Erasmus School of Social and Behavioral Sciences

M.Sc. International Public Management and Policy (IMP) 2019-2020

Interest Group Framing in the European Union: membership representation or institutional appeal?

Master Thesis

Submitted by:

Katharina Sophie Ruppert

550639

Rotterdam, 10 July 2020

Supervisor: Prof. Markus Haverland

Co-reader: Dr. Asya Zhelyazkova

Word count: 19,994

Abstract

This research starts from the observation that the study of interest groups and in particular of interest group framing remain a niche within political science although it is central to understanding the functioning of advanced democracies. By strategically highlighting some aspect of a policy proposal while omitting others, interest groups frame it. This study examines the extent to which different types of interest groups and European institutions affect the frame selection by interest groups when lobbying. This case study is based on the ePrivacy regulation. The 'two logics of interest groups', developed by Klüver, Mahoney and Opper (2015), serve as the theoretical basis. They postulate that the organizational structure of interest groups as well as the characteristics of the EU institution that has been lobbied, influence interest group's frame selection. Three types of interest groups, namely sectional groups, cause groups, and firms are subject to the analysis. They do not only represent different interests (private versus public interests) but they also possess different organizational structures. While scholars commonly approach the topic of framing quantitatively, this study takes a qualitative approach. It therefore overcomes underlying methodological obstacles and adds clear value to the existing literature. A dual approach of hand-coding and computer-assisted qualitative content analysis through the software MAXQDA allows to gain a detailed insight into the selected policy proposal, namely the ePrivacy regulation. This research revealed that frame choice varies systematically across the types of interest groups. Additionally, the findings also suggest that frame choice is not necessarily affected by the institutional characteristics of the European Commission and the European Parliament respectively. The narrow focus on studying economic and public frames with regards to the ePrivacy regulation provides room for further research. Extending this study to the Council, selecting another policy area or including other types of frames would allow to enrich the research findings.

Keywords: ePrivacy, European Union, framing, interest group, lobbying

Acknowledgements

I would like to thank my first supervisor Prof. Markus Haverland for professionnally guiding me through the process of writing my master thesis. His profound knowledge and valuable feedback alongside his positive attitude and confidence in my work allowed me to genuinely enjoy the writing process. I would like to thank the members of my thesis working group who contributed to fruitful discussions and shared their points of view with me. Furthermore, I would also like to express my gratitude to my second reader Dr. A.T. Zhelyakova whose detailed comments were of great help to me. I would also like to thank Lena who has accompanied me through this Master program as a great, sincere friend, intelligent and hard-working member of multiple group works and critical reader. Finally, I would like to thank my family for always supporting me. In particular, I would like to thank my sister Marie, who always believed in me and provided me with the supporting and productive environment I needed when Covid 19 made me return earlier than expected to my home country. I would also like to thank my sister Franziska for proofreading my thesis and making me think even more critically about my work.

Table of Contents

List of Figures

List of Tables (Body)

List of Tables (Appendix)

List of abbreviations

BEUC	Bureau Européen des Unions de Consommateurs
CDT	Center for Democracy and Technology
CFR	Charter of Fundamental Rights
CONNECT	Communications Networks, Content and Technology
CON	Congruence analysis
COV	Co-variational analysis
DG	Directorate-General
EC	European Commission
ECHR	European Convention on Human Rights
EDRi	European Digital Rights
EMMA	European Magazine Media Association
ENPA	European Newspaper Publishers' Association
EP	European Parliament
EPC	European Publishers Council
ETNO	European Telecommunications Network Operators
EU	European Union
EuroISPA	European Internet Service Provider Association
GDPR	General Data Protection Regulation
GSMA	Groupe Spéciale Mobile Association
IoT	Internet of Things
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MEP	Member of the Parliament
OTTs	Over-the-Top communication services
TELE WP	Telecommunications and Information Society working party

1. Introduction

1.1. Introduction and research question

The European Union (EU) is a democratic political system, in which non-state actors try to influence decision-makers according to their own interests and beliefs. With the extension of the qualified majority voting in the Council, the European Parliament (EP) received a greater role in decision-making and also became a popular target for lobbyists alongside the European Commission (hereafter Commission). "Because all policies are multi-dimensional, different policy actors focus their attention on different aspects of the policy as they seek to build support for their positions" (Baumgartner & Mahoney, 2008, p.436). In fact, "[l]obbyists are framers" (Baumgartner, 2007, p. 485). They strategically highlight one aspect over another in order to move the final policy outcome towards their own interest (Klüver, Mahoney & Opper, 2015). Through framing lobbyists can play a vital role in public policy debates (Eising, Rasch & Rozbicka, 2015). While research in this area has expanded, it still predominantly focuses on the effect of framing on interest groups' influence or success. It means that most commonly framing is treated as the independent variable and researchers assess to what extent the way interest groups emphazise certain aspects might affect their influence on EU policy-makers or success in moving the final policy outcome towards their own interest. Yet, it is interesting to examine the environment in which interest groups lobby decision-makers. More specifically, which factors might explain variation in frame selection? In the scholarly work, interest groups' characteristics as well as contextual factors have been identified as important factors that affect frame choices. Therefore, these two factors, which are captured by the 'two logics of interest groups', as developed by Klüver, Mahoney and Opper (2015), will provide this study's theoretical ground. Thus, deriving from the 'two logics of interest groups' the following research question has been formulated:

To what extent do the types of interest groups and European institutions affect interest group frame selection when lobbying the ePrivacy regulation?

As the Commission and the EP are the most popular targets of lobbyists, this study focuses on determining interest group frame employment vis-à-vis those two EU institutions. Additionally, the empirical focus of this analysis has been narrowed to the new regulation on privacy and electronic communications (ePrivacy). This regulation has been amongst the most lobbied initiatives in recent years. One of the reasons for the involvement of many interest groups was that many questioned the necessity for a separate legal instrument considering that the newly

revised General Data Protection Regulation (GDPR) already covers personal data independently of the means of transmission (Corporate Europe Observatory, 2018). The European Commission presented its proposal for the ePrivacy regulation in January 2017. In light of the increasingly connected world and the exponential increase in data generated by consumers, private and public entities and even objects (the Internet of Things (IoT)), the existing legal framework on personal data protection did not fit the new environment anymore (European Commission, n.d.). Additionally, while traditional communication channels have become less important, Over-The-Top (OTT)[1] communications services have become essential for today's communication. One of the greatest concerns was to include precisely these channels, as they did not fall under the remit of the previous directive (European Parliament, 2017a).

A qualitative content analysis of interest groups' responses to the Commission's consultation questionnaire, position papers and speakers' notes for the EP's hearing will be conducted. Handcoding will be complemented by using the computer-assisted content-analysis MAXQDA.

1.2. Theoretical and societal relevance

> The concept of 'relevance' (…) comprises two dimensions, a theoretical and a social dimension (…). The theoretical dimension of relevance relates to a project's contribution to a given theoretical discourse and represents social scientists' 'inside' or 'peer perspective', whereas social relevance (…) represents a project's 'outside' perspective and ideally increases citizens' political knowledge and awareness. (Lehnert, Miller & Wonka, 2007, p.23.)

In order to ensure the study's theoretical relevance, the scientific discourse on interest group framing has been analyzed. Only a few scholars have tackled the issue of interest group framing and furthermore concentrated predominantly on assessing the effect of framing on interest group influence as well as success. As this thesis builds on the existing pertinent body of literature on framing, it will strengthen the dialogue of the interest group literature on framing at the level of the EU. Testing similar hypotheses to those formulated by Klüver, Mahoney and Opper (2015) will allow to enrich their findings. More precisely, while their research analyzes interest group framing targeting the Commission only, this study will also take the EP into

[1] "OTTs are services that allow communication which bypasses the traditional content distribution system. They take their name from the way in which communication is ensured, as it goes 'over the internet' without the need for an operator of multiple cable or direct-broadcast satellite television systems." (Kononenko & Parise, 2017, p.1).

consideration, which will ultimately allow to compare interest groups' approach to lobbying different venues. Thus, conclusions about whether and to what extent the use of frames differs between these institutions can also be drawn. Lastly, most of the existing studies apply a quantitative approach. However, researchers studying interest groups framing quantitatively have been confronted with important methodological hurdles including to reliably identify frames (De Bruycker, 2017). Therefore, bselecting a qualitative design will not only complement the existing literature, but also overcomes the limitations of quantitative designs identified in the context of analyzing frames.

