following:

A: Senior Advisor to the LIBE committee	Lobbying is the attempt to influence policy-making by individuals or organisations that have a self interest. I would distinguish that from public advocacy interest groups if they do it for the public good. Then you can of course lump it together and say that lobbying is everything that tries to impact policy-making and then NGOs are also lobbyists. But I would not say that public institutions are lobbyists.
B: Former chair of a Facebook-supported lobby association	Lobbying is not a bad word, lobbying is an important thing to do because as a politician you need to have the outside world tell you what it's about. As a lobbyist you always have to tell the truth and nothing but the truth, and if you do that, then you have an influ-

	ence. People listen to you.
C: Former high-ranked Facebook representative at Brussels office.	Lobbying for me is explaining why a particular issue is relevant for a particular entity. Either the entity is a company or it is an institution or an organisation. I don't differentiate. Everybody needs to explain why something in particular is relevant or important for this particular entity...I don't have a positive or negative, I just think it's something, which you need in the architecture in the democratic system. You need to have it....You need an understanding of the complexity of the reality.
D: Independent expert in information technology lobbying	Lobbying is the communication of the current interests of businesses or individuals to political decision makers, with a view to having these interests considered or prioritised by decision makers.

The majority of these definitions are based on the notion that it is in the self-interest of the politicians of the EU institutions to maintain close contact with the private sector and civil society. By doing this they fulfil their institutional role and gain deep insights and information on topics on which they are not necessarily experts. On this basis they hope to survive in the political landscape by ultimately becoming reelected (Klüver 2013). Thus, the essence of lobbying is mistaken, if it is only viewed as a wrestling match deciding good and evil.

The amount of lobbyists in Brussels has been on the rise for years. Although the exact number of lobbyists is hard to assess, it is likely around 30.000 (Lobby Planet 2011). All representing the interests of everything from corporate companies, trade unions, NGOs, think tanks, religious groups and public authorities. Thus, lobbying is not only performed by huge corporations, but by a whole range of interest groups seeking to influence political decision.

In the literature of interest group representation in the European Union there is a consensus that as Michalowitz (2004) states: "information is the pre-product of the good of influence" (p 90). As policy makers in the European institutions often face time pressure and evermore complex legislation, the easy access to very specific information provided by external actors can be beneficial for the politician. In order to conceptualise this exchange, Bouwen (2002) introduces

the importance of “Access Goods,” which are traded during the legislative process in order to gain access and influence within the European institutions. All of Bouwen’s "Access Goods" are compiled by specific pieces of information from which the poitician can benefit in order to survive the next election. According to Bouwen (2002) information “is the most important resource to study in order to understand the exchange between business interests and the EU institutions.” (p 369). Klüver (2013) assesses that the probability of influencing a policy proposal steadily increases with a rise in relative information supply by lobby groups. In her study of 56 policy issues of 2696 interest groups, she found that interest groups which supply a high amount of information to the European institutions have a much better chance of influencing policy. Moreover, the effect is particularly strong for highly complex issues where a lot of information is required. Due to the politicians' lack of knowledge and time, highly complex proposals are subject to more information supply which in turn is exchanged for more influence. Klüver measures the complexity of issues by the number of recitals in the proposal, assessing that the average proposal includes around 30 recitals. Highly complex proposals include more than 100 recitals. The GDPR remains in a league of its own with 173 recitals, rendering it extremely complex and thus prone to influence.

EU institutions are often eager to interact with corporate companies because they need knowledge from the private sector in order to fulfil their institutional role. This needs to be recognized, when analysing the strategies of corporate lobbying. Bouwen (2002) therefore coined "The Theory of Access" to make an explicit link between the characteristics of private interest representation and the capacity of this representation to provide "access goods" and thereby gain access to the EU institutions. Bouwen establishes 3 categories of information, which can be traded for influence:

1. ***Expert Knowledge*** **(EK):**
   Providing technical expertise in a complex field.
2. **Information about the *European Encompassing Interest* (EEI*):***
   Providing knowledge on the interests from a specific sector in the European Arena.
3. **Information about the *Domestic Encompassing Interest* (DEI):**
   Providing knowledge about the sectoral needs called for in the domestic arena.

It is clear that information supply for Facebook is an important "access good," since the area of data privacy is highly complex and requires much specialized knowledge, which most politi-

cians do not have. Assessing the information supply is thus a viable path to follow when measuring how much influence Facebook exerted towards the policy makers of the GDPR. It will therefore be a focal point when applying the methods assessing Facebook's overall success. Bouwen (2002) concludes that the different European institutions demand different information at different stages in the legislative process. In order to grasp the complexity of the legislative process in the EU and the lobbying it attracts, it is necessary to understand the most important institutions. The most relevant institutions with regards to influencing the General Data Protection Regulation are the three decision-making institutions, which I will describe in the following:

The European Commission

The European Commission is the EU's executive branch with the exclusive power to draft proposals (Article 17 §2 TEU, 2012). It consists of one independent representative per member state, including a president, who is elected by the European Parliament based on a recommendation from the European Council (not to be mistaken with The Council) and elected by qualified majority (Art. 17 §4, 7 TEU, 2012). Each Commissioner is responsible for one political field, which is assigned by the President. The members of the European Commission should act completely independently and are announced every five years by the member states (Art. 17 §3 TEU, 2012). Each Commissioner manages a Directorate-General. The raison d'etre of the European Commission is stated in the Treaty of European Union (2012):

> *"The Commission works in the general interest of the Union. It oversees the application of Union law, coordinates, executive and management functions, ensures the Union's external representation and seeks to achieve interinstitutional agreements."* (Article 17 §1)

According to some scholars, the European Commission is designed to increase the efficiency of the EU's policy-making because it provides a permanent negotiation forum, which effectively insulates the decision-making process from domestic opponents (Moravcsik 1993). However, in order to be a legitimate broker it must be sure to present policy proposals that successfully pass the legislative process (Klüver 2013).

The administrative staff of the European Commission is much smaller than the administrative staff of many European cities (Bouwen 2009). Having in mind the workload pressure of Com-

missioners and staff, Commissioners are in need of multiple channels of information from expert sources and often listen to major companies of great economic importance for the EU (Klemens 2011). In its role as a promotional broker the European Commission needs information on EEI in order to gauge the complexity of a given European sector of business. In addition, it must secure a great amount of EK when proposing new legislation, whereas it is not interested in information on DEI at the early stage of legislation. Later, however, DEI could be crucial when European Parliament and the Council starts to propose amendments (Bouwen 2002).

The European Parliament

The European Parliament is a core part of the tripartite legislature of the EU, formed together with the Commission and the Council of Ministers. It is the only directly elected institution of the EU and its members are thereby directly accountable to voters (Majone, 1996). Through the years, the European Parliament has gained considerable power and is no longer considered the discussion forum that it once solely was. Now, as a result of its direct election, it is considered a major equilibrium to the EU's perceived democratic deficit and is designed to assure the democratic accountability of the European polity (Rittberger 2003).

The European Parliament is composed of 751 members (MEPs), including a President elected by the members for two and a half years with the option of re-election (Article 14 §2, 4, TEU, 2012). Every five years, MEPs are directly elected by EU citizens in the member states (Article 14 §3 TEU, 2012).

The European Parliament has legislative power but no legislative initiative, since this is the prerogative of the European Commission. The European Parliament does, however, have the right to request the European Commission to draft legislative proposals (Art. 225, TFEU, 2012). The European Parliament also has the power to confirm new Commissions and to approve or reject Commission proposals, or propose amendments. It can also force the Commission to resign (Article 234 TFEU, 2012). After the 2019 elections, the European Parliament is composed of eight political groups and 30 non-attached MEPs. In order to satisfy the demands of voters and to maintain their seat in the Parliament, MEPs are in need of citizen support, policy-relevant information, and the support of economically powerful actors (Klüver 2013). The degree of succesful influence therefore depends on the ability of interest groups to to supply these goods to MEPs.

In the European Parliament, there is a limited demand for EK, since the gathering of expert knowledge has been done in the Commission, leading up to the proposal. However, EEI and DEI on voter needs are often crucial for the European Parliament. In order to secure the following of members in specific sectors and get reelected, MEPs need to listen to private and national interests (Bouwen 2002).

The Council of the European Union

The Council of the European Union, also known as The Council or The Council of Ministers, is an essential EU decision maker. No legislative act can enter into force without the approval of the Council. This ultimately allows member states to check the legislative activities of the EU. Thus, the Council is also a target for lobbying.

The Council is composed of one representative from each member state at ministerial level who is authorized to vote on behalf of its government. Thus, the composition of the Council is configured according to which theme is discussed. There are 10 different configurations of the Council, ranging from Agriculture and Fisheries to Justice and Home Affairs (See Council configurations).

Meetings in the Council are chaired by the representative member of the country holding the Council presidency at the time. The presidency rotates every six months. Despite its intergovernmental traits, The Council's Secretariat and its Presidency embody a sense of collective purpose and commitment and thereby give this intergovernmental institution a supranational twist (Hayes-Renshaw 2006). Contrary to the European Parliament, the Council can act on issues related to foreign affairs and security policy. It may also request the Commission to draft a legislative proposal (Article 241 TFEU, 2012). The Council is assisted by the Committee of Permanent Representatives (COREPER) and more than 150 working parties and committees. They help prepare the work for the ministers who examine proposals in the different Council configurations. The Council and the European Parliament examine commission proposals simultaneously. This examination is known as a "reading". There can be up to three readings before the Council and the Parliament agree on or reject a legislative proposal. The Council is not legally obliged to take account of Parliament's opinion but it cannot take a decision without having received the Parliament's opinion. The Council's final position cannot be adopted until the Parliament has delivered its own first reading opinion.

Due to its extensive legislative responsibilities, the Council is always a lobbying target for interest groups (Hayes-Renshaw 2009). But particularly for domestic interest groups, who lobby their national governments in an effort to influence European policy-making through the Council (Eising 2004). In the Council, mainly national interest are at stake. And as a result, DEI is in high demand. At the same time, however, a considerable amount of EEI is needed because of the Council's aforementioned supranationalist traits. At this point in the legislative process, the need for EK is substantially reduced as the Council is more interested in information that can facilitate the bargaining process among member states (Bouwen 2002).

In addition, Klüver (2013) argues, that it is not sufficient only to look at the supply of information by individual interest groups. It is also necessary to include coalitions into the equation. Klüver assesses that lobbying is a collective process in which more interest groups simultaneously lobby decision makers. As a result, it is not the "access goods" of the individual interest groups that make the difference. It is the aggregated amount of "access goods" that matter.
It is thus important to keep in mind the benefit of the cooperation between businesses on which Coen (1997) elaborates, stating that when an issue does not cause a split among business interests, a group of corporates could be able to lobby efficiently. The same was concluded by Egdell and Thomson (1991), assessing that a "a coordinated or concerted approach is becoming increasingly necessary in promoting or affecting EU-wide regulations and directives" (p 128).
When it comes to coalitions, Klüver (2013) argues that there are more "access goods" to take into consideration than just information. She assesses that citizen support and economic power also play a major role in the process of influencing politicians. Citizen support is needed in order for the European institutions to gain electoral support. It enhances the legitimacy of European policy initiatives and decreases the risk of blame from the public. Worker's unions or NGOs can often provide citizen support because they are based on thousands of paying members. Corporations like Facebook often do not wield citizen support.
Contrarily, Facebook wields economic power. Not in the sense that it can bribe its way to succes, but rather because of its ability to invest in the European work force. Politicians generally aim at adopting policy proposals that are supported by a majority of their voters to secure their reelection. This means that they are more responsive to concerns raised by interest groups that control an important economic sector than to interest groups that do not have an impact on

business investment or employment. This power is indeed wielded by Facebook and its American counterparts.

Analysing Facebook's influence

> *"If the whole lobbying, not just from Facebook, but from all the industries, hadn't been there, then of course the final text could have been much stronger, that's clear. But I don't see a specific impact of Facebook anywhere."* (Interviewee A, line 202)

Measured on the amount of recitals (173) the GDPR is one of the most complex laws to be adopted in the European Union. Thus, theoretically, as we have learned from Klüver (2013), it was especially prone to be influenced by interest groups like Facebook. The following analysis will attempt to assess to which extent the GDPR was shifted towards Facebook's ideals, using the methods of *assessing attributed influence* and *preference attainment*. The analysis will also prove that Facebook did have a specific impact.

Assessing attributed influence

Multiple times during the legislative process, it was evident that the general effort to influence the GDPR was remarkable. An interviewee asserts that 95-98 percent of lobbying was put in place to weaken the level of protection of the GDPR (Interviewee A, line 38). In addition, then-Commissioner of Justice, Viviane Reding, asserted that the lobbying was "fierce" and unprecedented (Warman 2012). Later, as the European Parliament took GDPR through the next step of the legislative process, the Green Rapporteur of the GDPR, former IT lawyer Jan Philipp Albrecht, and the team of Shadow Rapporteurs received a whopping 3.999 proposals for amendments. The crowdsourced data platform Lobbyplag.eu later revealed that several MEPs had submitted amendments which were exact copies of industry recommendations (Corporate Europe 2013). In another thought-provoking case it was revealed that 229 amendments deemed mainly industry friendly had been submitted by the assistant of the Belgian MEP Louis Michel. Allegedly, without the approval of the MEP (Nielsen 2013).

Taking the fierce lobbying effort into consideration, it is interesting to take account of Facebook's own perception of itself as a lobbying entity with regards to GDPR:

> *"I don't even remember if my colleagues really tried to influence it (GDPR) in the traditional lobbying sense of understanding influencing. Which is really that you*

> *want to see this particular law change or this particular paragraph or aspect changed."* (Interviewee C, line 204)

Thus, even years after the GDPR was put into force, Facebook seems to play down the fact that it attempted to influence the GDPR. And avoid commenting on whether it succeeded. It is clear, however, that influence was attempted, both in face-to-face meetings and by submitting recommendations for amendments. As an interviewee puts it:

> "*Facebook wanted the weakest GDPR possible, ideally a very long and complex Regulation that ultimately had no teeth, but which, due to its complexity, gave it a relative advantage over other businesses operating in its multiple fields of interest."* (Interviewee D, line 26)

On 12 March 2014, the amended GDPR was adopted by the European Parliament with a great majority of 621 votes in favor, 10 against and 22 abstentions. More than one year - and plenty of lobbying - later, on June 8th 2015, the Council agreed on a general approach to the GDPR. The Council's proposal turned out to be much more industry friendly than in the European Parliament. It was criticised loudly because it would "override the rights of citizens in favor of large companies that make a lucrative market of personal data" (La Quadrature Du Net 2015). As it is stated by Bouwen (2002), member state representatives in the Council have a high demand for DEI and less demand for EEI. Thus, Council members were therefore most likely influenced by national interest groups who agitated for the well-being of local businesses. One interviewee even stated that national business associations "were up in arms" (Interviewee B line 120) attempting to influence national politicians. Due to the mainly national supply and demand of information, it is thus unlikely that Facebook as a relatively small individual lobbying entity was particularly involved in influencing the Council members in the European capitals.

After 10 trilogue meetings in the last half of 2015, the GDPR was finally adopted by the Council and the Parliament in April 2016 (EUGDPR.org). An expert interviewee describes the final outcome of the GDPR as "weakened" (Interviewee D line 23) compared to the Commission's initial proposal. However, interviewee A, who was very central in the legislative process found satisfaction in the chain of events that unfolded during the negotiation of the GDPR. Namely because of the cooperation, competence and specialised knowledge of central law makers. But also be-

cause of the Snowden revelations in 2013, linking Facebook to mass surveillance in cooperation with the US government and the privacy activist Max Schrems' court case against Facebook in the run-up to the trilogues. The interviewee believes that these events in combination led to heightened awareness on the benefits of data protection and thus less successful industry friendly lobbying:

> *"When we had the final trilogue on the final text, the Council presidency, just by coincidence, was Luxembourg and Luxembourg's government was in coalition with the green party. And the green party was also part of the government, so the responsible Minister for Justice was from the green party. And I'm not sure if that has ever happened before. (...) this whole GDPR has so many things that rarely happens: To have a green Rapporteur who is really an expert in the field, to have a green counterpart in the Council at the trilogue negotiations, to have a very committed Commissioner for Justice, to have Max Schrems helping us, and to have Snowden in between. All of these things are very rare and random in themselves. And the combination of them almost made me believe in God again, you know. This cannot just be a coincident."* (Interviewee A, line 78-94)

Despite the Council's stance on the GDPR, central lawmakers in the European Parliament seem to feel satisfied with the final outcome of the GDPR. Mostly due to luck. An interviewee seems secure in the belief that: "I don't see a specific impact of Facebook anywhere" (Interviewee A line 203). Law makers, however, have an interest in shedding a positive light on legislation in which they were centrally involved. However, even experts (Interviewee D line 58) and Facebook itself (Interviewee C line 204) seem to be at loss with regards to the question of whether Facebook was successful influencing the GDPR. Thus, there seems to be a gap of knowledge which this thesis can fill.

Facebook in coalition

"It is hard to work out who had what influence," (Interviewee D, line 59) states an interviewee rightly. Especially when lobbying is carried out in coalitions. Already early in the legislative process, it was clear that GDPR was not only lobbied by the usual NGOs, corporations and various assocations. Also entire countries were involved, namely the United States which attempted to protect the interest of US companies operating in the EU (Guarascio 2012). The United States was particularly active even before the European Commission presented the draft legislation. This early lobbying resulted in a watering down of the Commission's draft legislation,

for instance allowing the processing of data of children as young as 13, instead of 18 in the original draft and decreasing the maximum fine for a corporations to 2% of annual worldwide turnover, instead of the original 5% (Schildberger 2015).

Lobbying by countries is one example of lobbying taking place in coalitions where industries band together to influence law proposals towards its common ideals. Facebook used this strategy in an attempt to subtly amplify its ideals, since Facebook "knew that if they appeared too aggressively in the lobbying, it would backfire" (Interviewee A, line 102).

It is hard to get an exact overview of how many associations were backed by Facebook. However, research shows that Facebook did not participate in major associations like Techamerica Europe or DigitalEurope (EDRi 2013). It is also striking that while Google and Microsoft in the beginning of the legislative process were involved in up to 35 coalitions and assocations, Facebook, until 2015, was only engaged in two of these, according to official records. Until 2015, Facebook was a member of the powerful American Chamber of Commerce EU and the European Internet Foundation (Lobbyfacts 2018) and backed an unknown amount of associations and think tanks. But as an interviewee of a Facebook-backed association alludes to, it remains a question whether these associations actually represented Facebook's ideals and aligned with Facebook's interests when lobbying.

> *"I was not blind, I mean, they (Facebook) supported us in the beginning because then they could get a better face as I started to say. But then as an association you have to be so strict that you don't allow them to have influence. We also influenced them, it's not only them influencing us." (Interviewee B, line 139)*

Industry-backed associations of course have several reasons to understate influence from its backers. Avoiding a bad reputation is one of them. However, if this interviewee is trustworthy, it raises questions whether Facebook was in general able to leverage its lobbying effort in coalition with others. This, in combination with Facebook working outside of some of the main industry coalitions most likely damaged its overall success in shifting the GDPR towards its own ideals. As Klüver (2013) argues, "it is the aggregated amount of goods provided by entire issue-specific lobbying coalitions that matters" (p 3) and Facebook's work in this regard provides little evidence of success.

Facebook's information supply

As has earlier been established by Bouwen (2002), information supply is the biggest asset of a lobbyist when attempting to shift legislation towards its ideals. The more useful information supplied, the more influence the lobbyist is given. This theory is confirmed by an interviewee who states that the lobby of the pharmaceutical companies was successful, because it managed to provide trustworthy information from established academics and research foundations, which led "to the fact that we now have a privilege for further processing for research purposes that wasn't there before" (Interviewee A, line 163). Facebook, however, is ambiguous when self-assessing whether it detected an actual demand for its information among politicians. On the one hand Facebook believed politicians "sometimes had a limited understanding about how Facebook works" (Interviewee C, line 173). On the other hand, a former Facebook lobbyist believes that "there was never a single doubt that we dealt with politicians at the time who understood the issue" (Interviewee C, line 75). The competence within the realm of privacy and data, attained by central lawmakers like Rapporteur Jan Philipp Albrecht most likely put Facebook in a situation where it was difficult to exchange information and receive influence in return.

So how and where was Facebook's information supply applied? One of Facebook's main arguments was that the GDPR would challenge innovation among small and medium enterpises (SMEs) and thus the European economy would be weakened. Using this strategy Facebook attempted to situate itself as a European SME when calling for weakening changes in the GDPR. This strategy, however, "did not work at all," said one interviewee (Interviewee D, line 53). Mainly because Facebook by many politicians was considered a global giant, not an SME. This most likely boosted the lack of trustworthiness, thereby weakening Facebook's ability to supply quality information about the state of the technology sector in Europe, which in Bouwen's (2002) terms would be categorised as EEA. Another interviewee confirms this by characterising the information supply provided in the following way:

> *"They just tried to request meetings and talk to people and be nice and make us understand their concerns and that they already had many regulations to take into account and more would hinder innovation and that usual la-la that you hear all the time."* (Interviewee A, line 151)

The quote brings forward the notion that Facebook in many cases did not manage to contribute with sufficient new and trustworthy information to gain influence among MEPs. Here, the high quality knowledge, already obtained by some MEPs was crucial. In addition this knowledge was spread to other less specialised MEPs in order to counter Facebook's information supply. One interviewee simply educated other MEPs about the benefits of data protection in long meetings early in the process (Interviewee A, line 182). This effort most probably further weakened Facebook's ability to supply information, in this case EK. Based on these impressions it is evident that Facebook's information supply cannot be described as especially effective in shifting politicians' opinion towards Facebook's ideal of the GDPR. As a result "Facebook became less and less visible as the process moved forward" (Interviewee D, line 31).

Facebook's economic power

As mentioned previously, the European institutions demand economic power from interest groups, meaning that they are more responsive to concerns raised by interest groups that control an important economic sector than to interest groups that do not have an impact on employment or investment in a given economic sector (Klüver 2013). In 2012 when the GDPR was proposed, Facebook was a relatively small technology giant. As it went public in May 2012, its stock market cap amounted to $72 Billion. Compared to Facebook's competitors such as Google ($400B) or Microsoft ($250B), Facebook's economic power was dwarfed (Macrotrends 2019). But over the course of the next seven years Facebook grew. Today, Facebook is valued around $550 Billion. In addition, Facebook has raised its European lobby budget from $200.000 in 2011 to around $3,75 Million in 2018 (Lobbyfacts 2018a). That amounts to a nineteen-fold increase, ranking Facebook 5th among lobby spenders in Brussels (Lobbyfacts 2018b). In comparison, the top spender, Google, has increased its budget eleven-fold in the same time span (Lobbyfacts 2018d). Microsoft comes in second with a much more stable budget through the years (Lobbyfacts 2018d).

It is striking that Facebook's lobby spending started increasing rapidly after 2011 when the hearing process of the GDPR was launched. It adds to the interpretation that Facebook, like many other companies had a big stake in European data protection regulation and was eager to use its economic power to influence it. As Facebook grew in size, it played a more important part in the lobbying process due to its economic investment in the European work force.

Facebook's citizen support

In order to advance their objectives and ultimately become re-elected, the politicians within the European Commission, the Council, and the European Parliament not only need information and economic power, they also require citizen support. Citizen support is needed in order for the European institutions to gain electoral support. It also enhances the legitimacy of European policy initiatives and decreases the risk of blame from the public. Politicians thus aim at adopting policy proposals that are supported by a majority of their voters to secure their re-election (Klüver 2013).

To most Europeans, Facebook was not considered a danger in 2012. But as the Snowden leaks started to appear in the news, linking technology giants, including Facebook, to the illegal access to private information via the US-sponsored PRISM-program, criticism started to mount on the technology companies (Johnson 2013). Later, the data activist Max Schrems took Facebook to court. The unlawful practices unveiled in this process resulted in an invalidaton of the The Safe Harbour Agreement, which was a set of principles that governed the exchange of personal data between the United States of America and the European Union (Scott 2015). With the declining trust in Facebook, the amount of citizen support Facebook would be able to supply was weakened and it was used as a method to counter the lobbying, says an interviewee:

> *"It was our hope to counter the lobby pressure by public attention so our colleagues from the other political groups would not fully end up in line with the lobbyists, but also feel responsible towards the citizens."* (Interviewee A, line 51)

With these facts in mind, it can be concluded that Facebook had little citizen support in Europe during the legislative process 2012-2016. In fact citizen support kept dwindling as the Cambridge Analytica Scandal was made public only. Today, Facebook is considered the least trustworthy brand among technology giants (Stephenson 2019).

Important findings have been unearthed using the *method of attributed influence*. Among these are Facebook's lax efforts of supplying information, Facebook's limited work in coalitions, Facebook's exercise of economic and structural power because of its increasing wealth and investment in the European technology sector, and finally its lack of citizen support. However, the trustworthiness of this study requires the application of a second methodological approach: *The assesment of preference attainment.*

Assessing the degree of preference attainment

In the following, an analysis of Facebook's degree of *preference attainment* will be performed, using Facebook's document with recommendations to the Internal Market & Cooperation Committee (IMCO). The document was published in 2012 and spans 51 pages. It was thus part of the extensive process of reviewing the European Commission's proposal in the European Parliament. In the following I create an overview of the specific themes on which Facebook attempted to gain influence. Facebook's ideals are then compared to the final outcome of the GDPR. It is then possible to assess to which extent the GDPR shifted towards Facebook's ideals during the legislative process.

The Consistency Mechanism

The GDPR introduced a mechanism that provides consistency of interpretation throughout the EU. This mechanism means that although an organisation is processing data across borders, it will only deal with the supervisory authority of the EU country in which its main EU quarters is situated (Elshof & Van Es 2018).

Facebook's structural power is apparent as it describes the consistent mechanism as "sensible and positive" (Facebook p. 1) because it creates incentives for international organisations to establish in Europe. However, Facebook seems to be concerned about how the law applies to group companies, like itself. Facebook's EU department is situated in Dublin, Ireland, while its headquarters is situated in Menlo Park, California. Until 2018, Facebook's department in Dublin processed the data of all Facebook accounts outside the US and Canada. Therefore, the GDPR could potentially have a great impact on the processing of billions of users. After the GDPR came into force, Facebook resorted to moving 1,5 billion accounts from outside US, Canada and EU from its servers in Ireland to its servers in the US “because EU law requires specific language” (Hern, 2018c) which US law does not. In other words, the GDPR was integral to the moving of billions of accounts. In a Facebook employee's own words: "a major change" (Interviewee C, line 160).

When analysing Facebook's recommendations on this mechanism, it is clear, that Facebook was succesful in implementing 13 out of 32 recommendations. A rate of succes of 40.6 percent. In the following, the most prominent attempts of influence are anlalysed, thereby *assessing preference attainment:*

Successful influence	Failed influence
- **Recital 36, Art. 4:** Facebook wished that processors should not be subject to the same administrative obligations and regulatory scrutiny as controllers. This recital was changed in this direction. - **Recital 135, Art. 61, Art. 64:** The circumstances in which national data protection authorities, the Commission, and the European Data Protection Board can cooperate was succesfully limited. - **Art. 63a:** The IMCO proposal stating that the European Commission should have power to overrule the Data Protection Authorities is deleted. - **Art. 63, Recital 141:** The article which allows The European Data Protection Board to adopt binding opinions and force supervisory authorities to abide is deleted. - **Art. 80:** The word "citizen" is replaced with "data subjects."	- **Art. 3:** Facebook was unsuccessful in exempting the GDPR from applying to "monitoring of behaviour" (Facebook p 6). - **Art. 61:** Facebook unsuccessfully attempted to influence the time limits within which a supervisory authority should act. It also unsuccessfully allowed supervisory authorities to avoid cooperation if it involves "disproportionate effort" (Facebook p 10) - **Art. 64:** Facebook unsuccessfully intended to get rid of time limits for supervisory authorities to act and limit the cooperation between European Data Protection Board and supervisory authorities.

Based on the findings in Article 63 it is clear that the European Commission was obstructed from the right to overrule the decisions of national data protection authorities. The European Data Protection Board's powers were also significantly weakened. Facebook also aimed to limit the cooperation between the European Commission, the European Data Protection Board and national data protection authorities. That effort also seems succesful.

In the succesful process of replacing "citizens" with "data subjects," also becomes apparent that Facebook is concerned about the financial implications of citizens using "class action to litigate

against corporate groups" (Facebook p. 19). Here, it seems Facebook has learned from 2009 when a class action forced Facebook to pay a settlement of $9.5 Million (McCarthy 2009). In spite of a rate of succes of 40.6 percent, Facebook did not influence the proposal when it came to monitoring data subjects' behaviour or limit the European Data Protection to act in the case of "disproportionate effort." It is thus possible to conclude that Facebook's most salient issue were not affected.

Consent

The GDPR's formulation of consent was a major focus point for Facebook during in the lobbying process. As it appears in the final outcome of the law, consent is one of six ways to gain legal access to process personal data (Art 6 GDPR). It is given by a "clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement" (Recital 32 GDPR).

The analysis of Facebook's recommendations reveals that Facebook believed that the GDPR's requirements for consent were "over-prescriptive and often meaningless" (Facebook p 20). Facebook believed explicit consent would inundate users with tick boxes and "result in an overly disrupted or disjointed internet experience" (Facebook p 20).

In spite of Facebook's clear focus on this subject, the analysis of the document shows Facebook to be moderately successful in this area. Only 4 out of 18 recommendations (22.2 percent) can be traced in the final outcome of the GDPR. The following table lists the most prominent points.

Successful influence	**Failed influence**
- **Recital 32 and art. 4:** The word "explicitly" in the definition of consent is deleted. The word "explicit" is replaced with "unambiguous" (Facebook p 24). - **Art. 17:** The focus on a person's right to be forgotten if the data was made available when the person was a child is removed. - **Art. 17:** The paragraph which gives the Euro-	- **Recital 32:** Facebook unsuccesfully attempts to delete that "Silence or inactivity should therefore not constitute consent." - **Recital 42:** Facebook unsuccesfully attempts to add that consent should be a condition of access to a free service. - **Art. 7:** Facebook unsuccessfully adds numerous changes which would allow for

pean Commission the right to adopt acts that specify certain conditions and criteria for consent is deleted.	obtaining consent for a range of data processing activity in a single step. - **Recital 65:** Facebook is unsuccessful in deleting the particular focus on childrens' and former children's rights to have their data erased. - **Recital 65 and 66:** Facebook is unsuccesful in deleting texts that require data to be deleted but involves great effort and work. Facebook believes it is "technically impossible" and that it "directly conflicts with the way the internet works" (Facebook p 30). This is done in an effort to fend off the effort it would be to erase data made public by third parties.

In conclusion, it is apparent that while Facebook's ideals regarding consent are only incorporated in 22.2 percent of cases, Facebook has a serious impact on the definition of consent. Undoubtedly, replacing "explicit" with "unambiguous" makes room for more creative interpretations. One might also wonder why Facebook attempted to delete the explicit focus on a person's right to be erased if the data was collected during childhood. As a result, the GDPR, instead seems to be firmer in the focus on children's rights while they are under 16 (GDPR Art. 8). On numerous issues, however, Facebook is unsuccessful. For instance when making it easy and convenient to obtain consent. Facebook is thus moderately succesful in influencing this very salient issue.

Profiling

Profiling is defined to be any form of automated processing of personal data used to analyse or predict aspects concerning a person (GDPR Art. 4 (4)). It is therefore in many ways the holy grail to a platform like Facebook, which business model it is to analyse user behaviour in order to effectively target users with advertisement. It can thus be assumed that it was quite essential for Facebook to avoid significant limitations on profiling, and Facebook's argument exerted

structural power when arguing that the GDPR could lead to "consequences to the detriment of consumers and businesses and society as a whole" (Facebook p 36). Facebook argues that the GDPR "fails to strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce" (Facebook p 37). Another argument was that profiling techniques are so widely used that it does not make sense to limit it. According to one interviewee, Facebook argued that "was in the individuals' own interests" (Interviewee D, line 48). Out of Facebook's four proposed changes none made it into the final outcome of the GDPR. The table below gives an overview on the most prominents attempts of influence:

Successful influence	**Failed influence**
	- **Recital 63:** Facebook unsuccesfully deletes that any person should have the right to obtain data collected concerning them. - **Recital 71 and art. 22:** Facebook unsuccesfully deletes that any person should have the right not to be subject to profiling.