The thesis is also of significant societal relevance. According to Lehner, Miller & Wonka "[s]ocially relevant research furthers the understanding of social and political phenomena which affect people and make a difference with regard to an explicitly specified evaluative standard" (2007, p.22.). One of the critical aspects that arose repeatedly in the discussion on EU law-making concerns the question of transparency. With the gradual transfer of regulatory functions from EU member states to EU institutions the number of interest groups increased significantly in the 1990s. They have become an integral part of the EU policy process. As they seek to improve the functioning of the EU and thus the environment in which EU citizens live, they affect many people. Additionally, studying the factors which affect interest groups' frame selection vis-à- vis the Commission and the EP is socially relevant as it furthers EU citizens' understanding of interest groups' strategies to craft a persuasive political argument that helps them influence decision makers.

Furthermore, the topic of ePrivacy has become increasingly important as most communication services use private sensible information involved in the communication (Buttarelli, 2018). Data breach scandals, affecting millions of users, such as the Cambridge Analytica revelations of 2018, have also indicated the seriousness of the issue of ePrivacy and provided further ground why citizens'online privacy protection has become so important to the majority of the European population.

1.3. Research Structure

Chapter 2 provides an overview of the pertinent body of literature on interest groups. Chapter 3 sheds light on the Commission and the EP in the process of lobbying. Chapter 4 introduces the proposed regulation for this study. Chapter 5 outlines the study's theoretical framework and will elaborate on the classification of interest groups and frames. Chapter 6 discusses the research design and methodology. An overview of available research designs will be given to provide the ground for the selection of the appropriate design for this study. Chapter 7 analyzes interest group frame selection concerning the ePrivacy regulation. The study's findings with

regard to the formulated hypotheses will be discussed in Chapter 8. The last chapter answers the central research question and concludes by reflecting on limitations, practical implications and possibilities for future research.

2. Literature Review

2.1. The development of lobbying in the EU

Interests groups have become key actors in influencing politics and policies at the level of the EU (Coen and Richardson, 2009). Considering the EU's increasingly significant role in the international political landscape, EU decision makers also became an increasingly popular target of lobbyists (Biliouri, 1999). They are commonly perceived as "channels of societal representation of policy demands and as key actors in effective problem-solving and implementation of EU legislation" (Coen and Richardson, 2009, in Bunea & Baumgartner, 2014, p.1412). While the growing presence and involvement of interest groups in the EU is uncontested, scholarly work has been limited as compared to other subfields (Beyers, Eising & Maloney, 2008). As Beyers et al. (2008) argue, reasons for this development are conceptual, methodological and disciplinary obstacles. However, the gradual transfer of regulatory functions from member states to the EU institution has contributed to the Europeanization of interest groups and the increase in the number of empirical studies on interest groups.

2.2. Topics of interest group research

Interest group scholars concentrate on a variety of topics. These include but are not limited to interest group formation (Salisbury, 1969), access (Beyers & Braun, 2014; Bouwen 2004; Eising 2007; Dür & Mateo, 2013), organization (Greenwood, 2019), influence (Michalowitz, 2007; Dür & De Bièvre, 2007), success (Mahoney, 2007; Baumgartner, Berry, Hojnacki, Kimbell & Leech 2009; Dür, Bernhagen and Marshall, 2015; De Bruycker & Beyers, 2019) and framing (Boräng & Naurin, 2015; Bunea & Ibenskas, 2015; Eising, Rasch and Rozbicka, 2015; Binderkrantz, 2019). In particular, aspects of lobbying success and influence have been the center of researchers' attention (Bunea & Baumgartner, 2014). Lobbying success and influence are not synonymous. Success can either be the result of interest group influence or it can simply be luck (Klüver, 2013). Additionally, while access does not automatically translate into influence, it is perceived as an important step towards gaining political influence. In fact, an important prerequisite to be successful in influencing public policy is to get in contact with the representatives of the EU institutions (Beyers & Braun, 2014, p. 93). Regardless of the specific aspects studies focus on, they all either explicitly or implicitly refer to the importance of information. "[H]aving and presenting information to decision-makers is the most important

form of lobbying" (Rasch, 2018, p.3). Lobbyists working for a particular goal compete against each other to provide information to EU decision-makers (Rasch, 2018). In return for providing policy-relevant (expert) knowledge, interest groups seek to get legitimate access to the policy-making process in order to be able to steer it (Chalmers, 2013). What ultimately counts to be successful is that interest group get access to the right people in the right places at the right time (Bouwen, 2004). Multiple studies focus on assessing why some interest groups are more successful in changing the policy outcome towards their own preference than others. Whereas Dür and De Bièvre (2007) concluded that interests groups representing concentrated interests are more influential than interest groups representing diffuse interests, Klüver (2012) concluded that diffuse interests are better at influencing European policy-making. Additionally, Eising (2007) found, the more resources an interest group has, the better it can access European institutions. These results oppose to Mahoney (2007) and Baumgartner, Berry, Hojnacki, Kimball & Leech (2009) who did not find a clear relationship between these factors. In recent years, framing has become another dimension in the discussion on interest group prevalence in European institutions. It plays a central role in the legislative process of the EU.

2.3. Research on interest group framing

There are two commonly applied criteria that distinguish studies on interest group framing: The units of analysis they employ and the types of frames they address (De Bruycker, 2017).

2.3.1. Units of analysis: the two phases of framing

Framing has been studied from various angles. While some studies focus on actors, others focus on the different types of frames that prevail in a policy debate. De Bruycker (2017) and Baumgartner and Mahoney (2008) call these 'the two faces of framing'. De Bruycker (2017) suggests distinguishing between macro-level and micro-level framing while Baumgartner and Mahoney (2008) call these faces individual-level and collective-level framing. Both substantially mean the same: Macro-level framing looks at the aggregate level or the big picture and sets the tone for policy-making (Jensen & Seeberg, 2019; Baumgartner and Mahoney, 2008). It refers to the "process of how a policy debate is defined and understood" (Baumgartner & Mahoney, 2008; De Bruycker, 2017, p. 779). These frames can be identified by determining "the dominating aspects of a policy debate that are emphasized by institutions, advocacy coalitions and the news media" (Baumgartner and Mahoney 2008 in De Bryucker, 2017, p.779). In contrast, micro-level framing centers around interest groups as the main unit

of analysis. In this approach, frames are analyzed at the individual level focusing on the frame usage by interest groups (Baumgartner and Mahoney, 2008, p.441).

2.3.2. Types of frames

"[F]rames are seen as instruments of change or as strategic tools that interest groups rely on to obtain their political and policy goals" (De Bruycker, 2017, p.780). Klüver, Mahoney and Opper (2015) are interested in finding the factors that determine interest groups' framing choices towards the Commission. Other scholars concentrate on examining the characteristics of frames and attempt to cluster these. They commonly agree on the differentiation between generic and issue specific frames (Eising, Rasch & Rozbicks, 2015; De Bruycker, 2017; Boräng & Naurin, 2015) whereby issue-specific frames are linked to specific topics or events and generic frames can be identified across different issues (Vreese, 2005, p.54). The other dimension along which scholars attempt to cluster frames, however, varies from study to study. Eising, Rasch and Rozbicka (2015) who examined the effect of contextual factors and strategic highlighting on the number and type of frames in EU policy debates, classified frames also along the dimension of institutional versus policy frame. Institutional frames "derived from the institutional setting and relate to the general rules of the EU political system" (Eising, Rasch and Rozbicka, 2015, p.518) while policy frames "relate to substantial policy goals, norms, and instruments" (Eising, Rasch and Rozbicka, 2015, p.518). De Bruycker (2017) in contrast additionally differentiates between emphasis and equivalence frames as the second dimension. Emphasis frames highlight certain characterizations of an issue or problem instead of others (Druckman, 2004). Interest groups employ equivalence frames in case they provide the same information through different but logically equivalent phrases which make them change their preference (Chong & Druckman 2007, in Klüver, Mahoney and Opper, 2015). Three types of equivalence frames exist: "opportunities versus risks; gains (benefits) versus losses (costs) [and] positive consequences versus negative consequences" (De Bruycker, 2017, p.778). To determine the use of equivalence frames it is analyzed whether the arguments brought forward are related to the aforementioned aspects. Can the argument adopted be associated with the opportunities or risks of a specific policy issue? (De Bruycker, 2017). Furthermore, based on the dichotomy between issue-specific and generic frames, scholars have further specified frame types. While Boräng and Naurin (2015) distinguish generic frames into self-, other-, public- and ideal-regarding frames, Klüver, Mahoney and Opper (2015) have split them up into economic and public frames. Klüver, Mahoney and Opper (2015) study factors of frame choice when approaching the Commission and find that frames are tailored towards the Directorate

General responsible for the legislation draft. They conclude that the choice of frames varies systematically across interest group type and institution. Although scholars have succeeded in coming up with a scheme that allows to categorize frames, they are aware of the difficulties their approaches face. As outlined by De Bruycker (2017) frames can simultaneously fall into different categories. Generic and issue-specific frames can also be emphasis frames. Additionally, it can be difficult to distinguish between the effect of framing and the effect of other factors (De Bruycker, 2017).

Table 1

Summary of interest group research: units of analysis and types of frames

Unit of analysis	**Type of frame**	**Definition**	**Example**
Macro level	Issue-specific frames	They are linked to specific topics or events and can be identified by examining a particular policy debate or field and the role of organized interests therein (bottom up) (De Vreese, 2005; De Bruycker, 2017)	Framing of the death penalty debate in the United States. While the morality frame long dominated the death-penalty debate in the US, it has been replaced by the innocence frame (Baumgartner, De Boef & Boydstun, 2008)
Micro level	Generic frames:	They are not linked to a specific policy debate or issue but can be identified across debates or policy areas (Vreese, 2005).	
	1. Self-regarding frames	They refer to the preferences and interests of oneself, or the group one represents (Boräng & Naurin, 2015).	Business actors arguing that proposed regulations would over-regulate companies and thus would negatively affect their industry.
	2. Other-regarding frames	They refer to the interests or preferences of individuals belonging to other groups than those represented by the respondent. They emphasize the effects for other specific societal groups (Boräng & Naurin, 2015).	Actors (which do not represent a patients' group) arguing that proposed regulations would negatively impact patients.
	3. Public-regarding frames	They address general societal consequences (Boräng & Naurin, 2015).	Actors arguing that proposed regulations would negatively impact the environment.
	4. Ideal-regarding frames	They refer to the ideals of the speaker (Boräng & Naurin, 2015).	Examples include environmental protection, safety, or harmonization instead of outlining the impacts for a specific societal group.
	1. Economic frames[a]	They highlight the implications of a policy proposal on economic	Business actors arguing that proposed regulations would over-regulate

Unit of analysis	Type of frame	Definition	Example
		performance (Klüver, Mahoney & Opper, 2015).	companies and thus would negatively affect their performance.
	2. Public frames[a]	They emphasize the implications of a policy proposal for public goods (Klüver, Mahoney & Opper, 2015).	Examples include environmental frames, human rights frames, consumer protection frames and public health frames. As their names tell, actors might highlight the policy proposal's impact for the environment or for the protection of consumers. This can be both negative or positive, e.g. improving or deteriorating the current status quo.
Macro or micro level	Emphasis frames	They emphasize one aspect of an issue over others (De Bruycker, 2017).	The aforementioned examples of generic and issue-specific frames are also emphasis frames (De Bruycker, 2017).
Micro level	Equivalence/equivalency frames: 1. Opportunities versus risks 2. Gains (benefits) versus losses (costs) 3. Positive consequences versus negative consequences	They present different but logically identical information in a different way, which cause individuals to alter their preferences'. It typically involves 'casting the same information positively or negatively (De Bruycker, 2017).	All equivalence frames are generic frames, as they are "applicable across different policy issues" (De Bruycker, 2017, p. 778).
Macro level	Institutional frames	They "derived from the institutional setting and relate to the general rules of the EU political system" (Eising, Rasch & Rozbicka, 2015, p.518). The EU institutions frame policy proposals in a way that aims to unite relevant political and societal actors and reduces the amount of conflict between them (Eising, Rasch & Rozbicka, 2015).	Institutional frames "promote the emergence of frames related to market integration, regulation and policy harmonization" (Eising, Rasch & Rozbicka, 2015, p.519).
Macro level	Policy frames	They "relate to substantial policy goals, norms, and instruments" (Eising, Rasch & Rozbicka, 2015, p.518)	Frames that relate to specifc policy fields, e.g. environmental policies or education policies

a The grey fields highlight the types of frames that will be addressed in this study

2.4. The impact of framing

Scholars also combine various aspects of lobbying in their studies. Rasch (2018) has attempted to find out whether and if so to what extent framing contributes to lobbying success. Bunea and Ibenskas (2015) draw conclusions to interest groups' success by systematically analyzing policy position documents in the Commission's public consultation. They compare both a quantitative and a qualitative content analysis to see whether the method applied leads to different outcomes. They found that the use of quantitative content analysis which applies strict analytical assumptions can result in the exclusion of texts and relevant observations from the analyzed sample. Boräng and Naurin (2015) discuss "frame congruence between lobbyists and European Commission officials" (p.499). They study the correspondence of policy makers' and interest groups' frames and argue that the context of the lobbying influences framing success. They emphasize the importance of two contextual factors: the scope of conflict and the pertinence of media coverage that determine "whether the frames of business interests dominate those of civil society interests in the minds of the European Commission" (p.499).

2.5. Identification of a research gap

Overall, the number of studies in the field of interest groups is still limited. While some aspects have been studied quite extensively, others have only more recently attracted scholars' attention. This also includes the aspect of framing although it "offers a 'better specification of actor preferences (…) and a nuanced and empirically more accurate picture of the relationship between these actors" (Daviter, 2007, p.662) which is lacking in other theoretical models of EU legislative politics. In particular in the context of the EU, interest group framing remains under-researched (Eising, Rasch & Rozbicka, 2015, p. 516). Furthermore, from a methodological point of view, the phenomenon has mainly been studied quantitatively or as a mixed-methods approach (Voltolini, 2016). However, studying interest group framing by taking a quantitative approach has posed significant methodological difficulties, including the determination of frames in a reliable and valid way (De Bruycker, 2017). This study therefore seeks to explore the characteristics of frame usage in the ePrivacy regulation qualitatively. This allows to provide a more detailed analysis of the dynamics in this specific policy debate. In particular, while quantitative research excludes outliers from their sample in order to avoid disturbing the model, these are exactly the cases that will be explained in more depth. Thus, instead of looking at the general picture, individual interest groups and their types can be examined more closely. Additionally, while the strict analytical assumptions of quantitative content analysis might not adequaltely analyze the selected documents, a qualitative approach can take particular features suitably into account. For instance, although defined key words signal the use of a specific type

of frame, there might still be exceptional cases which would be misinterpreted using a quantitative approach.

3. Background: Lobbying in the European Union

Considering this study's focus, only the role of the Commission and the EP will be discussed. The Council of Ministers will be disregarded as it has a "long-standing and often repeated reputation of being the most secretive and least accessible of the EU institutions" (Directorate General for Research, 2003, p.42). Its General Secretariat does not keep any documentation of meetings with interest groups and the process of lobbying the Council is intransparent (Directorate General for Research, 2003) which explains the difficulty and unreliability of data collection that would result from including it in this study.

3.1. The European Commission

The Commission is the most important and most popular target for lobbyists due to its central role in the legislative process (Directorate General for Research, 2003). As agenda-setter, it is responsible for proposing and drafting new legislation (Bouwen, 2002). The Commission's administration is divided into different Directorates-General (DG) which are each assigned to a specific policy area (Hix & Høyland, 2011, p.8). For lobbyists it is important to identify the lead DG in order to systematically approach the actors that are responsible for drafting the new legislation. Consulting different stakeholders is not only the Commission's obligation, but it can also be considered a win-win situation for the Commission and interest groups. On the one hand, it helps to improve the quality of the policy outcome, on the other hand it increases the possibility for interested parties and the general public to participate in the policy process (European Commission, 2002). Despite these positive characteristics, it cannot be ignored that there is also criticism surrounding the work of interest groups. The democratic character of interest group participation in the EU's political process in particular has been questioned (Saurugger, 2008).

3.2. The European Parliament

With the introduction of the cooperation and the co-decision procedures, the EP became an increasingly important actor in the legislative process. While member states could formerly veto in the Council, the EP received the power to amend or reject legislation that the Council favored when the Single European Act entered into force in 1987. These institutional changes were accompanied by an intensification of interest groups' lobbying activities with the EP (Directorate General for Research, 2003, iii, p.33). As most of the legislative work takes place

in specialized standing committees, they are most frequently lobbied (Bouwen, 2004). These committees adopt reports and organize hearings which inform legislative proposals (European Parliament, n.d.). The EP thus comes into the focus of interest groups as soon as the rapporteur of the responsible Committee starts to prepare his or her report, and the discussion within the Committee begins (Directorate General for Research, 2003, p.33).