In the final outcome of the GDPR, it is stated that a data subject has the right not to be subject to profiling (Art. 22 GDPR). Thus, even though profiling was a core issue for Facebook, the Facebook lobbyists failed to influence articles or recitals about profiling.

In conclusion, Facebook's impact on the GDPR's restrictive measures on profiling is minimal, if not non-existing. The Right To Be Forgotten and the Right To Access remain key points in the GDPR. However, according to a Facebook interviewee, restrictions on profiling were never an issue and was not detrimental to its business model, which continued on the grounds that Facebook's advertising was not based on profiling or behavoiural advertisement (Interviewee C, line 130). The question is then, if it was never going to be an issue, why did Facebook lobby against it?

Controller and Processor

The GDPR defines a 'controller' as "the body that determines the purposes and means of the processing of personal data" (GDPR Art. 3 (7)). A 'processor' is defined as the body "which processes personal data on behalf of the controller" (GDPR Art. 3 (8)). In short, Facebook as a company is both processor and controller, assuming that its data processing is not outsourced to third parties. However, Facebook believed the two concepts could raise practical difficulties when a data controller and a data processor are part of the same company group. Under the Data Protection Directive, only data controllers were held accountable for anything that went wrong. But under the GDPR both data controllers and processors will be jointly responsible for compliance (Beaumont 2018). Facebook is against this and therefore suggests the responsibilities remain the same as in the 1995 Data Protection Directive. The analysis of the document shows that Facebook managed to shift the GDPR towards its ideal points in 10 out of 25 (40%) cases. The most prominent are listed below:

Successful influence	**Failed influence**
- **Recital 79, Art. 4, Art. 26:** The word "conditions" is deleted in numerous articles. - **Art. 28:** The part of the article which demands a processor to hand over data even when it is restricted from processing is deleted. - **Art. 15:** The part of the article which demands the provision of the time codes of collection of data is deleted.	- **Art. 4:** Facebook unsuccessfully attempts to clarify that a processor is the entity making decisions with regards to the processing. - **Art 24:** Facebook unsuccesfully adds that the controller should only take "reasonable" and "proportional" responsibility.

In conclusion, Facebook was able to influence the GDPR's focus on the processor and controller by deleting small passages here and there. It resulted in the slight watering down of some articles and recitals. However, Facebook did not succeed in its overall objective, namely reintroducing the Data Protection Directive's measures. One of the key changes to the GDPR remains in the fact that it applies to the processing of personal data by both controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. Therefore, Facebook's attempt to influence the GDPR's focus on processor and controller can be concluded as partly failed.

Overall, this analysis has shown that Facebook was successful in its attempt to influence the GDPR in 27 out of 79 cases. A success rate of 29.2 percent. For example, Facebook's ideals were met when the company attempted to:

1. Obstruct the European Commission and the European Data Protection Board from obtaining certain powers.
2. Limit the circumstances in which national data protection authorities, the Commission, and the European Data Protection Board can cooperate.
3. Replace "citizens" with "data subjects."
4. Replace "explicit" with "unambiguous" in the definiton of consent.
5. Minimize the focus on a person's right to be erased if the data was collected when it was a child.

These successful attempts of influence are put into perspective by the list of unsuccessful attempts of influence. Most importantly the attempts to:

1. Avoid regulation of "monitoring of behaviour."
2. Allow for obtaining consent for a range of data processing activity in a single step.
3. Delete that "Silence or inactivity should not constitute consent."
4. Delete the focus on childrens' rights to have their data erased
5. Delete the Right to Access
6. Delete the Right to be Forgotten
7. Exempt data controllers from being affected by GDPR measures

The two methods applied to analyse Facebook's influence towards the GDPR shows the multi-facetted nature of analysing influence. On the one hand, the attributed effects of Facebook's information supply, coalition work, economic power and citizen support gives the impression that Facebook was in an inferior position to influence the GDPR. On the other hand, it becomes apparent that 29.2 percent of Facebook's preferences were attained in the final outcome of the GDPR. This suggests that Facebook or other organisations with similar aims did have an influence on the final outcome. The character of that effect is discussed in the following chapter.

Discussing the measure of influence

> *"I think Facebook changed as well over the last years (...) I think there's an understanding now that sometimes legislations are more helpful, you know, instead of avoiding legislation."* (Interviewee C, line 79)

In 2010, Tim Wu argued that every technology since the telegraph has been captured by corporate interests with the help from governments. Back then, evidence was not there to uphold the claim that the Internet would end up the same way, but can Facebook's influence on the GDPR help us give an answer?

Although this case study in itself is not generalizable it can help us provide an answer to Wu's broad concept of the development of technologies from free and beneficial to limiting and damaging. The influence Facebook is allowed to have in the political sphere might help us understand whether the Internet can now be included on Wu's list of technologies held in corporate captivity with the assistance of governments.

The results found in the analysis of this research, using the *preference attainment method*, show that 29.2 percent of Facebook's proposed recommendations were successfully implemented in the final outcome of the GDPR. *The preference attainment approach* covers all channels of influence and is widely regarded as the most accurate approach when measuring influence. Rating the character of this influence largely depends on the observer and where one sets personal thresholds for corporate influence. However, objectively a 29.2 percent rate of success can be categorised as modest.

The other part of the analysis, operationalised by the *method of attributed influence*, shows that Facebook's ability to supply information to main politicians in the European Parliament and the Council was weakened. This happened due to a high level of knowledge among politicians, by coincidence of political alliances, by effective counterlobbying, by an ever weaker citizen support and finally by poor work in coalitions. Using, Bouwen's terms, the supply of EK, EEI and DEI from Facebook was not highly valued if even recognized. Especially not when engaging with politicians in the European Parliament. Due to the well-informed politicians in an otherwise highly EK-demanding European Parliament, there was an effort to dampen significant information supply by Facebook. At the same time, due to the low demand of EEA in the Council and some coincidental luck of political cooperation across institutions, Facebook's influence can not be attributed to the Council.

If this research had only *asssesed the attributed influence*, Facebook would have had no influence whatsoever. That assumption is however based on weak scientific evidence. In the process of interviewing central actors, one must realize that most actors in the sphere of influence have an interest in communicating a certain agenda. Thus, it is difficult, no matter how many interviews are carried out, to identify an exact amount of influence traded between interest group and politician.

The weaknesses of the research kept in mind, we are left with the question of how to reconcile the results of the present attempt of methodological triangulation. Dür (2008) argues that method shopping should be applied when measuring the influence of interest groups in the EU, but also addresses the well-known issue of what a researcher should do if different methods show different results. He suggests that conflicting results when method shopping is one of the drawbacks when applying more methods to a case. Thus, this seems to be simply a condition that researchers have to endure when using the currently developed methods within the science of interest group representation. Dür, however, also assesses that despite these drawbacks, method shopping is likely to lead to more reliable results than the alternative. Thus, an attempt should be done to qualify the somewhat conflicting results towards a coherent conclusion. Here, it is pivotal to assess the salience of Facebook's issues. Since 29,2 percent of issues were succesfully included in the GDPR, were these then Facebook's most salient issues or just minor details? A rate of success of 29.2 percent equals a rate of unsuccessfulness of 70.8. A simple analysis would then suggest that Facebook had modest influence. Unless the successful issues were the most salient ones. If that is the case, even if Facebook was successful in only 29.2 percent issues, it can be considered quite influential (Dür 2008).

In the case of Facebook, the most salient issue was consent (Interviewee C, line 131). Here, it is evident that Facebook was less successful than overall with a 22.2 percent rate of success. But considering that the the very definition of consent in mutiple recitals and articles was altered towards Facebook's ideal, the influence on this issue must be considered significant. To a certain degree, profiling was also a salient issue, since Facebook's business model is based on processing personal data for targeting ads. Here, however, Facebook completely failed to influence the GDPR. Another salient issue was reintroducing the measures of the Data Protection Directive (95/46/EC) with regards to processor an controller. But yet again, Facebook did not manage to influence this issue. Facebook's influence on these salient issues gives us a better idea of Facebook's success. However, it is still a mixed picture. A 22 percent rate of success on a

salient issue can be considered significantly influential, but a 0 percent rate of success with regards to profiling and reintroducing favourable measures can not be characterised as influential at all.

Analysing influence is often thought of as a question of exact knowledge. The reality is, however, that it rarely is. This study was executed in order to better understand whether the most comprehensive data protection legislation in the world was shifted towards the ideals of the world's largest and most controversial social media company in the world. It is a case study and therefore not generalizable to all companies in this field. For further research, a more generalizable study should be attempted. This would enable researchers to assess how actors compare when influencing EU regulation. A broader, more quantitative approach would enable researches to rank Facebook's success in comparison to other actors, thus enabling researchers to point out who were the winners and losers in the effort to influence the GPDR.

Facebook implemented the GDPR "in spirit" when the GDPR came into effect (Hern 2018c). But after the Cambridge Analytica scandal, Mark Zuckerberg has proclaimed that "the future is private," (Statt 2019) and that "we need a more active role for governments and regulators" (Press Association 2019). This is most likely done in recognition of the increased mistrust towards Facebook's previous policies. Whether it is purely branding is hard to say, since Facebook is still very secretive in its communication with governments. However, it is a sign that the increased focus on data privacy among the public has made companies as well as politicians and their voters more aware of the perils of gathering private data. With multiple GDPR-like regulations waiting to be implemented around the world there is a clear tendency towards strengthened protection of personal data on the internet. There is, however, a risk that as more rigourous compliance regimes are implemented, small and medium sized companies will be economically affected to a larger extent than the technology giants. In that case, the Internet might still end up in the hands of corporates with the help form governments. However, I would argue that as of now, there is little evidence that the Internet has yet ended up on Tim Wu's list of corparately captured technologies, since data privacy on the internet today is increasingly safeguarded by governments in the Western world.

Conclusion

This thesis has attempted to clarify to what extent the ideals of Facebook, the world's largest and most controversial social media company, was implemented in the General Data Protection Regulation, the world's most comprehensive data privacy legislation. The research was composed by a thorough analysis of an extensive primary source in addition to interviews with central actors involved in the legislative process of the GDPR. The thesis has applied two different methodological apporaches, namely the method of *assessing attributed influence* and the method of *assessing preference attainment*. In addtion, some of the most acknowledged theories in the field of EU interest groups were implemented, namely Bouwen's (2002) Theory of Access and Klüver's (2013) focus on aggregated goods in coalitions. These efforts were made to achieve a the most credible result possible.

The research concludes that Facebook's ideals were implemented in the GDPR in 27 out of 79 cases, amounting to an overall success rate of 29.2 percent. This overall rate of succes can be described as modest. However, the research also shows that Facebook was quite influential when it came to specific issues. For instance, Facebook scored a success rate of 22.2 percent on the issue of consent, which was one of its most salient issues. Here, Facebook watered down the very definiton of consent. Weakening the GDPR's stance on profiling was another highly salient issue for Facebook, but in this regard the GDPR was left unchanged. It is therefore evident that on some very specific issues, the GDPR was indeed shifted towards Facebook's ideals. But in most areas, it was not. This was most likely caused by Facebook's lack of information supply. The supply of information was weakened due to the high amount of advanced knowledge of central lawmakers. This already obtained knowledge made it difficult for Facebook to supply politicians with sufficient influential information in exchange for influence. At the same time, there was significant political cooperation across the European institutions in order to avoid influence from the likes of Facebook. In addition Facebook's poor citizen support and coalition work contributed to an end result, which cannot be considered excessively influential. The answer to the research question stated in the introduction must thus be answered as the following: In general, the GDPR shifted towards Facebook's ideals to a modest extent. However, on the very salient issue of consent, GDPR shifted significantly towards Facebook's ideals.

This study has contributed to the study of interest groups with qualitative knowledge about how the company that processes a significant amount of one third of the world's personal data attempts to gain influence on the political stage. It concludes that Facebook to a large extent

was denied influence in European data regulation. However, there is a good argument to be made that it is not only Facebook's successful influence that is of interest. It is indeed its failed attempts as well. Because based on the failed attempts of influence a clear picture of intentions appear. It is a picture of a company whose ideals were to dodge the regulation preferences of the European Union. A company which will struggle to convince the World that it has changed its practice of moving fast and breaking things.

Literature

Beaumont, S. (2018): The Data Protection Directive versus the GDPR: Understanding key changes, Synopsys.com, Available: https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/

Bernhagen, P. (2012): Who Gets What in British Politics – and How? An Analysis of Media Reports on Lobbying around Government Policies, POLITICAL STUDIES: 2012 VOL 60, 557– 577

Bernhagen, P. & Bräuninger, T. (2005): Structural Power and Public Policy: A Signalling Model of Business Lobbying in Democratic Capitalism, Political Studies 53(1): 43–64.

Beyers, J., Eising, R. & Maloney, W. (2008): Researching interest groups politics in Europe and elsewhere: much we study, little we know?, West European Politics 31(6): 1103 – 128.

Bouwen, P. (2002): Corporate lobbying in the European Union: The logic of access, Journal of European Public Policy, 9:3, 365-390).

Bouwen, P. (2004a): Exchanging access goods for access: A comparative study of business lobbying in the european union institutions. European Journal of Political Research, 43(3), 337-369.

Bouwen, P. (2004b): The Logic of Access to the European Parliament: Business Lobbying in the Committee on Economic and Monetary Affairs, Journal of Common Market Studies, 42(3): 473–495.

Bouwen, P. (2009): The European Commission. In Lobbying in the European Union: Institutions, Actors, and Issues, ed. David Coen and Jeremy Richardson. Oxford: Oxford University Press, pp. 19–38.

Bouwen, P. (2002): Corporate lobbying in the European Union: The logic of access, Journal of European Public Policy, 9:3, 365-390.

Brown, S. (2019): Facebook co-founder Chris Hughes calls for company's breakup, Cnet.com. Available: https://www.cnet.com/news/facebook-co-founder-chris-hughes-calls-for-companys-breakup-zuckerberg/.

Bryman, A. (2012): Social Research Methods, 4th Edition Oxford University Press.

Bunea A. & Baumgartner, F. R. (2014) The state of the discipline: authorship, research designs, and citation patterns in studies of EU interest groups and lobbying, Journal of European Public Policy, 21:10, 1412-1434.

Burson Marsteller (2013): "A Guide to Effective Lobbying in Europe - The View of PolicyMakers," Burson-Marsteller's lobbying survey 5th edition. Available: http://lobbyingsurvey.burson-marsteller.com/wpcontent/uploads/2013/05/european_lobbying_survey_2013.pdf.

CFR (2012): European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html

Coen, D. (1997): The evolution of the large firm as a political actor in the European Union, Journal of European Public Policy 4(1): 91–108.

Coen, D. & Richardson, J. (eds) (2009): Lobbying the European Union, Oxford: Oxford University Press.

Constine, J. (2019): Facebook shares rise on strong Q3, users up 2% to 2.45B, TechCrunch. Available: https://techcrunch.com/2019/10/30/facebook-earnings-q3-2019/

Corporate Europe (2013): Crowdsourced lobby exposé shows Internet giants have footprints on our data privacy laws. Available: https://corporateeurope.org/en/lobbycracy/2013/02/crowdsourced-lobby-expos-shows-internet-giants-have-footprints-our-data-privacy

Council configurations (2019), European Union, Available: http://www.consilium.europa.eu/en/council-eu/configurations/

Cowles, M. G. (1996): The EU Committee of AmCham: The powerful voice of American firms in Brussels, Journal of European Public Policy, 3:3, 339-358.

Denzin, N. K. (1970): "The Research Act: A Theoretical Introduction to Sociological Methods, Aldine Pub. Co.

Diggelman, O. & Cleis, M. N. (2014): How the Right to Privacy Became a Human Right, Human Rights Law Review, 14, 441–458.

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

Dür, A. (2008): Measuring Interest Group Influence in the EU: A Note on Methodology. European Union Politics 9(4): 559–576.

Egdell, J. & Thomson, K. (1999): The Influence of UK NGOs on the Common Agricultural Policy, Journal of Common Market Studies March ,Vol. 37, No. 1 pp. 121–31.

Eising, R. (2004): "Multilevel Governance and Business Interests in the European Union." Governance 17(2): 211–245.