To conclude, lobbying in the EU has steadily intensified. The Commission as well as the EP have an interest in consulting private actors and vice versa. Contrary to the common belief that lobbying is a unidirectional activity of non-state actors vis-à-vis the EU institutions, it can, in fact, be considered an exchange relation between both parties (Bouwen, 2004).

4. The ePrivacy regulation

Privacy and data protection are fundamental rights as outlined in EU primary and secondary law (Monteleone, 2017). Article 7 of the Charter of Fundamental Rights (CFR) as well as Article 8 of the European Convention on Human Rights (ECHR) provide the legal basis for the right to privacy. Until 2017 the Data Protection Directive (95/46/EC) complemented by Directive 2002/58/EC regulated data privacy in the EU (Monteleone, 2017). Since the last revision, pervasive technological, economic and social changes have taken place and have verifiably altered the way electronic communication is used. The ePrivacy Directive did not adequately reflect these recent developments (Schrefler, 2017). Only traditional telecom operators were covered whereas new internet-based forms of communication were not included. The new proposal made by the Commission in January 2017 takes up on the former ePrivacy directive but seeks to align existing rules for e-communications with the new GDPR and new technological and economic developments in the market (Monteleone, 2017).

Within the EP, the proposal was assigned to the Committee on Civil Liberties, Justice and Home Affairs (LIBE). The vote in the LIBE committee on the Parliament's positions (first reading) took place 19 October 2017 and opened interinstitutional negotiations with the Council (European Parliament, 2017b) (Table 2).

Within the Council, under the Maltese Presidency, the proposal was assigned to the Telecommunications and Information Society working party (TELE WP), which completed a first examination of the proposal. The Council published several redrafts since September 2017. While the EP has already decided to start inter-institutional negotiations in October 2017, an agreement within the Council has not yet been reached (Stolton, 2019). In November 2019 Finland presented the last compromise proposal on the ePrivacy regulation which, however,

did not lead to any agreement at the Council Working party on telecom (European Parliament, 2019b).

Table 2

Overview of key events concerning the ePrivacy regulation

Date	Key events
Between April and July 2016	Commission's public consultation
10 January 2017	Publication of the legislative proposal
16 February 2017	LIBE announced as the responsible Committee, 1st reading/single reading
11 April 2017	EP committee (LIBE) held a hearing
9 June 2017	The initial rapporteur presents LIBE's first report
19 October 2017	Vote in committee, 1st reading/single reading; adoption of the first report, committee decision to open interinstitutional negotiations; new rapporteur
23 October 2017	Committee report tabled for plenary, 1st reading/single reading; committee decides to enter into interinstitutional negotiations conformed by plenary
4 December 2017	Debate in Council
21 October 2019	Committee referral announced in Parliament, 1st reading/single reading
November 2019	The Council presented the last compromise proposal on the e-Privacy regulation; no agreement at the Council Working party on telecom

Source: Own illustration, based on data of the European Parliament *Legislative Observatory.*

5. Theoretical Framework

5.1. The concept of framing

Before explaining the theory underlying this study, it is important to clearly define what is meant by framing considering its conceptual ambiguity as discussed in the literature review. While the term seems omnipresent in a wide variety of disciplines, a commonly agreed theory of how frames manifest themselves and which impact they have (Entman, 1993) does not exist. However, "central to any conceptualization of framing is that the manner in which certain aspects of reality are expressed has the potential to affect the decision of an actor choosing from a set of possible actions" (Klüver, Mahoney & Opper, 2015, p.483). Entman's (1993) definition of framing is broadly accepted amongst scholars and will thus also be used for this study. According to Entman, "[t]o frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the

item described" (Entmann, 1993, p.52). Applied to the policy process of the EU, this means that interest groups highlight specific aspects of the proposal. This can cause disagreement between interest groups considering their potential different points of views. Furthermore, it implies that lobbying is essentially a strategic communicative activity. Whereas there is at least some consensus about the definition of framing amongst interest groups scholars, there is little consistency in the types of frames they have identified (De Bruycker, 2017). Therefore, it is fundamental to be very explicit about which types of frames are of interest to this study (Cacciatore, Scheufele & Iyengar, 2016).

5.2. Selecting a theoretical framework: The two logics of interest groups

The study's aim is twofold: Firstly, it aims to find out how frame selection varies depending on the type of interest group when lobbying the Commission and the EP. Secondly, by comparing frame choices vis-à-vis these EU institutions, it will be assessed whether and if so how it differs across EU institutions. As there is a wide range of factors that might cause variation, which would exceed the scope of this research, it is essential to concentrate only on the most important factors. These factors will be determined by drawing on existing studies. It will help to decrease the probability of omitting an important factor which would negatively influence this study's internal validity. However, as the number of studies on interest group framing is still limited and many of these additionally focus on the effect of framing on lobbying influence and success, the range of suitable theories for this study is restricted. With their 'two logics of interest groups', Klüver, Mahoney and Opper (2015) seem to provide the only theoretical basis which fits this study's purpose. Other theories which focus on the properties of interest groups and EU institutions in order to explain interest groups' frame choice do not exist in the current scholarly work. Schmitter and Streeck (1999) originally developed the notion of the 'logic of influence' and the 'logic of memebership' to study the organization of business interests. However, whereas their early study concentrated on analyzing businesses' strategic autonomy on the basis of these logics, Klüver, Mahoney and Opper (2015) adopted their theory to study interest group framing. They postulate that the internal structure of interest groups as well as contextual characteristics are the most important factors that influence interest groups' frame choice.

5.2.1. The logic of membership

According to the logic of membership, interest groups have to employ frames that correspond to their constituency structure, thus their members' positions, to receive the required

resources from them (Klüver, Mahoney & Opper, 2015). Therefore, the type of interest group is an important factor that will be analyzed in order to assess why interest groups‘ frame choice varies across type of group (Klüver, Mahoney & Opper, 2015). Klüver, Mahoney and Opperman (2015) distinguish interest groups according to their organizational form and nature of interest. Organizationally, a distinction can be made between associations and firms. Associations have members who are individuals, companies, public institutions or other associations. In contrast, firms do not have any members (Klüver, Mahoney & Opperman, 2015). Associations can be further divided into ‘cause groups’ and sectional groups’ (Klüver, Mahoney and Opperman, 2015). While sectional groups represent special economic interests of a section of society such as farmers, cause groups represent diffuse public interests and work to provide public goods including environmental protection or consumer protection (Klüver, Mahoney & Opperman, 2015). No special requirements have to be fulfilled to become a member of a cause group (Klüver, Mahoney & Opperman, 2015). Deriving from this argumentation the first hypothesis can be formulated as follows:

H1: Frame choice varies systematically across type of interest group. Cause groups will employ public frames, sectional groups will employ economic frames and firms will show a great diversity of frames as they do not need to adhere to any members’ position.

5.2.2. The logic of influence

According to the logic of influence, interest groups employ frames that appeal to and thus allow them to influence decision-makers and ultimately the policy outcome (Klüver, Mahoney and Opperman, 2015). Klüver et al. (2015) argue that interest groups need to respond to the institutions’ characteristics in order to be able to maximize their influence. As the Commission takes a vital role in the policy formulation process through drafting the proposal, it is a popular target of interest groups. These proposals are typically the product of a preceding consultation process with expert groups, advisory committees and stakeholders (Klüver, Mahoney & Opper, 2015). When lobbying the Commission, interest groups should tailor their frames to the Directorate General (DG) which is responsible for drafting the policy proposal. Furthermore, each DG has specific competences, areas of interest and beliefs which is important for interest groups to consider when approaching them. Whereas the DG competition for instance represents more liberal views, DG industrial policy is more interventionist (Morth, 2000). Therefore, Klüver et al. (2015) emphasize the significance of tailoring framing strategies to the specific preferences and beliefs of the responsible lead DG.

As Klüver et al. only concentrate on interest group framing with regard to the Commission, their proposed theoretical framework will be expanded to the EP in this study. In fact, members of the EP are distributed in a number of specialised standing committees. As these committees are considered the 'legislative backbone' of the EP where the real scrutiny of EU legislation takes place, most lobbying activities also take place in the committees rather than at the plenary (Hix & Høyland, 2011, p.58; Neuhold, 2001). More specifically, each committee deals with certain issues, which is already reflected in their names (e.g. International Trade (INTA) or Civil Liberties, Justice and Home Affairs (LIBE) (European Parliament, n.d.). Committees propose amendments to legislation, which are modified (if necessary) and voted in the full plenary session (Hix & Høyland, 2011, p.58). Thus, the EP's position is decided in the responsible committee ahead of plenary sessions. Therefore, in line with their reasoning interest groups frames also need to match the responsible EP committee's orientation.

H2: Frame choice is affected by the institutional properties of the European Commission and the European Parliament accordingly.

H2.1: Frames that interest groups employ are specifically tailored towards the Directorate General in charge of drafting the proposal. Interest groups will use public frames when the lead DG focuses on public goods aspects whereas they will use economic frames when the lead DG focuses on handling economic aspects.

H2.2: Frames that interest groups employ are tailored towards the EP committee in charge. Interest groups will employ public frames when the responsible committee focuses on public goods aspects whereas they will employ economic frames when the committee is responsible for handling economic aspects.

6. Research Design and Methodology

Firstly, both a qualitative and quantitative approach will be introduced. This will ultimately serve as the basis to argue why the co-variational analysis has been chosen as the appropriate and feasible design for this study. Secondly, the methodology for analyzing and explaining interest group framing in case of the proposed ePrivacy regulation will be discussed. Most importantly, the concept of frames and their operationalization will be elaborated. Details concerning the data collection and operationalization will also be provided thereby reflecting on potential obstacles and limitations which (might) occur.

6.1. Discussion of available research designs

6.1.1. Quantitative design: Cross-sectional observational study

Quantitative research entails "the collection of numerical data, a deductive view of the relationship between theory and research" (Bryman, 2016, p.149). It can be observational or experimental. As "implementing an experiment often proves to be unworkable, and sometimes downright impossible" (Kellstedt & Whitten, 2013, p.82), this study only considers observational research designs. Time-series design and the cross-sectional design are commonly used types. Time-series observational studies "focus on variation within a single spatial unit over multiple time units" (Kellstedt & Whitten, 2013, p. 84). Applied to the present research question, this would mean that interest groups' choice of frames over a longer period (for example comparing the current regulation to its predecessors) would need to be analyzed. This is, however, not the research's aim. The cross-sectional approach in contrast is considered an appropriate observational design. It focuses on "explaining the variation in the dependent variable" (Kellstedt & Whitten, 2013, p.85). Applying it to framing allows to examine a greater variety of factors that might influence interest group frame selection. For instance, proposals of different degrees of salience covering different policy areas could be analyzed and compared. It would also allow to look more closely at patterns and potential variation across multiple directives or regulations. As all data are collected more or less simultaneously, the problem of "ambiguity about the direction of causal influence" arises (Bryman, 2016, p. 53). From the resulting data it can be inferred that the variables are related, however, it remains uncertain whether the identified relationship is really causal. Applied to the topic of framing, this means that it must be ensured that interest groups' frame selection really derived from the predetermined factors and not from others. Accordingly, the usage of control variables (e.g. salience, date of proposal) is particularly important.

6.1.2. Case study design

Case studies are small-N studies that are widely used as they allow a deeper and more detailed investigation than other, specifically quantitative, designs. According to Gerring (2004) a case study is "an intensive study of a single unit with an aim to generalize across a larger set of units" (p. 352).

Amongst the approaches to small-N studies are congruence analysis (CON) and co-variational analysis (COV) (Blatter & Blume, 2008). CON is used when the researcher seeks to explain whether one theory over others provide empirical evidence for the social reality

(Blatter & Haverland, 2014). Since theoretical explanations for the choice of frames are scarce and this study only looks at two specific factors that might influence interest group frame selection, namely type of interest group and type of institution, this approach is not appropriate. In contrast, COV aims to draw "implications from one or a few cases to the appropriate wider population of cases" (Blatter & Blume, 2008, p. 349). The existence of the "co-variation between an independent variable X and a dependent variable Y will be examined to infer causality" (Blatter & Haverland, 2012, p.33). As the aim of this study is to explore to what extent the types of interest groups and EU institutions (X) determine interest groups' frame selection (Y), the application of a co-variational design is suitable. In order to address the problem of validity of causal interference inherent to COV, cases need to be selected carefully. These need to vary as much as possible on the independent variable of interest (type of interest group and institution), while other variables (here: other potential factors determining interest group frame selection such as salience) need to be as similar as possible (Blatter & Haverland, 2012). A policy proposal that involved lobbying activities of three types of interest groups has been selected. In addition, the orientation of the Commission's DG and the EP committee that were responsible for this proposal differed. More precisely, while the DG (DG CONNECT) focuses on economic aspects, the EP Committee (LIBE) focuses on public goods. As frame choice vis-à-vis the Commission and the EP is analyzed with respect to only one EU regulation, other variables including salience are identical.

The limited scope ensures the study's feasibility. Although research findings are not generalizable to the entire population, they still add value to the existing literature on interest group framing and to the understanding of the selected regulation more specifically. Such a method performs significantly better with respect to its internal validity (Voltolini, 2016). This is informed by its underlying rich and detailed contextualization. Triangulation, thus consulting multiple sources, different data types and different methods increases the study's reliability (Voltolini, 2016, p. 362). In this case, reliability will be ensured by analyzing a variety of official EU documents, position papers and contributions to the public consultation and hearings dealing with the selected regulation.

6.1.3. Selection of Research Design

In order to answer the central research question, both a co-variational design as well as a cross-sectional design could be applied. On the basis of the research objective and the identified research gap, an in-depth analysis of the different lobby groups' frame selection approaching the Commission and the EP in the case of the ePrivacy regulation was conducted.

The co-variational analysis has been selected as this study aims to investigate in detail whether the types of interest groups and EU institutions make a difference in interest groups' choice of frames concerning the selected regulation. Altough this study will not tackle the issue of interest group frame selection quantitatively using statistical models, numerical data about the frequency of the different types of frames employed by the different types of interest groups will nevertheless be generated through counting.

6.2. Choosing a regulation

This study focuses on the policy debate of the ePrivacy regulation. The regulation was selected on the basis of two criteria. Firstly, to ensure the availability of data when lobbying the Commission and the EP, the EU directives or regulations needed to be subject to both a Commission's public consultation process and an EP hearing. This way, it could be ensured that reliable sources including official responses to the Commission's consultation questionnaire, position papers (in the case of consultation) and speakers notes (in the case of EP hearings) could be obtained and analyzed. Additionally, using consultations and hearings as a selection criterion offers two advantages. According to the *General principles and minimum standards for consultation of interested parties by the Commission* (2002), the European Commission only consults on important policy initiatives, which are expected to have a significant impact on a specific sector (p. 15). By including only those legislative discussions, it can thus be ensured that the study focuses on "politically important policy debates that raised a minimum amount of attention and controversy" (Klüver, Mahoney & Opper, 2015, p.487f.). Another "major advantage of only choosing policy proposals which have been preceded by public consultations is the availability of textual data for the measurement of interest group framing" (Klüver, Mahoney & Opper, 2015, p.488). Secondly, for relevance reasons of this study, only EU directives or regulations that included consultations and EP hearings that were held later than in 2010 were eligible.

After the co-variational research design has been chosen, it is imperative to discuss the adequate measurement for interest group framing.

6.3. Operationalization

6.3.1. Determining the types of interest groups

The theoretical framework has outlined the classification of interest groups for this study. Following the concept of Klüver, Mahoney and Opper (2015), a division between sectional groups, cause groups, and firms will be made. To recall, sectional groups represent

the interests of a specific group of members (private interests), cause groups represent the interest of their members (public interest) and firms only represent their own interests (Klüver, Mahoney & Opper, 2015). This classification not only facilitates getting a clear overview of interest groups' involvement in the policy process, but it also contributes to the study's precision. In order to identify what types of interest groups have been involved, their respective websites will be consulted to generate supplementary information on their organizational structure and field of interest. This research will be conducted both for the interest groups that were involved in the Commission's consultation and the EP's hearing.