EUGDPR.org (2019): Timeline of events, available: https://eugdpr.org/the-process/timeline-of-events/

European Digital Rights (EDRi) (2013): Industry Coalition for (sic) Data Protection. Available: https://edri.org/files/ICDP.pdf

Facebook (2012): Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 26 October 2012, Available: https://lobbyplag.eu/docs (Analysed document can be found in Appendix. Here, successful influence is marked in blue end unsuccesful lobbying mark red)

Fordham, B. O. & McKeown, T.J. (2003): Selection and Influence: Interest Groups and Congressional Voting on Trade Policy', International Organization 57(3): 519–49.

GDPR (2016): 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, and repealing Directive 95/46/EC

Glancy, D. J. (1976): The invention of the right to privacy, 21 Arizona Law Review.

Greenwood, J. (2007): Interest Representation in the European Union, Basingstoke: Palgrave Macmillan.

Greenwood, J. and Aspinwall, M. (1998) Collective Action in the European Union: Interests and the New Politics of Associability, London and New York: Routledge.

Guarascio, F. (2012): US lobbying waters down EU data protection reform, EurActiv.com. Available: https://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/

Hansen, J. M. (1991): Gaining Access: Congress and the Farm Lobby, 1919–1981. Chicago: University of Chicago Press.

Hayes-Renshaw, F. (2006): The Council of Ministers. In The Institutions of the European Union, ed. John Peterson and Michael Shackleton. Oxford: Oxford University Press, pp. 60–80.

Hayes-Renshaw, F. (2009): Least Accessible but not Inaccessible: Lobbying the Council and the European Council. In Lobbying the European Union: Institutions, Actors, and Issues, ed. David Coen and Jeremy Richardson. Oxford: Oxford University Press, pp. 70–88.

Hern, A. (2018a): Facebook: we were too slow to recognise our 'corrosive' effect on democracy, The Guardian. Available: https://www.theguardian.com/technology/2018/jan/22/facebook-too- slow-social-media-fake-news-hiring.

Hern, A. (2018b): Cambridge Analytica did work for Leave.EU, emails confirm, The Guardian. Available: https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm

Hern, A. (2018c): Facebook moves 1.5bn users out of reach of new European privacy law, The Guardian. Available: https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.

Hoofnagle, C. J., van der Sloot, B. & Borgesius, F. Z. (2019): The European Union general data protection regulation: What it is and what it means, Information & Communications Technology Law, 28:1, 65-98,

Hootsuite (2019): Global Digital 2019 report. Available: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

Johnson, K. , Martin, S., O'Donnell, J. & Winter, M. (2013): NSA taps data from 9 major Net firms USA Today. Available: https://eu.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/

Jones, H. & Soltren, J. H. (2005): Facebook: Threats to Privacy, Massachussets Institute of Technology. Available: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf

Joos, K. (2011): Lobbying in the new Europe: Successful representation of interests after the Treaty of Lisbon. Weinheim: Wiley-VCH.

Kahn J., Bodoni S., Nicola S. (2018): It'll Cost Billions for Companies to Comply With Europe's New Data Law, Bloomberg, Available: https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law)

King, R. (2013): Facebook bug exposed personal data of six million accounts, ZDnet. Available: https://www.zdnet.com/article/facebook-bug-exposed-personal-data-of-six-million-accounts/

Klüver, H. (2013) Lobbying in the European Union: interest groups, lobbying coalitions, and policy change, Oxford University Press

Kollman, K. (1998): Outside Lobbying: Public Opinion and Interest Group Strategies. Princeton, NJ: Princeton University Press.

Kramer, I. R. (1990): The Birth of Privacy Law: A Century Since Warren and Brandeis, 39 Cath. U. L. Rev. 703 Available: http://scholarship.law.edu/lawreview/vol39/iss3/3

Kraus, J. L. (1993): On the Regulation of Personal Data Flows in Europe and the United States, 1993, Columbus Law Review 59.

La Quadrature Du Net: IS THE COUNCIL SELLING OUR PERSONAL DATA TO PRIVATE COMPANIES?, 2015 https://www.laquadrature.net/en/2015/06/24/is-the-council-selling-our-personal-data-to-private-companies/

Lecher, C. (2019): Elizabeth Warren says she wants to break up Amazon, Google, and Facebook, Theverge.com. Available: https://www.theverge.com/2019/3/8/18256032/elizabeth-warren-antitrust-google-amazon-facebook-break-up

Lobby Planet (2011): Lobby Planet Guide 4th Edition. Available: http://corporateeurope.org/sites/default/files/publications/ceolobbylow.pdf.

Lobbyfacts (2018). Facebook Ireland Limited. Available: https://lobbyfacts.eu/representative/64755e0fc2a14e46aa9d8646df6f8f19/facebook-ireland-limited

Macrotrends (2019): History of companies' stock market caps can be found here: https://www.macrotrends.net/stocks/charts/FB/facebook/market-cap

Majone, G. (1996): Regulatory Legitimacy. In Regulating Europe, ed. Giandomenico Majone. London: Routledge, pp. 284–301

March, J. (1955) An Introduction to the Theory and Measurement of Influence, American Political Science Review 49(2): 431–51.

Mazey, S. and Richardson, J. (eds) (1993): Lobbying in the European Community, Oxford: Oxford University Press.

McCarthy, C. (2008): Class action suit means Facebook's Beacon just won't go away, CNET. Available: https://www.cnet.com/news/class-action-suit-means-facebooks-beacon-just-wont-go-away/

McCarthy, C. (2009): Facebook notifies members about Beacon settlement, Cnet.com. Available: https://www.cnet.com/news/facebook-notifies-members-about-beacon-settlement/

Moravcsik, A (1993): "Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach." Journal of Common Market Studies 31(4): 473–524.

Michalowitz, I. (2004): EU lobbying - principals, agents and targets: Strategic interest intermediation in EU policy-making.

Naughton, J. (2016): The evolution of the Internet: From military experiment to General Purpose Technology, Journal of Cyber Policy, 1:1, 5-28,

Newman, A. L. (2011) Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe, Journal of Comparative Policy Analysis, 13:2, 181-194

Nielsen, N. (2013): Belgian MEP blames assistant for industry-scripted amendments, EU Observer. Available: https://euobserver.com/institutional/122205

OECD (1980): Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, revised in 2013.

Dionisopoulos, P. & Ducat, C. (1976): The right to privacy, West Publishing Co.

Palmer, D. (2019): Where GDPR goes next: How digital privacy is taking over the world, ZDnet.com. Available: https://www.zdnet.com/article/where-gdpr-goes-next-how-digital-privacy-is-taking-over-the-world/

Pappi, F. & Henning, C. (1999): The organization of influence on the EC's common agricultural policy: A network approach. European Journal of Political Research. 36. 257-281

Pijnenburg, B. (1998): EU lobbying by ad hoc coalitions: an exploratory case study, Journal of European Public Policy, 5:2, 303-321,

Press Association (2019): Mark Zuckerberg calls for stronger regulation of internet, The Guardian. Available: https://www.theguardian.com/technology/2019/mar/30/mark-zuckerberg-calls-for-stronger-regulation-of-internet

Reidenberg, J. R. (2001): E-Commerce and Trans-Atlantic Privacy, 38 Houston Law Review, 717-730.

Rittberger, B. (2003): "The Creation and Empowerment of the European Parliament." Journal of Common Market Studies 41(2): 203–225.

Rosenberg, M., Confessore, N. & Cadwalladr, C. (2018): How Trump Consultants Exploited the Facebook Data of Millions, The New York Times. Available: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Sanders, J. & Patterson, D. (2019): Facebook data privacy scandal: A cheat sheet, Techrepublic.com. Available: https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/

Schildberger, L. (2015): Lobbying and its influence on the draft of a General Data Protection Regulation of the European Union unveiled in 2012. Available: https://www.law.tuwien.ac.at/Schildberger_Einreichversion.pdf

Scott, M. (2015): Data Transfer Pact Between U.S. and Europe Is Ruled Invalid, New York Times. Available: https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html

Sengupta, S. (2011): F.T.C. Settles Privacy Issue at Facebook, The New York Times. Available, https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html

Sheidlower, J. (2006): A Lobbyist by Any Other Name? National Public Radio. Available: https://www.npr.org/templates/story/story.php?storyId=5167187?storyId=5167187&t=1568722478994

Sherr, I. (2019): Facebook lost control of our data. Now it's paying a record $5 billion fine, Cnet.com. Available: https://www.cnet.com/news/facebook-lost-control-of-our-data-now-its-paying-a-record-5-billion-fine/

Solove, D. J. (2001): Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393, 1407–9.

Solove, D. J. (2006). A Brief History of Information Privacy Law in PROSKAUER ON PRIVACY, PLI.

Statt, N. (2019): Facebook CEO Mark Zuckerberg says the 'future is private', Theverge.com Available: https://www.theverge.com/2019/4/30/18524188/facebook-f8-keynote-mark-zuckerberg-privacy-future-2019

Stephenson, P. (2019): New Research Shows Facebook Brand Trust Lowest Out Of Top Tech Players With Apple Ranking Highest, which50.com. Available: https://which-50.com/new-research-shows-facebook-brand-trust-lowest-out-of-top-tech-players-with-apple-ranking-highest/

Stevenson, Alexandra (2018): Facebook Admits It Was Used to Incite Violence in Myanmar, The New York Times. Available: https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html

TEU (2012): Consolidated Version of the Treaty on European Union [2008] OJ C115/13. Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 47, 55, art. 16(1)). Available: http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

TFEU (2012): European Union, Consolidated version of the Treaty on the Functioning of the European Union, 26 October 2012, OJ L. 326/47-326/390; 26.10.2012, available at: https://www.refworld.org/docid/52303e8d4.html

Transparency International (2015): Lobbying in Europe - Hidden influence, privileged access, Available: https://www.transparency.org/whatwedo/publication/lobbying_in_europe

Voss, G. W. & Houser, K. (2019): Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies p 41. 56 American Business Law Journal 287-344. Available: https://ssrn.com/abstract=3389515

Warman, M. (2012): EU Privacy regulations subject to 'unprecedented lobbying', The Telegraph. Available: https://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html

Warren, S. D. & Brandeis, L. D. (1890): The Right to Privacy, Harvard Law Review 193
Weisbaum, Herb (2018): Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal, NBC News, Available: https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011

White, A. (1997): Control of Transborder Data Flow: Reactions to the European Data Protection Directive, International Journal of Law and information Technology Vol 5 no. 2.

Wu, T. (2010): The master switch: The rise and fall of information empires. New York: Alfred A. Knopf,

Zarsky, T. Z. (2017): Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall Law Review 995 13.

Zuboff, S. (2018): The age of surveillance capitalism: The fight for the future at the new frontier of power, London: Profile Books

Appendixes

Questionnaire: Experts embedded in the law making process

1. In your own words, define "lobbying."

2. What are politicians' interests when meeting with lobbyists?

3. Which European institutions were lobbied most extensively with regards to GDPR?

4. In your opinion, was GDPR weakened or strengthened as a result of the lobbying process?

5. In your experience, what were the strategies of Facebook during the lobbying process?

6. Did Facebook lobby independently, in coalition or both?

7. Is there a difference when lobbying in coalitions, in your opinion?

8. Which parts of the GDPR did Facebook lobby primarily?

9. What kind of information/arguments did Facebook's representatives bring to the table when lobbying?

10. How would you rate the credibility and impact of the information/arguments?

11. To which degree did Facebook influence the final text of GDPR?

Questionnaire: Lobbyists from Facebook or in association with Facebook

1. What was your organisation's objective when lobbying the GDPR?
2. Can you describe the your means or strategy in this process, lobbying process?
3. Can you describe the advantage of lobbying in coalition
4. Were you satisfied with the final outcome of GDPR?
5. How would you define lobbying in your own words?
6. To what extent were you as able to contribute effectively with information to politicians?
7. Which part of the GDPR was most important to your organisation?
8. To which degree do you think Facebook was succesful in influencing the final text of GDPR?

Interviewee A

A Senior Advisor to the LIBE committee

What's your definition of lobbying?

I don't think I have a fully elaborate definition of lobbying, but my general understanding is that lobbying is the attempt to influence policy-making by individuals or organisations that have a self-interest. I would distinguish that from public advocacy interest groups if they do it for the public good. Then you can of course lump it together and say that lobbying is everything that tries to impact policy-making and then NGOs are also lobbyists. But I would not say that public institutions are not lobbyists... but of course when the US mission has approached us, it's a fine line whether it's diplomatic relations or lobbying.

What are your interests when you meet up what do you want to get out of meeting with lobbyists?

Our main interest was to meet as many lobbyists as possible and try to respond to all the meeting request mainly because we wanted to know what they told the other MEPs. It was really interesting sometimes that our colleagues sometimes used the exact same arguments that we had heard from the lobbyists the day before. Sometimes it was interesting to find out "oh my god" they are using these nasty data collection practices. I wasn't even aware of that, but thanks for telling me. And of course in certain circumstances it was good to get a better understanding of how the lobbyists businesses actually worked and what data they needed and how they get it and so on.

And which European institution was lobbied most extensively?

It's a bit hard to tell because I only experienced it in the Parliament, but normally where it goes on in the preparatory phase is in the Commission. The Commission has to publish the meetings with lobbyists, but they also just go for a coffee all the time, so it's not so transparent. And then the Parliament was of course heavily lobbied. Of course the shadow rapporteurs and us, but also people in the opinion giving committee. But also other MEPs and group leadership and so on. That was quite a lot, which led to the fact that in the end there was 3999 amendments on my table which had to be distilled into the compromise text. But

then when the Parliament is done, normally the lobbying moves to the capitals because then they want to influence the member states and get their positions into the council position. I don't really know how intense that was. I guess it was less intense than here in Parliament because in Brussels it's easier to approach people and you don't have to travel across Europe.

In your opinion was the GDPR weakened or strengthened in the lobbying process?

I mean, I would say 95% to 98% of the lobbying was trying to weaken data protection rules in all kinds of aspects. They mostly had the same interests like when can you get data without asking for consent before. And then also using data you have already collected for different purposes. But then also we had some lobbying around the fines by some financial sector lobbyists. They said: maybe you want to measure the fines by the percentage not of our global annual revenue or turnover but only the money they make in Europe. And then I always will I told them "ok are you already telling me now that you are planning to breach the law?" haha. But then on the other hand we had very engaged NGOs. It was mainly coordinated through EDRi, but also some member states from the European countries like Netherlands, Germany and Poland. So in this setting when we knew that Jan Albrecht who was already known as a data protection guy became Rapporteur we thought the lobbying would be even harsher and so we expected this kind of backlash. But on the other hand we tried to compensate that by a lot of media work so my colleague who did press relations put in a lot of energy and time into setting up interviews and op-eds and TV Appearances and so on. So it was our hope to counter the lobby pressure by public attention so our colleagues from the other political groups would not fully end up in line with the lobbyists, but also feel responsible towards the Citizens. And then there are of course some factors that helped. You saw Snowden but also Max Schrems was quite an important factor. Also because he built this platform you may have seen called LobbyPlag together with some open data journalists from Berlin. And that was really helpful because it was in the middle of the amendment phase so then when journalists came they were all interested in seeing this as another example of lobby influence in Brussels. So the first week of reporting was mostly about lobbying and then some of them also dug a little bit deeper and became interested in the topic and started to report about this data protection reform: what is it actually about, what are the conflicts and the discussions and so on. It was quite a unique situation because the lobbying landscape was very imbalanced. There was a lot of industry lobbyists who wanted to weaken it and a few NGOs to strengthen.

So the normal outcome would have been a massive watering down of the GDPR. But we were in the lucky situation that Jan was the Rapporteur. And he was a data protection lawyer with a degree in data protection law and I before I came to Brussels was an academic researcher on data protection and governments for 10 years. So we really knew our shit. It also led to the fact that - you probably know that the Commission already in 2010 came up with the communication to prepare for the GDPR and then to this communication the Council and the Parliament normally reacts to already say where the majority is lying and what kind of things go and not go - we already in 2011 inserted the clause that we do not want to lower the existing level of protection from the 1995 directive. That was already then the baseline and we could always refer back to it. That really helped us a lot because we wanted to make sure very early on in the process that this was commonly agreed and we wouldn't deviate from it. And then in the end we were also lucky later in the process. Because with the final negotiation in the Council, the Council position was much weaker and industry friendly. They wanted to allow for accepting and processing data for different purposes which is an absolute no-go since it would be against the charter. But when we had the final trilogue on the final text, the Council presidency, just by coincidence, was Luxembourg and Luxembourg's government was in coalition with the Greens. And The Greens was also part of the government so the responsible minister for Justice was from the Green Party. And I'm not sure if that has ever happened before. At the moment the Greens are only in Government in two or three member states, so you can calculate how many years will last until they will be in the Council Presidency again. And then having a Green Rapporteur helped us a lot in preparing the negotiation sessions already beforehand to really oversee: OK, how do we in a way "script" the negotiations to get the outcome we want.

So it was kind of a perfect storm for you?

It was just a really lucky coincidence. I mean this whole GDPR has so many things that rarely happens: To have a green Rapporteur who is really an expert in the field, to have a green counterpart in the Council at the trilogue negotiations, to have a very committed Commissioner for Justice, to have Max Schrems helping us, and to have Snowden in between. All of these things are very rare and random in themselves. And the combination of them almost made me believe in God again, you know. This cannot just be a concident.

What was the name of the minister from Luxembourg?

Felix Braz

Diving a bit more into the Facebook lobbying how do you see the lobbying of the Parliament with regard to the GDPR?

Facebook but also the other big Silicon Valley companies like Google, Yahoo and whatever and to lesser extend Microsoft and Apple, they knew that if they appeared too aggressively in the lobbying it would backfire, because there was already a growing fear for these companies among Europeans. Facebook specifically, I think, we had a few meetings with them on different levels like with Erika Mann who became their chief lobbyist in Brussels, but also with Richard Allen...sir Richard Allen...apparently a good old friend of Tony Blair who was the European chief lobbyist. But what they also did was and this is even more for Google, they set up and supported industry associations to hide behind them so to speak. And it was not only the traditional already established industry associations like TechAmerica, but also certainly these new industry associations that hadn't been there before. Suddenly you had an Industry association for data protection and then when you look into it of course it was against data protection and mainly funded by big tech from the US. It was something like the European Industry Coalition for Privacy and Data Protection but also suddenly this app developer Alliance or something like that who claimed that they represented 5000 small independent app developers from all across Europe. And then the colleagues from Corporate Europe Observatory started digging into it and found that they were mainly funded by Google and Apple.

So that was their strategy, basically to not be so transparent?

Yeah yeah.

But if you were to describe the strategies in your words what would they be?

As I said to not appear too aggressive and direct and rather hide behind some industry associations and umbrella organisations.

But you did have meetings with them?

We had a few meetings yes and as I said we tried to meet everybody I wanted to see what they would tell the other groups.

What kind of knowledge of points did Facebook representatives bring to the table?
I really have to guess. It's so long ago. But it was mainly about lowering consent and being able to use their services and platforms without being asked about too many things and let them use the data also four things they don't tell you and stuff like that. Maybe at the end but I'm not sure there was also some lobbying around the age limit for consent

And how did you find those meetings and the knowledge that they probably gave to you? Was there a kind of exchange situation where Facebook had some knowledge they wanted to give you and in exchange they get influence? How did you experience that?
Not so much as I recall. I know Facebook I have read some things about Facebook: how it works and so on with the data they collect. So it wasn't a big surprise. We expected them to demand what they demanded, so nothing really special or surprising. The only thing I found interesting in the meeting with Richard Allen was that I asked him about data subject access request for Europeans and for Americans and he confirmed to me that Facebook already provided more data access to European - because they had to under their 95 directive. But they don't give the same rights to American customers or users. And I found that really interesting because then I could tell my friends in Washington that you might want to know that they give Europeans more rights than Americans.

You would think maybe Facebook would have an elaborate strategy on how to influence you. You didn't see that?
No, actually most of the lobbyists didn't seem to have an elaborate strategy. They just tried to request meetings and talk to people and be nice and make us understand their concerns and that they already had many regulations to take into account and more would hinder innovation and that usual la-la that you hear all the time. Nothing that really looked like a strategy. I think the only group that really had a strategy that actually worked in the end was the pharmaceutical companies. Because they didn't come to us themselves, but they always sent their Welcome Trust set up by the pharmaceutical industry years ago to conduct studies and research. And they came to us and always claimed to represent the students, researchers

and academics and said it was in the public interest and la-la-la and they really systemically got established research institutions on board like for example the German research foundation and serious academic professors and universities. They really made them crazy and made them believe that the GDPR would hinder them from doing research. And that really led in the end to the fact that we now have a privilege for further processing for research purposes that wasn't there before. But that was really the only, I would say, elaborate strategy. Everybody else was just trying to have meetings be nice and you know: these poor companies they have so many applications and we must not prevent innovation and all that. It wasn't too brilliant, haha.

Ok. Interesting. So, I guess you talked about it already, but which piece of information from any of these stakeholders do you consider most impactful?

From all stakeholders it's hard to tell. I mean, we met so many of them and they had an impact on bits and pieces of the GDPR all over the place.

It seems, and that's just my immediate analysis, that you were so knowledgeable about the legislation and the field that maybe there was not so much information there to be provided to you. Do you think that other legislators might have been lobbied and influenced because they didn't know that much?

Yeah that's how lobbying normally works, haha. I mean, people legislate on all kinds of issues and they never can be experts on everything. But you would have to ask the other MEPs about that. We tried to counter that for example by also meeting with the MEPs regularly and I have very long meetings when the process began in 2010/2011. With the assistance of Axel Voss, the EPP Shadow Rapporteur who was new to the field of data protection. We sat long afternoons in one of the coffee bars in the Parliaments and I walked him through the idea and history and purpose of data protection and that of course also helped to counter the industry lobby to a certain extent I hope.

Would you tell me, if you had been lobbied successfully?

I Have been lobbied by many, but I'm not sure they had so much of an impact because really we had our knowledge in the field and clear principles and understanding of the whole thing.

It was rather tactical that we had to know what they tell the others. You always need to know the arguments floating around, and we had to figure out ways to counter them and stuff like that. And then also maybe alert our NGO friends or sometimes even people from the Commission that there is this strange argument going on, you have to do something. Please talk to a shadow rapporteur.

To which degree do you think Facebook influenced the GDPR?

Haha, it's really hard to tell. I'd be interested to see when you go through the lobby documents if there's any bits and pieces may contain traces of Facebook in the final text. I would doubt that. But as I said because we had already at the very beginning made clear that we would not lower the existing level of protection, so opening up the process like the Council wanted, that was for us a clear no go. So I'm not exactly sure if Facebook had any particular impact on the final text. If the whole lobbying, not just from Facebook, but from all the industries, hadn't been there, then of course the final text could have been much stronger, that's clear. But I don't see a specific impact of Facebook anywhere.

Did the coalitions of tech companies have an impact? Do you think the fact that they worked together made an impact?

Yeah, it made their arguments and demands more aligned. I guess it's more problematic if one company asked for A and the another for B and another for C. But then again, as I said, the Silicon Valley companies mainly used it to hide behind these associations and not appear too aggressive.

Ok, well, thank you, it was a pleasure talking to you

No problem good luck with the thesis

Thank you.

Interviewee B

Former chair of a Facebook-supported lobby association

Yes hello, we agreed that I could call around 10AM?
Yes, now is a good time.

Then let's start with the first question: What was the raison d'etre behind your organisation?
I mean, it was to...I called the access to data, or the privacy, the hidden freedom, I mean, we have all those freedoms as human rights and that was a forgotten human right. And I wanted to put into the open that we all have a right to privacy.

And so you gathered these different backers into this association, why was there a need for that?
That is the way to be visible and have access to people. You can't come as a private person. Nobody would talk to you.

But companies could do it individually, right?
What companies?

Companies like Facebook.
Yeah but you can't compare, I mean Facebook is more important than individual countries and you can see now there are Ambassadors in Silicon Valley because those companies are so powerful. So we need to have somebody to go against them, to give another agenda and not theirs.

But wasn't Facebook one of the backers of your organisation?
Mmm yeah, because, I mean, they didn't give us much, but I mean Facebook realized because of us and others, that they needed to have another face, a propos FACEbook, they needed to have another face in the public. And so, therefore they supported us, because they could see the necessity of having somebody defending this agenda.

OK. So as a result of this legislative process and lobbying process what's your opinion on the GDPR text. Was it weakened or strengthened?
It was absolutely strengthened; we were up against many, also many governments. I was a little bit shocked how difficult even the governments were in the beginning very, very reluctant and I have never found out why. It was not only the business world, it was also government, and I think we made an impact, also together with very good MEPs and now you see that this legislation has actually been a pattern for the rest of the world.

Great. How would you define lobbying in your own words?
I mean lobbying is not a bad word, lobbying is an important thing to do because as a politician you need to have the outside world tell you what it's about. As a lobbyist you always have to tell the truth and nothing but the truth, and if you do that, then you have an influence. People listen to you.

So what kind of arguments did you bring to the table in these conversations with politicians?
I can't remember anymore but I mean we had made studies, independent studies by people from the university and consumers. And we told the politicians how important was the Right To Be Forgotten. That was one of our really strong words together with access to information.

And you were talking about, Facebook being one of the backers. How much influence did they have on the work you did?
I have to admit that I can't remember, I don't think they had much influence, because we didn't allow that. They came up with factual information. We wanted to be credible by talking to those we were attacking the GDPR. They have a lot of knowledge, they could tell us about how they work and the whole system, so they were important, but I mean you can never be credible if they have influence.

But is knowledge also not a kind of influence?
Yes knowledge is influence, of course, I mean in a Western society knowledge is important.

But if Facebook provided knowledge to you - didn't they have some kind of influence?
I mean, I would not define that as an influence. You work on the basis of knowledge. I find this question a little bit odd, I have to say. Knowledge, I mean, you also don't work in a world without knowledge. Knowledge and influence, I mean, knowledge is the basis of how you work, so I find it a little bit strange I have to say.

Ok, so if I rephrase it, maybe information can give influence? To what extent were you able to contribute effectively with information to politicians?
Yes, information, and then, I mean, then of course, when you get information you also value it and evaluate it and when I got information from Facebook, I evaluate it: Is it something I can use, is it trustworthy or what is it, yeah. I mean, knowledge, how would they manage it? Do they have a mechanism to make sure data can be forgotten? How would they fulfill our requirements? I mean, that's information. And if we were proposing something that was totally irrelevant and totally not possible to realise, then I mean it would be silly. So therefore factual information is important.

Can you describe the your means or strategy in this process, lobbying process?
I think I have done it, I mean...

Did you hold meetings? What were the...
...We made workshops. I mean, I have never met Facebook if that's the question. But I mean, we made workshops and web seminars on the website. Open webseminars so people that have knowledge could be involved. It was a very, very open process.
I had knowledge about how to do politics and I didn't have any technical knowledge. Therefore we needed to have technical knowledge yeah?

Which part of the GDPR was most important to your organisation?
For me, it was the Right To Be Forgotten and access to your own data. I invented the phrase, the forgotten human rights. And therefore, when you have this phrase, then of course the

person isn't in the center and therefore the right to be forgotten as a person and the right to have access to your own data, because that is what you own. For me it's about human rights.

And that seems to be also the opinion that many of the MEPs were of. That there should be a need or a Right To Be Forgotten, but which part did you want to change....

...To implement it is a technical issue and when I had dealings with politicians and business and they told me how difficult it could be. They always argued on a technical scale and I always argued from a point of view of human rights. That was my angle, because I'm not an IT person, but that was why I took this job.

But did you find a lot of agreement with the politicians?

Yeah, and the Greens, I mean, often I was very agreeing with the Greens because they have the same point of view with putting the person in the center.

So, to which degree do you think you were successful in influencing the GDPR?

I don't know, I mean, we were a small association, you also have the time, during those years, the time also went so it was more pro...I mean, we started the discussion and became more and more joint, so there are many factors. You also have to have the timing correct. And the timing was great and maybe it dragged on for many years and maybe it was alright because then the surroundings changed, as you can see now with the climate crisis. I mean suddenly people realise that this is an important issue, and I think during those years, where it dragged on and on, people realised that even the national politicians who were against it, because they were lobbied by businesses locally saying the law was ridiculous and we didn't need it and da-da-da-da-da, but then things changed yeah?

Can you explain a little bit more about the national politicians? Why were they against it?

I mean they were lobbied. Take the business associations, they were up in arms. And I had many, many discussions with my own government, my party was in the government during those years, and they just heard all the complaints. That it was so difficult and impossible, and all the red tape. They hadn't any clue about it, and even some of those politicians couldn't see the need and therefore it is important that you have a European Association that has the fuller picture and sees it from a broader perspective, yeah?

So that was the goal with the organisation?

Yeah, and put focus on this forgotten human right. And I also wrote a lot of articles about that. And now people realise that this data is really valuable, I mean, in the beginning Facebook only wanted to have this very human approach of connecting people, but I suddenly saw that they made money from the data. That is really the problem now. That is what ruins, and Facebook gets problems about it, and you can see how it was misused with Brexit and Trump and all that. In the beginning, data was not their asset and now it's really a dangerous business, really dangerous. And therefore I have never supported Facebook, I think it's really...and people should really realize how problematic it is, but that's another point.

Some think that Facebook's strategy was to exactly go into associations for them not to seem too powerful.

Yeah, I mean, so it is. I was not blind, I mean, they supported us in the beginning because then they could get a better face as I started to say. But then as an association you have to be so strict that you don't allow them to have influence. For me, I have always seen it, I'm very cynical, I know exactly what it is about, but I could also use them in the sense that I could get information from them. I could challenge them and say OK: I have the strategy that it's better to have them on board and influence them. We also influenced them, It's not only them influencing us. And then be very aware of what they were doing. I think it's a two-way street. And I know exactly why they did it, to show they were good, but on the other hand, we could also use them to confront them. And then you had to realise we also needed some money. You can't lobby without money. I didn't get any salary, but we had some expenses. I wouldn't pay my trips on my own. We needed a little bit of money to do the trips.

When one reads about the organisations like yours in the news and articles it is easy to get the impression that you were in the pocket of the tech giants and stuff like that and that you weren't transparent. What do you think about that?

It's nonsense, we were not, I mean, I never met them, I mean, I never met the top guys and we have a website that's transparent. We have to obey to the rules of the Commission, I mean, I don't think it's fair to say that.

OK. But who from Facebook did you meet with?

I think we met in Brussels, they had lobbyists in Brussels. I mean we didn't meet them much. We met with scholars and university professors and geeks, technical experts. And also human rights experts. And then I have to say, we were one of the first that started it, so it is easy to criticise us. But who were the critics? And you have to start somewhere. I mean we were the first to take this issue very seriously.

Ok, good. Great.

Are we finished? Are we soon finished?

Yes, let's say that was it and then I'll say thanks.

Interviewee C

Former high-ranking Facebook representative at Brussels Office

So the first question would be a general one: What was your organisation's objective when lobbying the GDPR?

I mean, my personal opinion is that, you know, whoever is doing the lobbying you have to be extremely serious, so not lobby in the sense in believing you can convince a policy maker about your own opinion, you want to explain the situation and the situation for each company is totally different and you need to be serious about it so that's the most important. And that's true for companies and NGOs. I wasn't lobbying on GDPR. That's true for, I would say most of the companies. Because in these kind of cases this is dealt with by the various department responsible for data privacy and data protection. So that's not something an office individually would handle. And this is true for all major companies. It's different if you have a very small company but maybe then you don't have the capacity neither with the exception its an item which is extremely important for a small company. Otherwise the small company will not have the capacity to deal with such an important item. It typically comes in much later that the big companies.

Ok. So you're saying you didn't lobby for yourselves you lobby in association with other organisations?

No, I didn't lobby at all. It wasn't my issue. I was at the time, when was it, I even have to try to remember. Facebook already had a unit in Ireland, which is still there dealing with these kinds of issues. So it was their responsibility. That's normal for all because you would have the same situation if it was not data protection but for example copyright. You would have the copyright unit and these companies dealing with these issues wherever they are located. Because these topics are very particular and very specific so you need to have the complete knowledge about, not just how the processes work internally, but you need to have a long history in law. And understanding all the potential legal implications too (Which typically is not something a head of an office would be able to do) Yes, I know the history of course of the copyright law or the data protection law. But it's something very different when you look at it

from a company angle. You really have to be certain that all the processes you have in place either correctly reflecting what the law wants you to do or you have to understand from a technical point of view in particular when you are a young company, you know: is the technology actually advanced enough to implement what they want you to do. And then in this case maybe you want to go in and make a case and it's maybe more difficult than the lawmakers expected it to be from the beginning. I'm happy to connect you to the people there, if you really want their opinion and if they are allowed to talk to you.