6.3.2. Measuring interest group frames

Different interest groups tend to focus on and highlight different aspects of the same policy proposal (Klüver, Mahoney & Opper, 2015). In a policy debate which discusses a potential ban of single-use plastics for example businesses that are directly affected by the proposal could highlight the underlying negative economic effects they are confronted with as producers of plastics while non-governmental organizations might highlight the positive effect for the environment. As interest groups focus on a specific aspect and disregard others, they frame it. Scholars have differentiated between various frames (Table 1). However, for the purpose of this study, a differentiation will only be made between public frames and economic frames. Klüver, Mahoney and Opper (2015) also follow this classification which clearly derives from the logic of membership. When an interest group focuses on highlighting aspects referring to public goods, it uses public frames. Public goods "cannot be withheld from consumers who do not pay for them, and whose consumption does not reduce their availability to other consumers" (Ravenhill, 2017, p.421). Crime and security frames but also environmental frames, human rights frames, public health frames and consumer protection frames belong to the category of public frames (Klüver, Mahoney & Opper, 2015). Considering that this study analyzes the ePrivacy regulation in greater detail, it does not make sense to include all of the aforementioned public frames. Thus, the public frames 'crime and security', 'consumer protection' and 'human rights' will be subject to this analysis alongside economic frames, which are used when the interest group highlights economic aspects.

Interest groups' submission to the Commission's consultation usually involves several policy issues which constitute different dimensions of one proposal. "Within the EC [European Commission] consultations, an issue refers to those policy aspects on which the EC asks for stakeholders' input" (Bunea & Ibenskas, 2015, p.433). Submitted responses to the Commission's questionnaire for the public consultation will be gathered from the lead DG's

website in order to get an overview of the most important interest groups that were concerned with the proposal. As this study is interested in framing which assesses individual's argumentation and choice of language, the questionnaire's free text fields will be analyzed. More precisely, important key words and word combinations will be determined to cluster and differentiate between different types of frames (Klüver, Mahoney & Opper, 2015). In a first step hand-coding will be conducted. "A code in qualitative inquiry is most often a word of short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data" (Saldaña, 2015, p.4). Applied to the study at hand, it means that words and phrases which indicate the usage of a public frame or economic frame will be determined. These key words were adopted from other studies on framing, including the one by Klüver, Mahoney and Opper (2015) and were furthermore determined in the process of pre-coding. Following an inductive, data-driven approach, codes were developed after viewing the data. It means that initially all documents were carefully read paying attention to words and word combinations that might signal the use of one of the four frames (consumer protection, crime and security, human rights and economic). Those words and word combinations that are used most frequently when referring to an economic argument or a public goods argument will be determined as 'keywords'. For instance, if interest groups use words such as 'business', 'competition' and 'innovation' they use an economic frame while words such as 'criminal' or 'fraud' indicate the use of a crime and security frame (public frame). In addition, it is important to note that within one sentence two or more types of frames can be identified depending on the interest group's choice of words. Table 3 provides a more detailed overview of the indicating words for the frame selection in the case of the ePrivacy regulation. Considering that this regulation deals with aspects concerning the digital single market, environmental aspects did not play a role and thus the environmental frame is also not listed in the table. Furthermore, it is important to highlight that 'framing' cannot be synonymously used for interest groups' preferences. This means that interest groups speaking on behalf of the industry may feel that the proposal could have negative economic consequences. However, it could still use a public frame rather than an economic, depending on the reasoning. Important for the identification of frames is what the interest group says and not what their motives might be. The idea behind this approach is that "words that co-occur 'in similar contexts tend to have similar meaning' and 'documents that contain similar word patterns tend to have similar topics" (Klüver, Mahoney & Opper, 2015, p.488). Looking only on the presence of single words might cause difficulty to clearly differentiate between different types of frames. Consumer protection frames and crime and security frames in particular seem to be quite similar. In both cases the

word ‘security’ and ‘secure’ for instance could indicate their occurrence. However, while consumer protection frames clearly deal with individuals’ security, the crime and security frame refers to the concept of public or collective security. In order to determine the choice of frames more accurately, it is thus essential to take a closer look at the context or more precisely the neighboring words and the co-occurrence of word combinations. In contrast to crime and security frames, only those are classified as consumer protection, which contain a combination of at least one of the signal words ‘protect/safeguard/ secure’ (and lemmata) and ‘citizen/ indi-vidual/consumer/customer/user’ in the same sentence (Table 3).

In order to cross-validate the obtained results of the hand-coded framing analysis, they were compared by using the computer-assisted qualitative content analysis software MAXQDA (see Eising, Rasch & Rozbicka, 2015). In a first step, all documents were prepared for integrating it into the software. All text passages which did not directly refer to the interest groups’ views on the policy debate were removed. These included interest groups’ self-descriptions, consultation questions and questions asked by interest groups themselves. In a second step, the signal words were integrated into the software to create the corresponding codes for each frame. Initially, the advanced lexical search function of MAXQDA allowed to check the quality of key words and word combination determining a frame. It revealed which word combinations need to be excluded from the search as they would have distorted the results[2]. Overall, the use of this software helped to facilitate the research process through organizing and structuring the data more systematically. Additionally, it helped to ensure methodological rigor. Deeper insights into the selected regulation could be gained by automatically identifying all key words and word combinations which might have been missed otherwise.

[2] For instance, in the case of the economic frame, proper names, which included key words of an economic frame such as ‘commerce’in ‘Ecommerce Europe’ were excluded as not all arguments including their organization’s name could be classified as economic arguments. In addition, replies which were repeated and did not add a new argument by an interest group could also be easily identified through MAXQDA and were excluded.

Table 3

Indicating words and word combinations for frame classification

Type of frame	Indicating words and word combinations	Excluded word combinations
	Public frames	
Consumer protection frame	- protect/safeguard/secure in combination with citizen/individual/consumer/customer /user - protection/safety/security in combination with citizen/individual/consumer/customer /user - safe/secure in combination with citizen/individual/consumer/customer /user	- Consumer protection authorities/bodies/instrument/law/ rules - Right in combination with protect/safeguard/secure in combination with citizen/individual/consumer/customer /user - Right in combination with protection/safety/security in combination with citizen/individual/consumer/customer /user - Right in combination with safe/secure in combination with citizen/individual/consumer/customer /user
Human rights frame	- Charter of Fundamental Rights - Confidentiality of communications in combination with right - Right of individuals to secure their communications - Right of confidentiality of communications - Right to respect for his or her private and family life, home and communications - Fundamental right - (Fundamental) right to privacy - Fundamental rights to privacy and data protection - Fundamental rights and freedoms of individuals - Right to privacy and confidentiality - Right to data protection - Human right - Rights and freedoms of individuals	
Crime and security frame	- Abuse - Criminal, crime - (Data) breach - Exploit - Fraud - Hacking, hacker - Illegal	- Security/secure in combination with citizen/individual/consumer/customer /use - Network and Information Security (NIS) Directive

Type of frame	Indicating words and word combinations	Excluded word combinations
	- Security, secure - Malicious - Malign - Malware - Misuse - Oppressive - Threaten - Unlawful - Unauthorized	
	Economic frame	
	- Business - Commercial - Company - Competition, compete, competitive, competitivity, competitiveness - Corporate - Cost - Economic - Enterprise - Entrepreneurial - Expense, expensive - Financial, financially, financed - Firm - Growth, grow - Industry - Innovation, innovate, innovative - SME - Level playing field - Market - Money, monetary, monetizing - Pay - Productivity - Profit - revenue - Trade/trader	- Law firm - At all costs - Names including: Ecommerce Europe, Telecommunications Single Market Regulation, Unfair Commercial Practices Directive, Trade Association representing corporate companies (Explanation ETNO), Danish Business Forum

Note. The order of indicating words does not play a role. They just need to co-occur in the same sentence.

For the EP, the procedure was repeated. Instead of submitted questionnaire responses and position papers as in the case of the Commission's consultation, speakers' notes of the EP hearing were analyzed.

Qualitative content analysis has several advantages: The diversity of language employed in position papers can adequately be taken into consideration when analyzing interest groups' positions which is not equally possible using a quantitative design[3] (Bunea & Ibenskas, 2015).

[3] An example can be found in section 7.2.2.1. Access Now used the expression 'level playing field' which typically highlights the use of an economic frame (Table 3). Due to its explanation, however, it indicated the use of a consumer protection frame.

Furthermore, “categories, relationships and assumptions that inform the respondents’ view of the topic” (Basit, 2003, p.143) could be determined in greater depth. However, there are also some shortcomings. Hand-coding takes a lot of time and resources (Bunea & Ibenskas, 2015). Additionally, “[c]oding is not a precise science; it is primarily an interpretive act” (Saldaña, 2015, p.5). In order to minimize the inaccuracy of hand-coding, “pre-coding circling, through highlighting, bolding, underlining or coloring rich or significant participant quotes or passages that strike you” (Saldaña, 2015, p.20) as well as computer-assisted content analysis were conducted.