Ok. But can you describe more generally what Facebook's opinion was towards the GDPR?

Was very positive. I mean not positive in the sense...companies are neither positive nor negative, they analyse cases. They analyse the law. And try in case something they believe is not reflecting correctly, either how they handle it or how the law maker believes it can be done, then he will come in and talk about it. I mean I only have good opinions about the way it was handled at the time. There was never a hostile feeling against the law. It was more challenging, it can become quite challenging in a global environment so you want to understand the implications and don't forget at the same time there were already legal cases pending so the complexity, the team wanted to understand in a a correct way.

And you're saying this thing about that you tried to provide knowledge to the politicians from your perspective. To what extend do you think you were able to do that as a corporate company?

You know, I think this would need a little bit more reflection to give a correct answer. The past is something that gets overshadowed quickly. I have different impressions and on have to be very careful. I don't remember in the single case. I remember the very early days. It was a small team, keep in mind Facebook was a small company. We tend to forget this. It was a very small team, not just a small team in Brussels but even relatively small in London at the time and in Dublin. London was still the policy department where most of the people were located at the time. It's completely different now, but at the time it was like this. so you know, I mean it was really much more discussion. At the time it was really not well understood how these technologies work, so there were many discussions and in most cases I wasn't involved. Yes, I went to some meetings but in most instances my colleagues were involved, and I would not be

able to tell you how they felt about it. Politicians typically, there was a good team of politicians and legislators involved. They were quite experienced, they had a quite good knowledge not just about the privacy situation, but about these new companies, too. Maybe less understanding how Facebook worked because some of them were Facebook sceptics, which overshadowed their opinion to some degree too. Many of them were more on Twitter than they were on Facebook and Twitter has a completely different function. So one has to keep this in mind, but nonetheless they were experienced and understood how in general these technologies work. Or shall work. So even the most critical whom I know well, like Jan Albrecht we are from the same constituency, so we know each other well. I mean, he's a serious politician, you know, there was never a single doubt that he wouldn't understand the consequences. Maybe not all the consequences what might happen in the future if some of the changes would be introduced. But this is difficult at the beginning of law making. You can't overlook all the implications. But there was never a single doubt that we dealt with politicians at the time who understood the issue and the same was true in the Commission. so yeah.

And if you look at the final GDPR text. was Facebook happy with that?

You mean the outcome? I think so, I think Facebook changed as well over the last years in understanding that even in areas where you can't completely grasp always all of the implications once they are implemented, I think there's an understanding now that sometimes legislations are more helpful, you know, instead of avoiding legislation. So I think this understanding is there. There's still some, I'm pretty sure, less Facebook, more in the public and the commission maybe, more doubts if all of the aspects of the legislation are really always helpful. But for companies...and that's something I learned, something maybe legislators don't always understand, is how serious companies are in implementing legislation. So once you have a legislation you try everything you can to play and to support these kinds of legislation. You don't go against them. Because of liability risk, legal risk, many other risks, which you have. And that's just not the way companies operate. At least not the companies I know. They don't do this. so they take this extremely serious. It's just not always easy because these are complex laws. In particular, the GDPR, is a super complex law because it's a regulation, but at the same time in certain environments it is implemented in member state law differently. So it is one of these seldom regulations which are not always 100% identically interpreted in the different member states, because of the responsibility of the

national data protection office. So, one needs to keep this in mind, which is of course challenging because you would expect to have a law which was completely uniformly applied across the EU. And in particular in an important field where you have to deal with many online challenges, where you want to have a unified law. And so far it is a very opaque law in certain areas. And you can see this in the court cases and the discussion of the European Data Protection Board. So it's not always easy for companies, but, I mean, big companies can handle it. It's much more difficult for small companies.

I've talked to other people who believe GDPR has affected the business model of Facebook. Do you think so?

Not automatically, I don't understand why. The business model existed before so yes there are changes on the advertisement side, changes on certain implementation you can't do in Europe as quickly as you do globally, certain rules on facial recognition and other stuff. You need another tier in the development face, another tier of consent procedures, but I don't remember that the business model changed. Maybe it did. Maybe I'm just not aware about it. Could have happened. I'm not a super active user, so it's not like I wouldn't have recognised what would have changed. I mean, you have more safeguards in place. There is a bit better description about what users can do, users are more alerted to it. You have much more steps how users are informed about things. This all changed but this is not really affecting the business model because that relates more to the advertisement angle. And it's true, there are some changes but I'm not sure if the work is already done on the research side. There are changes of course because at the time developers had much more freedom on how to develop their own ecosystems on Facebook. And I'm talking about developers, not advertisers but of course sometimes there's a crossover. If developers need access to the advertisement side too. So there must be some changes. Because you see that the developer side is much more constrained, but this was in my understanding less related to GDPR but much more related to the access developers were given before the Cambridge Analytica case, but I'm not so sure this relates to the GDPR. But someone needs to look into this to be honest about it.

But in a general sense you would think that when a company's access to gathering data is limited and when the business model based on data then it must have an affect on the actual business model?

GDPR is not limiting access to data. As soon as you have informed consent you are allowed to collect the data. And in the cases of Facebook you can't provide the service if you are not allowed to do it. It's very simple. Once you have the...What you can do but Facebook never did this. They were never able to do it - there's a misunderstanding about what is called behavioural advertisement. My understanding is in the traditional sense of the behavioural advertisement is, I have never seen Facebook being able to do this and they never did it. What they do is much more related to... You have certain cluster that advertisers use and they then apply across the spectrum of the users. You can check and go to the advertiser side and check how it is done. You select a city of a country or a region and then you sub select. So these are not very detailed behavioural descriptions, so I don't know why they should have changed, why? They're pretty raw, not detailed, so why would the business model have to change? But maybe I'm missing something, I could.

I'm just thinking, if there's a need for more explicit consent maybe less people would provide their data to Facebook for example?

They don't provide data. That's another misunderstanding. As a user you never provide data. You provide information in the sense that you fill in the information about whatever you believe is relevant in your news feed. But that's not data. That's information. Now, you can call information data, but before you can make it valid you would have to translate all the informational input you put in back into raw data. And then for an advertiser to make money out of it, you're back in the cluster field. So is it really helping you? When is it helping you from a business perspective? So, I don't know that the GDPR would have introduced a change there. I can't see it, maybe I'm missing something?

So you didn't see at Facebook a threat in the GDPR?

No. The concern at the time was really much more: Can the consent really work and how much would you have to differentiate between the European legal space and the global space. Because at the time it was: Ireland handled all of the data globally with the exception of the United States and Canada, which was handled in the US. This changed after GDPR. So after GDPR, Ireland was only handling the EU data which is different than before. So that's a change. But it's more a change on the global scale. On the legal liability scale. Because once you have a GDPR, which is by the way an interesting situation because before Europe was

practically the center for Facebook for handling data privacy and protection. After, it changed. And so it was only dealing with the European sphere, not the rest of the globe. So that's a major change, but less a change related to the business model and more a change related to the legal risk environment.

You were talking about the politicians' opinion towards Facebook during the process. How was it to be a Facebook representative in that time? There was another awareness in the public on data legislations and maybe also among politicians. How did you experience that?

I mean, the only case which was at the time relevant for us was Max Schrems. He was one of the active players and then you had some players from the US and some other players for Europe and of course Paul (inaudible) who looked at it from the human rights angle. I mean, I never had an uncomfortable discussion with any politicians in the parliament, in Germany or elsewhere. The only thing I say, and I said this to them as well: I believe they sometimes had a limited understanding about how Facebook works, but that's natural. It's not something you can use as an argument. It's true for all other environments. So that's somehow natural. But I felt sometimes that sometimes there was complaining about some of the issues, where I felt: That's why you want to have Facebook, because, it's not like twitter. I felt sometimes maybe the understanding wasn't as complete as I wanted it to be. It was in the early phase too. I'm pretty sure, if you talk to them now, the situation would be different.

Ok. Interesting. How would you define lobbying in your words?

I have seen lobbying from all angles. I was lobbied many times, and I lobbied. And I look at it from a completely objective angle. Lobbying for me is explaining why a particular issue is relevant for a particular entity. Either the entity is a company or it is an institution or an organisation. I don't differentiate. Everybody needs to explain why something in particular is relevant or important for this particular entity. And for a policy maker when designing a law, you look at the law from a legal and a political angle, so you design a law and there are many aspects you can get wrong, because the real world that the law will face one day, is much more diverse than you have in mind in the beginning. So you need to have these exchanges and then you fine tune a law. And that is the obligation of a politician to either accept certain opinions or views or to neglect them. So lobbying, I don't have a positive or negative, I just

think it's something, which you need in the architecture in the democratic system. You need to have it. If you don't have it anymore, if somebody believes politicians can handle this in combination with the government on their own and that there needs to be no influence, I don't think that's a way a democratic system can work. It's just not possible. It just doesn't work. You need an understanding of the complexity of the reality. You actually need more proactive outreach as a policymaker to much more diverse backgrounds to understand the implication of a particular law. You typically face the same people, companies and trade organisations and you overlook those who can come to you because they are too small or don't have enough money. You often overlook their needs and desires because you only focus on particular groups. But that's purely political and not looked at from a company angle.

And just to ask this, maybe you can't answer, but to which degree do you think you at Facebook were able to influence the GDPR?

I don't even remember if my colleagues really tried to influence it in the traditional lobbying sense of understanding influencing. Which is really that you want to see this particular law change or this particular paragraph or aspect changed. I would have to reflect upon this much more to give you a really precise answer.

I'm looking into your recommendations documents right now. And looking at your recommendations to changes in the GDPR and there are some...

Exactly, that's what I would want to look into. Tell me, if you have it in front of you.

I'm noticing points about children rights.

The age limit. I think at the time there was a dispute about setting the age lower.

Yes, and then you have a lot of focus on processor vs. controller and that there should be different rights.

Yeah, this was because all of these companies, but again I would ahve to look back, just keep this as a very first exchange on this topic. I believe there was this time the question that if you sit in Ireland and you have to send a lot of data to the US, so it was the question not just about the privacy shield and they way data is handled, but who is actually the controller and who is the processor. Yeah, that's true.

And what you were aiming for was that Ireland should merely be a controller and the US should a processor?

Yeah, I believe this was the discussion at the time, or at least the US would be both. You can be a joint controller and processor too. The US would obviously have to be both and I believe this was the discussion but Ireland indeed couldn't definitely handle both things. We looked at it from legal angle.

And then you were also worried about the Commission's power, it seems with regard to have judicial power.

I believe this related at the time, I don't know when any longer, I believe it related to that there was kinds of executive functions in the Commission without Parliament oversight and there was general concern in companies about i. Not about the quality or the capability which is always highly regarded in the Commission of course, but mostly regarding the system. Because system, that's another thing that is sometimes misjudged. For companies it is always important that you have a really true democratic system in place and as soon there is kind of inbalance in the system, like politicians tend to get nervous, companies tend to get nervous too, but I don't think its relevant for the debate at all.

OK. But you must have had a feeling of which impact you had on the actual legislation. I don't know if you're doing evaluations inside the organisation...?

Again because I didn't do it, I mean that's something you should ask the team who is really dealing with this in Ireland, because already then at the time they had the oversight. I can talk to them and can check if they are willing to talk to you about it. I can't promise they will but I can promise you I will talk to them. I'm not aware that we have done an analysis about it. But I can be completely wrong.

Good. Thank you for participating and thank you for taking the time

Sure. Take good care.

You too, bye.

Interviewee D

An independent expert in information technology lobbying

In your own words, define "lobbying"

Lobbying is the communication of the current interests of businesses or individuals to political decision-makers, with a view to having these interests considered or prioritised by decision-makers.

What are politicians' interests when meeting with lobbyists?

This is very varied. The interest can be a. to be able to say that all stakeholders were met/taken into account, b. to learn how to prioritise the interests of a particular industry or company, for example if the politician sees a personal or broader strategic interest in helping that industry or company c. to gather information to help better oppose the interests of a particular industry/company and/or pass on details of the lobbying to other parts of industry.

Which European institutions were lobbied most extensively with regards to GDPR?

It is difficult to tell... it depends in part if you consider national-level lobbying to be lobbying of the Council or Commission or both. They were all very extensively lobbied.

In your opinion, was GDPR weakened or strengthened as a result of the lobbying process?

Weakened.

In your experience, what were the strategies of Facebook during the lobbying process?

Facebook wanted the weakest GDPR possible, ideally a very long and complex Regulation that ultimately had no teeth, but which, due to its complexity, gave it a relative advantage over other businesses operating in its multiple fields of interest.

Did Facebook lobby independently, in coalition or both?

Both. Although Facebook became less and less visible as the process moved forward.

Is there a difference when lobbying in coalitions, in your opinion?

Yes. Lobbying via coalitions is less subtle and more aggressive, because companies are rarely if ever held accountable for what is done in their name. It is hard to make a strong political case by shouting "look, Facebook is a member of that trade association that is a member of that coalition that is demanding an end to data protection", for example.

Which parts of the GDPR did Facebook lobby primarily?

I don't have any evidence but, at the beginning, when Facebook as at its most visible, the lobbying focussed on the essence of data protection, seeking to undermine the definitions and legal grounds for data processing.

What kind of information/arguments did Facebook's representatives bring to the table when lobbying?

The only ones that I saw myself were a. they argued that they were an SME in most European countries and their interests were aligned with those of SMEs, when they called for "simplification" (=overcomplication) of the legislation and 2. that profiling is simply misunderstood and profiling individuals' personalities to manipulate them commercially was in the individuals' own interests.

How would you rate the credibility and impact of the information/arguments?

The SME argument did not work at all. I heard Billy Hawke , the Irish data protection commissioner at the time, parrot the profiling argument, adding that he had never had a complaint from an individual about this (invisible, untransparent - my words) activity.

To which degree did Facebook influence the final text of GDPR?

I have no idea. See https://edri.org/lobbyplag-eudatap/. Between their lobbying, the lobbying of their trade associations - TechAmerical Europe, Digital Europe, EuroISPA, etc, lobbying by the astroturfing fake think tanks like the "European Privacy Association, it is hard to work out who had what influence

Analysis of Facebook's recommendations to IMCO

In the following analysis I have marked Facebook's succesfully implemented recommendations in blue and Facebook's unsuccessful recommendations in red. In addition, I have corrected the article and recital numbers in order for them to easily be found in the final version of the GDPR.

Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

1. Jurisdiction/One-stop shop/Consistency mechanism

The core principle of a single Data Protection Authority (DPA) having jurisdiction over organisations that operate across multiple European countries is a sensible and positive development in the draft Regulation. The 'one-stop shop' principle has the potential of creating the right incentives for international organisations to establish and invest in Europe. However there are some aspects of the drafting of the draft Regulation which need to be improved if this principle is to be realised. This will in turn provide better protection for European citizens who will be able to seek redress in the European Union (the "EU").

In particular, for citizens and international organisations with a presence in the EU to reap the full benefits of the one-stop shop principle, it must be clear how the law applies in the case of group companies. Where if there is already an EU based controller within a corporate group, that controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority.

Further, many provisions of the draft Regulation undermine the intent of the one-stop shop principle and create legal uncertainty for businesses. These provisions should be revised to maintain the robustness of the changes that are proposed.

<u>Drafting recommendations</u>:

Article 3 (Territorial scope): If there is already an EU-based controller processing the same personal data as a non-EU based controller within a corporate group, the EU-based controller should be responsible for compliance in respect of the relevant data processing (as per Article 3(1)).

As further explained in section 4 "profiling" of this document, the draft Regulation as it is currently worded is set to apply to non-EU controllers when the processing relates to the 'monitoring of an individual's behaviour'. It is our view that the express reference to 'monitoring' undermines the principle of technology neutrality. *Article 55 (Mutual Assistance):* The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities. We therefore propose:

- deleting the mutual assistance obligations regarding prior authorisations (Article 55(1)) and the ability to take a provisional measure and submit the matter the EDPB where a request for assistance is not actioned within 1 month (Article 55(8) and (9));

- the measures required to reply to a request of another supervisory authority must be "reasonable". Further, requests made by another supervisory authority for general "enforcement measures" should be specifically limited to requests for the communication of any enforcement decision which relates to processing operations that have been proven to be contrary to the Regulation (Article 55(2)).

- the mutual assistance provisions should only apply:

  - where individuals in several member states are likely to be affected by the processing to operations that "produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner" (Article 55(1));

  - unless complying with request for assistance would "involve disproportionate effort" (Article 55(4)(b)).

Article 58 (Consistency Mechanism - Opinion by the European Data Protection Board): The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and damaging bureaucratisation of the decision making process by the data protection authorities.

Drafting suggestions:

Recital 27 The main establishment of a controller or a processor in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.	Recital 27 36 in final regulation The main establishment of a controller ~~*or a processor*~~ in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. ***The main establishment of the processor should be the place of its central administration in the Union.***

Justification Retain the European Commission's text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

Recital 97 (EC proposal) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	Recital 97 124 Where the processing of personal data ~~*in the context of the activities of an establishment of a controller or a processor in the Union*~~ takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.
Justification The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.	

Recital 105 In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing	Recital 105 In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where ~~*a*~~ ***the competent*** supervisory authority intends to take a measure as

operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring ***of*** such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism***. Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion***. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	regards processing operations that are related to ***the fundamental rights and freedoms of a data subject*** ~~*the offering of goods or services to data subjects in several Member States, or to the monitoring of such data subjects*~~, or that might substantially affect the free flow of personal data. It should also apply where ***those factors are present and*** any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.
Justification The consistency mechanism should only apply in limited circumstances (and where there is a substantial public interest) to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism, the ability of the Commission to launch it, and the process to be followed need to be carefully worded so that they can reflect the practical viability and resources required. References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51. Further, the express reference to 'monitoring' violates the principle of technology neutrality. In any event, any adverse effects to the data subject that may result from the 'monitoring of an individual's behavior' are already adequately protected by the provisions of this regulation.	

Recital 108 (EC proposal) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified	Recital 108 116 There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, ~~*a*~~ ***the competent*** supervisory authority should be able to adopt provisional measures with a

period of validity when applying the consistency mechanism	specified period of validity when applying the consistency mechanism.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 109 (EC proposal) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	Recital 109 The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by ~~*a*~~ ***the competent*** supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 111 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. ***If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed***	Recital 111 141 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. ~~*If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed.*~~
Justification Retain the European Commission's text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that	

opinion. Such powers should ultimately lie with the courts, not the EDPB.

Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established***, or before the European Data Protection Board on grounds of inconsistency with the application of the present Regulation in other Member States***	Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established***.***
Justification Retain the European Commission's text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that opinion. Such powers should ultimately lie with the courts, not the EDPB.	

Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods ***and*** services to such data subjects in the Union***, including services provided without financial costs to the individual, or;*** (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place	Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to~~:~~ ~~*(a)*~~ the offering of goods ***or*** services to such data subjects in the Union~~; or~~ ~~(b) the monitoring of their behaviour~~ ***except where the processing of personal data is carried out by a controller within the same corporate group of a controller to which paragraph 1 applies.***

where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law..
Justification The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller. Any adverse effects to the data subject that may result from the 'monitoring of an individual's behavior' is adequately covered by the provisions of this regulation. It is unclear why an express reference to this should be made under the territorial scope provisions – such reference could jeopardise the technologically neutral nature of the proposal.	

Article 4(1)(13) 'main establishment' means ***the place where*** the controller ***or the processor has*** its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller ***or a processor*** in the Union take place.	Article 4(1)(13) 16 'main establishment' means ***as regards*** ~~***the place where***~~ the controller, ***the place of*** ~~***or the processor has***~~ its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller ~~***or a processor***~~ in the Union take place. ***As regards the processor, 'main establishment' means the place of its central administration in the Union;***
Justification	

Retain the European Commission's text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

	Article 4(1)(20)new ***'competent supervisory authority' means the supervisory authority of the controller in accordance with the Article 51(2) &(3)***
Justification 'Competent supervisory authority' should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further, the reference to 'competent' reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.	

Article 51 (EC proposal) 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	Article 51 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller ~~*or a processor*~~ in the Union, ***and the activities of a controller within the same corporate group not established in the Union or where*** the controller ~~or processor~~ is established in more than one Member State, the supervisory authority of the main establishment of the controller ~~or processor~~ shall be competent for the supervision of the processing activities ~~*of the controller or the processor in all Member States, without prejudice to*~~ the provisions of Chapter VII of this Regulation. ***All references to the competent supervisory authority shall be***

	interpreted in accordance with this Article 51(2).
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	4. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Justification

The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.

'Competent supervisory authority should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further. the reference to competent reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.

Processors should not be subject to the same administrative obligations and regulatory scrutiny as controllers as per our position in relation to Recital 65 / Article 28 (Documentation) / Article 9.

Article 55 (EC proposal)	Article 55 61
1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data	1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out ~~*prior authorisations and*~~ consultations, inspections and prompt information on the opening of cases and ensuing developments where data

subjects in several Member States are likely to be affected by processing operations.	subjects in several Member States are likely to be affected by processing operations ***that produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner;***
2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.	2. Each supervisory authority shall take all ~~*appropriate*~~ ***reasonable*** measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or ~~*enforcement measures*~~ ***communicating any enforcement decision taken*** to bring about the cessation or prohibition of processing operations ***that have been proven*** contrary to this Regulation.
3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.	3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.
4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation.	4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation ***or would involve disproportionate effort.***
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.
	6. Supervisory authorities shall supply the

6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format. 7. No fee shall be charged for any action taken following a request for mutual assistance. 8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57. 9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission. 10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format. 7. No fee shall be charged for any action taken following a request for mutual assistance. ~~*8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.*~~ ~~*9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.*~~ 10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
Justification The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.	

Article 58 (EC proposal)	Article 58 64
1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.	1. Before ~~a~~ ***the competent*** supervisory authority adopts a measure referred to in paragraph 2, this ***competent*** supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.
2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:	2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects ***concerning the fundamental rights and freedoms of a data subject*** and which:
(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or	(a) relates to processing activities which are ***likely to produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect the individual in a significantly negative manner*** ~~*related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour*~~; or
(b) may substantially affect the free movement of personal data within the Union; or	(b) may substantially affect the free movement of personal data within the Union; or
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or	~~*(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or*~~
(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or	~~*(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or*~~
(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or	~~*(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or*~~
(f) aims to approve binding corporate rules within the meaning of Article 43.	(f) aims to approve binding corporate rules within the meaning of Article 43.
3. Any supervisory authority or the	3. Any supervisory authority or the

European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.	European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism~~, *in particular*~~ where ~~*a*~~ ***the competent*** supervisory authority does not submit a draft measure referred to in paragraph 2 ~~*or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.*~~
4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.	4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter ***related to the category of measures referred to in paragraph 2*** shall be dealt with in the consistency mechanism.
5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.	5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.
6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.	6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The	7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The

opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public. 8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.	opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the ***competent*** supervisory authority ~~*competent under Article 51*~~ of the opinion and make it public. 8. ~~*The supervisory authority referred to in paragraph 1 and t*~~***T***he ***competent*** supervisory authority ~~*competent under Article 51*~~ shall take ***utmost*** account of***, but not be bound by,*** the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.
Justification The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism (paragraph 2), the ability of the Commission to launch it (paragraph 4), and the process to be followed (paragraphs 7 and 8) need to be carefully worded so that they can reflect the practical viability and resources required. With regard to the process to be followed, experience shows that despite their best efforts, supervisory authorities are not organized and resourced in a way that allows them to meet strict timeframes. Therefore, it is very likely that the timeframes set out will be routinely missed and, as a result, any decisions or measures subject to the consistency mechanism will be unnecessarily and unjustifiably delayed. In view of this, the consistency mechanism should only be engaged in a minority of situations and where there is a substantial public interest.	

Article 59 (EC proposal)	Article 59

1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.	1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.
2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.	2. Where the Commission has adopted an opinion in accordance with paragraph 1, the ***competent*** supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.
3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.	3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.
4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.	4. Where the ***competent*** supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Article 60 (EC proposal) 1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned	***delete***

decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to: (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or (b) adopt a measure pursuant to point (a) of Article 62(1). 2. The Commission shall specify the duration of the suspension which shall not exceed 12 months. 3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.	

Justification

The power granted to the European Commission to adopt interpretive opinions and draft measures undermines the principle of independent data protection supervision. Such powers should lie with the data protection supervisory authorities and ultimately the courts, not the Commission. Where an issue arises in relation to an opinion or draft measure issued by the European Data Protection Board (under Article 58) this would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.

Article 61 (EC proposal)	Article 61
1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the	1. In exceptional circumstances, where ~~a~~ ***the competent*** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way

procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The ***competent*** supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.	2. Where a ***competent*** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion ***of the European Data Protection Board*** where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.
4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51. The specific reference to the European Data Protection Board creates certainty about the relevant body that the Supervisory authority can submit a request for an urgent opinion to.	

Article 63 (EC proposal)	Article 63
1. For the purposes of this Regulation, an enforceable measure of the supervisory	1. For the purposes of this Regulation, an enforceable measure of the ***competent***

authority of one Member State shall be enforced in all Member States concerned. 2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.	supervisory authority of one Member State shall be enforced in all Member States concerned. 2. Where a ***competent*** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the ***competent*** supervisory authority shall not be legally valid and enforceable.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Article 63a new Appealing procedures Without prejudice to the competences of the judiciary system of the Member States and of the Union, the European Data Protection Board can issue binding opinions if: (a) a data subject or data controller appeals on ground of inconsistent application of the present Regulation across the Member States and (b) the Consistency Mechanism described in Article 58 to 63 has failed to ensure that a simple majority of the members of the European Data Protection Board agrees on a measure. Before issuing such opinion, the European Data Protection Board shall take into consideration every information the competent Data Protection Authority knows, including the point of view of the interested parties.	***delete***
Justification The EDPB should not be granted the power to adopt binding opinions. The primary function of interpreting the law should lie with the data protection supervisory authorities and ultimately the European Court of Justice whose primary function is to	

interpret the law.

Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 ***and in Article 63a***;	Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 ~~***and in Article 63a***~~;
Justification This amendment relates to the proposed new Article 63(a) above.	

Article 73(2) Any body, organisation or association which aims to protect ***citizens***' rights and interests shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	Article 73(2) 80 Any body, organisation or association which aims to protect ***data subjects***' ~~*citizens'*~~ rights and interests ***concerning the protection of their personal data and has been properly constituted according to the law of a Member State*** shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.
Justification The reference to 'citizen' rights' is inconsistent with the draft Regulation which refers to 'data subjects' throughout. Further, it creates a suggestion that consumer organisations or claim foundations could bundle claims of consumers and class action could be used by some as a mechanism to litigate against corporate groups. The potential scale of such collective actions, time, cost and outcome - on top of penalties - might have severe financial implications for companies. The effect of this judicial remedy would be disproportionate to the aims of deterrence and effective enforcement of the data protection provisions in the proposed Regulation.	

2. Consent

Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the highly prescriptive nature of the requirements for consent contained in Articles 4(8) and 7(2) could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk

of inundating users with tick boxes and warnings and may result in an overly disrupted or disjointed internet experience. This will inevitably lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. It may also prevent organisations from being innovative about the way they interact with individuals.

Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given".

It is important to keep in mind that there are many services, such as social networks, which are expressly designed for people to be able to connect and share information.

A great amount of privacy best practice has been developed, especially in the online environment, to provide users with transparency and control. We are seeing great innovation (including granular and sophisticated control tools) from many players in the market to empower users to understand how their information is used and how services work when they choose to share information online. Equally many internet players are incorporating 'privacy by design' into their privacy programmes. These practices must not be hampered by over-prescriptive and often meaningless consent requirements.

Drafting recommendations:

32 4 (11)

Recital 25, Article 4(8) (Definition of Consent): The reference "explicit" in the definition of consent is counterproductive and unrealistic in the majority of processing situations. We therefore propose that the reference that consent must be given "explicitly" and "silence and inactivity should not constitute consent" should be deleted from Recital 25. We have suggested language that makes clear that "other conduct that leads to an unmistakable conclusion that consent is given" is valid consent. We also recommend that there should be some flexibility in the way that this is provided i.e. "either by a statement or by a clear affirmative action or by any other method" (see Recital 25 and the definition of Consent contained in Article 4(8)).

The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. Therefore, we propose adding wording to Article 4(8) to state that the information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (as contained in Article 5).

Article 7 (Conditions for Consent): We propose that:

- The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data. This position is reflected in the proposed changes to Article 7(1).

- The Regulation shall provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. This position is reflected in the proposed changes to Recital 32 and Article 7(2).

- Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. We have therefore suggested that the controller shall be entitled to suspend or terminate services where such provision of services relies on consent to the processing which has been withdrawn by the individual (see Article 7(3)).

- Controllers should be able to make consent to the processing a condition of access to a service which may not be otherwise free. This position is reflected in our amendments to Recital 34 and Article 7(4).

Drafting suggestions:

Recital 25 (EC proposal)	Recital 25
Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is	Consent should be given ~~*explicitly*~~ by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement ~~*or*~~ by a clear affirmative action by the data subject, ***by taking some other conduct that leads to an unmistakable conclusion that consent is given***, ensuring that individuals are aware that they give their consent to the processing of personal data ~~*including by ticking a box.*~~ ***Consent may be given*** by taking an action when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. ~~*Silence or inactivity should therefore not constitute consent*~~. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request

32

provided.	must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Justification

Unambiguous consent shall be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given".

Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the proposed requirement for consent may lead to an overly disrupted or disjoined internet experience and may also prevent organisations from being innovative about the way they interact with individuals.

The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it.

Furthermore, controllers should be allowed some technical flexibility as to the way that data subjects' consent is obtained.

Recital 32 (EC proposal) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.	Recital 32 Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given, ***including by identifying and explaining the relevant data processing activities in a data protection statement or privacy policy***

	made available to the data subject at the time of obtaining his or her consent.

Justification

The draft Regulation should provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. It should also allow controllers to define the most appropriate channel and level of information to be provided to data subjects for each processing activity. The information to be provided for the purposes of obtaining the data subject's consent shall be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (considered below in the justification for the proposed changes to Article 4(8)).

Recital 34 (EC proposal)	Recital 34 43
Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. ***However, a data controller may legitimately make consent to the processing a condition of access to a service, particularly when the service is free of charge to the data subject.*** Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Justification

Controllers should be able to make consent to the processing a condition of access to a

service which may not be otherwise free. See also the proposed changes to Article 7(4).

Article 4(8) (EC proposal)	Article 4(8)
'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	'the data subject's consent' means any freely given specific, informed and ~~*explicit*~~ ***unambiguous*** indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action ***or by any other method***, signifies agreement to personal data relating to them being processed. ***The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with Article 5;***
Justification Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given". The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles under Article 5.	

Article 7 (EC proposal)	Article 7
1. The controller shall bear the burden of	1. ***For the purposes of Article 9(2)(a), t***he

proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. ***The data subject's consent may be exercised by a single step provided that all relevant matters to which the consent relates are made clearly available.*** 3. The data subject shall have the right to withdraw his or her consent at any time ***and the data controller shall be entitled to suspend or terminate the provision of services to the data subject where such provision relies on the consent to the processing withdrawn by the data subject.*** The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller, ***except where consent to the processing may legitimately constitute a condition of access to a service by the data subject.***
Justification The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data. Controllers should be entitled to obtain consent for a range of data processing activity in a single step as long as they provide them the appropriate level of information for each processing activity. Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. The controller shall be entitled to suspend or terminate	

services where such provision of services relies on consent to the processing which has been withdrawn by the individual.

Controllers should also be able to make consent to the processing a condition of access to a service which may not be otherwise free.