6.4. Step-by-step explanation of the hand-coding procedure

Whereas it is straightforward to determine the lead DG and the EP committee in charge of the proposal, determining the type of frame can be quite challenging. Frames usage might not be as clear-cut, and frames might even overlap. The following steps will be taken in order to structure the process of identifying a frame:

1. What is the interest group asking for? (general interest)
2. Based on the occurrence of key words, what arguments have been used by the interest group to convince the DG/ EP committee of its position?
3. Following the classification of all arguments, the frequency of economic and public goods arguments will be counted.
4. In case the number of economic arguments exceeds the number of public arguments, the interest group overall used an economic frame and vice versa.

6.5. Data Selection and Collection: Documentation

After both the research design and the method have been discussed and selected, it is imperative to elaborate on the process of the data selection and collection. Initially, the data source consulted for the purpose of this study will be discussed. Subsequently, the process of data collection will be further explained thereby reflecting on potential obstacles that might be faced.

According to Yin (2003) six sources are most commonly used as evidence for case studies. These include documents, archival records, interviews, direct observation, participant-observation, and physical artifacts. As all these sources have their individual strengths and weaknesses, the use of as many different sources as possible is recommended (Yin, 2003). For the study at hand, however, it did not make sense to include other sources than documentation. Potential drawbacks of documentation as outlined by Yin (2003) include their inaccuracy as

well as their deliberate manipulation. The likeliness that these drawbacks also hold true for the documents that have been consulted for this study, however, is very low. The analyzed documents are official in nature and derived from the Commission's consultations, the interest groups websites and the EP hearing. As interest groups themselves aim to influence policy makers to the greatest extent possible they make every effort to formulate their positions as precisely and accurately as possible. Therefore, interest groups pay great attention and control the process of filling in the EP's questionnaire or producing position papers. Furthermore, it is very unlikely that the Commission and the EP publish inaccurate accounts of interest groups' position as they are subject to the scrutiny of businesses and citizens. While it was initially clear that sources such as archival records or direct observation would not be consulted as supplementary sources to documentation, conducting interviews has been considered. However, they were not included as they did not add value to the study. On the contrary, there are certain weaknesses inherent to interviews which are particularly problematic to this study considering that it examines interest group framing which is clearly a concept that relies on written accounts. These weaknesses include inaccuracies or even biases which result from the way questions are asked or responses are recalled (Yin, 2003). Interviewees also naturally do not assign the individual words the same importance that they assign in a written context, which however, greatly impacts framing. Interpersonal relationships further influence interviews. Thus, one should not overly rely on the information provided. Adding a variety of different sources would furthermore be problematic given that they can be very different in nature and scope. Even for the purpose of gathering background information about the selected topic, namely ePrivacy, interviews were considered an insufficient source. Instead gathering information through desk research was considered to be most accurate and objective.

Documentation is a useful and commonly applied source of evidence for case studies. It does not only help to verify correct spellings, but it also allows to confirm or contradict information gathered through other sources (Yin, 2003). For the case at hand, documentation plays an important role in the process of data collection both in case of the Commission and the EP.

6.5.1. Consultation in the European Commission

Data for this analysis largely derived from the Commission's public consultation on the ePrivacy regulation. The Commission is mandated to consult widely on important legislative measures (European Commission, 2002). In the context of the Commission's consultation process, interest groups' responses to the questionnaire as well as position documents have

become an important data source for estimating their policy positions and demands (Bunea & Ibenskas, 2015). "Consultation data are useful insofar as they provide an accurate picture of lobbying patterns (…), including which specific groups lobbied and what their preferences were regarding the new regulation" (Atikcan & Chalmers, 2019, p.550). The Commission also regularly consults interest groups via conferences and public hearings. However, as information on interest groups participation does not exist for these events, they are excluded for this study (Atikcan & Chalmers, 2019).

The ePrivacy regulation was subject to consultation with different policy actors, which took place in 2016 (DG CONNECT, 2016). Via the Commission's website[4] a full report on the public consultation on the ePrivacy reform, individual responses submitted to the questionnaire as well as additional position papers could be accessed. Additionally, a detailed overview of all stakeholders involved, ordered according to their institutional features was provided. Therefore, the prerequisites for the analysis of frame usage proved to be satisfactory.

6.5.2. Hearings in the European Parliament

Despite its own committment to greater transparency, the collection of data for the EP is not as easy and accessible as in the case of the Commission. The EP does not conduct public consultations. Interest groups are, however, involved in the EP decision-making process. An important source of information are hearings conducted by EP committees. Although the plenary session has the final say on legislation, most of the EP's legislative work takes place in its specialized committees (Bouwen, 2002). These public hearings do not only increase the legitimacy and transparency of the EP's decisions, but they also provide members of parliament with (expert) knowledge that helps them to grasp the background of the issue discussed. Most importantly in the context of this study, hearings allow invited interest groups to present their position on a given policy proposal (Eising & Spohr, 2017).

For the ePrivacy reform the hearing was conducted in January 2017. Via the EP's website[5] the speakers' notes could be accessed. They are publicly available and allow to determine the number and types of interest groups that were involved in the hearings as well as their position. Therefore, types of frames can be identified using this proposed source of information.

[4] The website is accessible via https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive

[5] The website is accessible via https://www.europarl.europa.eu/committees/en/product-details/20170328CHE01221

7. Analysis

This section is dedicated to identifying interest groups' frame selection approaching the Commission and the EP concerning the selected policy debate. The comparison of three types of interest groups and two EU institutions will allow to answer the central research question.

7.1. European Commission

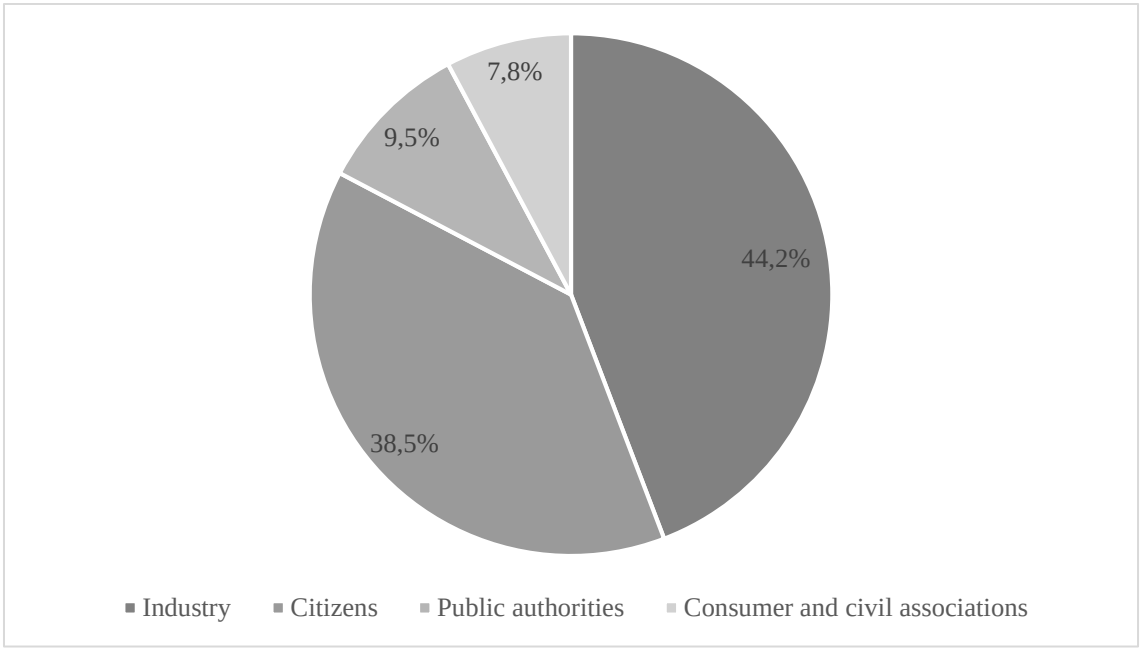
The Commission held a public consultation covering the evaluation and review of the ePrivacy directive between April and July 2016 (Schrefler, 2017).

7.1.1. Identification of involved interest groups

Overall 421 responses from the EU and outside the EU were submitted to the Commission's public consultation. It received 186 replies (44,2%) from industry actors, 162 from citizens (38,5%), 40 replies from public authorities (9,5%) and 33 from consumer and civil society associations (7,8%) (DG CONNECT, 2016).