3. Right to be forgotten

The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However, the right to be forgotten needs very careful consideration. As drafted, apart from not harmonising national laws, it raises major concerns with regard to the right of others to remember and of freedom of expression. There is also a risk that it could result in measures which are technically impossible to apply in practice and therefore make for bad law. A right balance should be found between data subject's right to get their data deleted, the fundamental rights of other individuals and the reality of the online environment. The proposal prescribes a right for people to have their data deleted and also requires data controllers to take all reasonable steps to obtain erasure of content copied to a third party website or application.

It is important to differentiate between three challenges presented by the 'right to be forgotten':

The *first* is in relation to people who have posted personal information about themselves online and later wish to delete that information.

The *second* is in relation to the practical difficulty to identify the necessary information to ensure compliance with the right to be forgotten. This challenge arises in two specific situations:

- The first situation concerns the deletion of personal data of an individual made available online by another individual. In practice, the operator of a website or hosting platform is unlikely to know in many cases which information available on the platform constitutes the personal data that should be deleted. It is virtually impossible to control what information millions of users may make available about other individuals – many of whom will not be users themselves – and to determine where all of the information is and whether that information is the personal data of the person making the request. Therefore a broad obligation to delete any information made available by users upon request of other individuals would be likely to present major implementation challenges to the extent that it would be practically unworkable.

- The second situation concerns the specific provision under Article 17(2), which requires informing third parties of the request for deletion of links to or copies of

an individual's personal data. This would involve identifying any such links or copies of the information elsewhere on the Internet and communicating with those responsible for placing the links or copying the information to request such links or information to be deleted. Again, we do not see any practicable means for services like social networking to control which links to or copies of someone's personal data exist in other places on the Internet, let alone communicate with the third parties responsible for their dissemination.

In order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the Internet. There is concern in the Internet community that it could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

The *third* is in relation to any personal data made publicly available and the fact that there may be strong grounds to justify under certain circumstances the right of others to know certain facts concerning individuals, as this is closely linked to the right to freedom of expression and other democratic values. It is clear that there is a potential conflict between the right for people to express themselves and the privacy rights of others. It is important to consider fully the implications on the open Internet and personal expression as we determine the right balance. The scope of freedom of expression contained in Article 80 and further clarified in Recital 121 is defined quite narrowly and should be extended to cover for example mere expressions of opinion, user generated content and more generally recognise the nature of new forms of communication such as blogging and social networking.

Finally, the debate on the "right to be forgotten" affects a number of Internet services, which rely on user-generated content. This issue is not unique to social networking. Policy makers should take into account the "right of others to remember" and reach a balanced conclusion which respects freedom of expression.

<u>Drafting recommendations</u>:

Recital 53 / Article 17 (Right to be forgotten and to erasure): The right to erasure in Article 17(1) is welcome, but the wording should be amended to ensure that it balances the competing interests set out above As such, we propose that:

- Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data. Therefore we have suggested that the right of an individual to require erasure when it is 'impossible or involves a disproportionate effort' (Article 17(1)(e)).

- The right of erasure may be overridden by the interests or fundamental rights and freedoms of others (Article 17(1)(f) and Recital 53).

- The right to be forgotten, as drafted, raises major concerns with regard both to the right of others to remember and to freedom of expression. Moreover, it is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms. We therefore resist the wording contained in Article 17(2) and Recital 54.

- An exemption should apply when a controller wishes to process the information for a certain legitimate purpose (such as the provision of system, network or information security). This position should be limited to circumstances where the interests of the controller are not outweighed by those of the individual and we have therefore proposed changes to Recital 53 in this regard.

Drafting suggestions:

Recital 53 Any person should have the right to have personal data concerning them rectified and ***the*** right to ***have such personal data erased*** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be	Recital 53 65 Any person should have the right to have personal data concerning them rectified the right to have such personal data erased where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. ~~*This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.*~~ However, ***certain exemptions should apply, particularly when***

allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	***identifying all relevant personal data in question proves impossible or involves a disproportionate effort and when in relation to personal data made publicly available by the data subject himself or herself, such right is overridden by the interests or fundamental rights and freedoms of others. An exemption should also apply to enable the data controller to process data for their legitimate interest, as for instance for the purpose of providing system, network or information security.*** ~~*and*~~ ***T***he further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

Justification

The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However, certain exemptions should apply to recognise that:

- Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data;
- Where an individual makes information their information publicly available, there is a potential conflict between the right of others to know and the right of others to remember (including where the data subject has given their consent as a child);
- The right to know is closely linked to the right to freedom of expression and other democratic values; and
- An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security.

Recital 54 66 To strengthen the right to ***erasure*** in the online environment, ***such*** right should also be extended in such a way that a	***delete***

controller who has ***transferred*** the personal data ***or made them*** public ***without being instructed to do so by the data subject*** should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.	
Justification It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms. Furthermore, these provisions might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.	

Article 6 (EC proposal)	Article 6
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take

steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of	steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. ***The processing of data to the extent necessary for the purpose of providing system, network or information security constitutes a legitimate interest of the data controller.*** 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) ***a legally binding obligation*** to

the right to the protection of personal data and be proportionate to the legitimate aim pursued. 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	which ***a*** controller is subject. The ***legally binding obligation*** must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.
Justification An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security.	

Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 ***is extended*** to each recipient to whom the data have been disclosed ***without the control of the data subject***.	Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 ***is extended*** to each recipient to whom the data have been disclosed ***without the control of the data subject, unless this proves impossible or involves a disproportionate effort***.
Justification Retain the European Commission's proposal to the extent that this obligation should not apply where compliance would be impossible or involve a disproportionate effort in addition to the language proposed by the rapporteur.	

Article 17 – Right to ***erasure***	Article 17 – Right to erasure
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ~~*especially in relation to personal data which are made available by the data subject while he or she was a child,*~~ where one of the following grounds applies:
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;	(c) the data subject objects to the processing of personal data pursuant to Article 19;
(d) the processing of the data does not comply with this Regulation for other reasons.	(d) the processing of the data does not comply with this Regulation for other reasons.
	except where:
	(e) identifying all relevant personal data in question proves impossible or involves a disproportionate effort;
	(f) such right is overridden by the interests or fundamental rights and freedoms of others.
2. Where the controller referred to in paragraph 1 has ***transferred*** the personal data***, or has made such data*** public ***without being clearly instructed by the data subject to do so***, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data	~~*2. Where the controller referred to in paragraph 1 has transferred the personal data, or has made such data public without being clearly instructed by the data subject to do so, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to,*~~

subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication. 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit	~~*or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*~~ 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit the personal data into another automated

the personal data into another automated processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. 9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. ~~*9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:*~~ ~~*(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;*~~ ~~*(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;*~~ ~~*(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.*~~
Justification The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft	

Regulation. The right to erasure in Article 17(1) should be reviewed to recognize that the right balance is struck between the rights of a data subject to get their data deleted, the rights of individuals to remember and the right to freedom of expression. The practical difficulties associated with identifying the necessary information to ensure compliance with this provision must also be taken into account. Certain exemptions should apply to recognise that:

- It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online);
- The right of erasure may be overridden by the interests or fundamental rights and freedoms of others;
- An exemption should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security

Moreover, the right to be forgotten in Article 17(2) needs very careful consideration. It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, this provision might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

For the reasons above and because the right to erasure is sufficient to give data subjects control over their personal data, Article 17(2) should be deleted.

4. Profiling

The specific provisions on "profiling" contained in the draft Regulation are unnecessary, over-broad, and legally vague. Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.

Article 20 extends the scope of the 95/46/EC Directive provisions relating to automated individual decisions to cover a range of new factors including location, personal preferences and behaviour. It also introduces a new and undefined test of "significant effect". Failure to adequately distinguish between processing with legal or significant effect and content customization could indiscriminately subject a potentially enormous range of activity (and yet-to-be-invented applications) across every industry sector to the stricter consent provisions of Article 7 and the provisions relating to prior authorization as defined in Article 33 and 34. As well as being burdensome on data protection authorities, this fails to strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce. Customization is an essential element in a competitive online marketplace, and such broadly-framed provisions are likely to have unintended consequences and affect many legitimate practices in the process negatively.

Measures on profiling do not distinguish between the technology and its use. The current drafting of the Regulation shows that there is no recognition of positive uses of profiling and no differentiation is made between the technology and its uses. Article 20 clearly violates the principle of technology neutrality which is alluded to in Recital 13, and which is critically important in crafting future-proof regulation. Given the numerous other safeguards in this draft Regulation, profiling techniques do not need be treated differently to any other type of personal data processing.

The legitimate interests of the data controller should provide a legal basis for "profiling". The legitimate interests pursued by a controller should be an additional legal ground for lawful profiling, along with consent, in order to ensure that profiling techniques and technologies that do not aim at identifying data subjects but at extracting aggregate baseline data that can be used to manage, improve or customize services for similar customers are not prohibited under the draft Regulation. It is important that this be the case here as with other sections of the draft Regulation, to ensure that the use of profiling techniques for legitimate purposes such as security, anti-fraud, accounting are not prohibited**.**

<u>Drafting recommendations</u>:

Recital 51 / Recital 58 / Recital 59 / Article 20 (Measures based on Profiling): Prohibiting or severely restricting profiling is not adequate for a technique that is enabled by various technologies, is used across sectors for various purposes and, whilst potentially presenting risks in certain cases, also has benefits for consumers, business and the economy.

Recital 13 recognises that, in order to avoid a serious risk of circumvention, "the protection of individuals should be technologically neutral and not depend on the techniques used". Article 20 clearly violates this principle of technology neutrality, which should be core to any laws that deal with technology if they are to withstand the test of time and technology evolution.

Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.

Therefore, it is proposed that Recital 51, Recital 58 and Article 20 be entirely deleted, as well as a reference in Recital 59.

Drafting suggestions:

Recital 51 (EC proposal) 63 Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	***delete***
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Recital 58 71 Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be ***forbidden only*** when expressly ***stated*** by law, ***not*** carried out in the course of entering or performance of a contract, or when the data subject has ***withdrawn*** his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child. ***The data subject, when this profiling is not necessary for entering or performing a contract, should always have the possibility to opt-out.***	***delete***
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Recital 59 (EC proposal) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of	Recital 59 73 Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, ~~*measures based on profiling*~~, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of

human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Article 20 22 ~~*1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.*~~	***delete***

2. Subject to the other provisions of this Regulation, a ***measure which produces legal effects on a*** person ***or significantly affects this person, based solely on automated processing intended to evaluate certain personal aspects relating to this person or to analyse or predict in particular the person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour, is lawful*** only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 ***in Article 15 and Article 16***. 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9. 4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. 5. The Commission shall be empowered to	

adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	

Justification

Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size -fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.
Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.

5. Controller/Processor

The concepts of data processor and data controller have been appropriately defined in the existing data protection legislation (i.e. Directive 95/46/EC). In the draft Regulation, the concept of data processor is not clearly defined and, as a result, there may be situations where a data processor may unjustifiably be regarded as a data controller. For example, under Article 26(4), if a processor is considered to be taking independent decisions then that processor will be deemed as a controller. In practice, the interaction between the two concepts might raise practical difficulties when a data controller and a data processor are part of the same company group and both parts of the group collaborate on a daily basis. The policies and protocols will be defined by the data controller, but often implemented independently by the data processor.

Drafting recommendations:

Recital 62 / Article 4(5) (Definition of Controller) / Article 4(6) (Definition of Processor) / Article 24 (Joint Controllers) / Article 26 (Processor): Proposals regarding the definition of the data controller need to be narrowed down to ensure that organisations can operate efficiently with legal certainty. The definition of data processor should also be modified to allow certain elements of co-decision-making.

Article 22 (Responsibility of the Controller): This provision introduces new accountability provisions on controllers. These include requirements to demonstrate compliance with the draft Regulation through the adoption of internal policies, assignment of internal responsibilities and verification of compliance. Even though these provisions are sound, there may be some difficulty in situations where the level of prescription in the draft Regulation is such that they may not reflect practices that are otherwise appropriate to safeguard personal data. To this end the Article would requires further consideration.

Recital 65 / Article 28 (Documentation) / Article 9 (Co-operation with the supervisory authority): Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome. We have therefore suggested that the obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) and co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.

Drafting suggestions:

Recital 62 (EC proposal) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	Recital 62 79 The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes ~~*conditions and*~~ means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

Recital 65 (EC proposal) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	Recital 65 82 In order to demonstrate compliance with this Regulation, the controller ~~*or processor*~~ should document each processing operation. ~~*Each*~~ ***The*** controller ~~*and processor*~~ should be obliged to co-operate with the ***competent*** supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.
Justification	

Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome.

Article 4(5) (EC proposal)	Article 4(5)
'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes~~,~~ ***~~conditions~~*** and means of the processing of personal data; where the purposes~~,~~ ***~~conditions~~*** and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

Article 4(6) (EC proposal)	Article 4(6)
'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	'processor' means a natural or legal person, public authority, agency or any other body which processes personal data, ***including making decisions with regard to the processing,*** on behalf of the controller;
Justification The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller.	

Article 15(d)	Article 15(d)
the period for which the personal data will be stored ***and the time of collection***;	the period for which the personal data will be stored ***~~and the time of collection;~~***

Justification Retain the European Commission's proposal. The obligation added by the rapporteur has the potential of being administratively burdensome for the controller.

Article 22 The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	Article 22 24 The controller shall adopt policies and implement appropriate ***and reasonable*** measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. ***For the purpose of this Regulation, appropriate and reasonable measures will mean measures that are proportional to the risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology.*** 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the ***competent*** supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms ~~*to ensure*~~ ***for*** the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.
Justification	

The obligations on controllers to adopt policies and appropriate measures should be clear. Such policies and measures should be "appropriate and reasonable" and proportional to the "risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology".

Article 24 Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***Where such determination is lacking or is not sufficiently clear, the data subject can exercise his rights with any of the controllers and they shall be equally liable.***	Article 24 26 Where a controller determines the purposes~~, *conditions*~~ and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

Article 26 1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the	Article 26 28 1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the

processing to be carried out and shall ensure compliance with those measures. 2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited; (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; (c) take all required measures pursuant to Article 30; (d) enlist another processor only with the prior permission of the controller; (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise; (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article. 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	processing to be carried out and shall ensure compliance with those measures. 2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited; (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; (c) take all required measures pursuant to Article 30; (d) ~~*enlist another processor only with the prior permission of the controller;*~~ ***not conflict with the instructions given by the controller when enlisting another processor;*** (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles ~~*30*~~ ***29*** to 34; (g) ~~*hand over all results to the controller after the end of the processing and not process the personal data otherwise;*~~ ***not process the personal data further after the end of the agreed processing;*** (h) make available to the controller ~~*and the supervisory authority*~~ all information necessary to control compliance with the obligations laid down in this Article. 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

Justification

The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller. In particular:

Processors should be able to enlist sub-processors that enable the requirements of the Regulation to be met (rather than only with the prior permission of the controller (Article 26(2)(d)).

Processors should not be able to process personal data after the end of the agreed processing (rather than being required to hand over all results to the controller after the end of the processing and not process the personal data otherwise (Article 26(2)(g).

Processors should provide information to the controller necessary to control compliance with the obligations laid down in the Article but not to the supervisory authority (Article 26(2)(h)).

Article 28 1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data	Article 28 1. Each controller ~~*and processor*~~ and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data

subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3). 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority ***and, in an electronic format, to the data subject***. 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation that is processing personal data only as an activity ancillary to its main activities. 6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3). 3. The controller ~~***and the processor***~~ and, if any, the controller's representative, shall make the documentation available, on request, to the ***competent*** supervisory authority. 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers ~~***and processors***~~: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. 6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
Justification Processors should not be subject to the same administrative obligations as controllers. The administrative processor related obligations to keep the same documentation as	

controllers is unduly burdensome. The obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) should not extend to processors. References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51).

Article 29 (EC proposal) 1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph. 2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	Article 29 1. The controller ~~***and the processor***~~ and, if any, the representative of the controller, shall co-operate, on request, with the ***competent*** supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph. 2. In response to the ***competent*** supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the ***competent*** supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the ***competent*** supervisory authority.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51). Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers is unduly burdensome. Therefore the obligations placed on controllers as regards co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.	

International Transfers

Article 41(2)(a)	Article 41(2)(a)

the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, ***jurisprudential precedents*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, ~~*jurisprudential precedents*~~ as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
Justification The European Commission should not be granted the power to give consideration to judicial precedents. This would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.	