Figure 1

Responses to the public consultation



Source. Own illustration

As this study focuses on three types of interest groups, namely firms, cause groups and sectional groups, responses by individual citizens, public authorities and anonymous

stakeholders were excluded considering that they do not belong to or cannot be accurately classified according to any of these types. This reduced the sample of potential units of analysis to 200 which still did not allow for a detailed qualitative analysis with respect to the foreseen scope of the study. The final sample of six cause groups, eight sectional groups and nine firms was thus based on a variety of additional predefined criteria. Firstly, all firms and civil or consumer associations that only represent national interests were excluded to avoid a national bias. Secondly, with respect to the content of the proposal, interest groups representing a wide variety of interests ranging from telecommunication to publishers were subject to the analysis. Thirdly, the size and importance of the interest with respect to the proposal also played a role. As the bigger companies and associations tend to be more powerful than the smaller ones, they were selected preferentially. Fourthly, in case an interest group did not specify any of its given responses to the Commission's questionnaire in the provided free text fields, it was also excluded from the sample as these fields were subject to the analysis. Lastly, if an interest group participated in the EP's hearing, it was also selected for the analysis of frame selection when approaching the Commission. This was the case for Facebook, Telefónica, Access Now and the European Consumer Organisation (BEUC). Records of Telefónica's and BEUC's presentations to the EP were, however, not publicly available. Intensive research on their own websites, websites such as the EU Observer or Politico for open letters as well as contacting them directly via mail and LinkedIn did not help to acquire the needed documents. Therefore, they could not be selected for this study. An overview of the final selection of interest groups is provided in Table 4.

Table 4

Selected interest groups for frame choice analysis vis-à-vis the Commission

Cause groups	Sectional groups	Firms
Access Now	Application Developers Alliance	Cisco
Bits of Freedom	DIGITALEUROPE	Facebook
Bureau Européen des Unions de Consommateurs (BEUC)	Ecommerce Europe	Google
Center for Democracy and Technology (CDT)	European Telecommunications Network Operators (ETNO)	Microsoft
European Digital Rights (EDRi)	European Internet Service Provider Association (EuroISPA)	Mozilla

Open Rights Group	European Magazine Media Association (EMMA) / European Newspaper Publishers' Association (ENPA)	Nokia
	European Publishers Council (EPC)	Orange
	Groupe Spéciale Mobile Association (GSMA)	Telefónica
		Vodafone

7.1.2. Frame usage

The following section is dedicated to analyzing interest groups's frame choice. They are grouped according to their common goal (fighting for individuals' digital rights) and the sector (telecommunication, digital communication, publisher, advertising) they represent. Direct quotes, taken from their responses to the Commission's public consultation and their position papers, provide evidence for their overall frame use. The frame employment is determined by the highest number of arguments (within one type). An in-depth analysis of the aspects that are highlighted as well as a brief explanation of each organization and an analysis of their individual positions regarding the ePrivacy regulation can be found in Appendices A, B and C.

7.1.2.1. Cause groups

Defending individuals' digital rights

Multiple organizations representing citizens' fundamental rights in the digital sphere are part of the controversial debate of the ePrivacy regulation. These include Access Now, Bits of Freedom, European Digital Rights and the Open Rights Group. As all these organizations defend user's rights online, they also predominantly focus their argumentation on aspects related to public goods. They form the camp that actively supports the Commission's proposal emphasizing in particular that the protection of personal data is a human right. Access Now argues that "[t]he GDPR does not specifically cover the right to private life enshrined in Article 7 of the EU Charter of Fundamental Rights, and specific protections will have to be articulated in the future revised e-Privacy" (Access Now, 2016a). Bits of Freedom draws attention to the inadequacy of the former ePrivacy Directive. It states that it "has failed to achieve full protection of the individual's right to privacy, confidentiality of communications and freedom to seek information without being continuously profiled and monitored online" (Bits of Freedom, 2016). Thus, a revision of the existing ePrivacy rules is needed. In line with this argumentation, EDRi (2016a) stresses that "[t]he European institutions need to make an extra effort to ensure that privacy and confidentiality of communications of European citizens are not considered as a tradeable asset, but as a right to be strongly protected". As the interest groups

used key word combinations such as ‘Charter of Fundamental Rights’, ‘right to privacy’ and ‘right to privacy and confidentiality’ the employment of a human rights frame is indicated. From an economic point of view, these organizations also support the proposal. Access Now (2016a) argues that “the costs arising from the revised ePrivacy rules are justified by the improved safety for users”. Bits of Freedom (2016) discusses that data protection should not be a matter of money. “Privacy protection should not be commodified, leading to different levels of protection depending on how much an individual could afford.” And EDRi (2016a) even emphasizes that “the proposed Regulation will be a boost for innovation and economic growth in Europe.” As all these arguments contain at least one of the key words ‘costs’, ‘money’, ‘innovation’, ‘economic’ and ‘growth’ the use of an economic frame is signaled.

Overall, these analyzed organizations emphasize the need to update the ePrivacy directive to strengthen people's rights and enhance their protection. Their argumentation is predominantly based on arguments of human rights and consumer protection. Thus, as the number of counted public goods arguments exceeds the number of economic arguments for all these organizations, they relied on a public frame when trying to convince the Commission of their positions.

Other sectors

Alongside the dominant lobby groups defending specifically consumers’ digital rights, the European Consumer Organisation (BEUC) represented general consumer interests at the EU level. Aspects of ‘consumer protection’, by using this key word combination, were most prominently highlighted by the organization. It stresses that “[i]t is essential to protect the confidentiality of communications and guarantee a high level of consumer privacy protection across all services” (BEUC, 2016). In light of the increasing importance of OTT for consumers’ communications it highlights that “[t]hese new services are massively used by European consumers but they currently fall outside the scope of the Directive (…). Consumers are not aware and do not understand these differences in protection” (BEUC, 2016). BEUC also points to aspects of human rights. “A robust legal framework that protects consumers’ fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services” (BEUC, 2016). As it uses the key words ‘fundamental rights to privacy’ the employment of a human rights frame is indicated.

The Center for Democracy and Technology (CDT) also lobbied the Commission. CDT does not believe that ePrivacy rules are redundant despite the existence of the GDPR. In contrast, it argues that “[a] compelling argument for proposing a new instrument to replace the

E-Privacy Directive is the fact that the GDPR is not based on Article 7 of the Charter of Fundamental Rights of the EU on the right to privacy and confidentiality of communications" (Center for Democracy and Technology, 2016). In its eyes, GDPR does not sufficiently protect the right to confidentiality of communication, therefore "a new instrument should primarily target the areas not covered by the General Data Protection Regulation (GDPR)" (Center for Democracy and Technology, 2016). By referring to 'Charter of Fundamental Rights' and 'the right to privacy and confidentiality' the use of a human rights frame is indicated. CDT reflects on the economic side to the proposal in more detail than on aspects related to public goods. It stresses in particular the need for technology and innovation-friendly legislation.

> [A] new instrument should (…) built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes" (Center for Democracy and Technology, 2016).

Using words such as 'business' and 'innovation' signal the use of an economic frame. It becomes clear that CDT sees a necessity in adapting existing rules in the way that it enhances consumers' protection while also allowing for innovation.

Overall, while BEUC predominantly stresses public goods aspects and employed a higher number of public goods (16[6]) as opposed to economic arguments (4), CDT elaborates in particular on prospective economic implications by providing 22 economic arguments and only 5 public goods arguments. Thus, BEUC overall employed a public frame while CDT relied on an economic frame.

7.1.2.2. Sectional groups

Telecommunication

Organizations that represent the telecommunications sector heavily lobbied the ePrivacy regulation which is reasonable considering that they are most affected by the proposal. ETNO as well as GSMA which represent established network and mobile operators are subject to this study. While they believe that the Commission's proposal on ePrivacy rightly seeks to create a level playing field between telcommunication and digital service providers offering similar services, they fear that regulatory gaps will remain (ETNO, 2019). GSMA (2016b) provides multiple arguments that include the key words 'consumer/user' in combination with 'protection' which signal the use of a consumer protection frame. It argues that

[6] The number in brackets always indicates the number of arguments provided by the interest group which has been identified through the qualitative content analysis and counting.

> [t]he ePDs current scope does not reflect the converging area of electronic telecommunications where functionally equivalent services are not subject to the same regulatory constraints. Accordingly, the ePD is neither technology-agnostic nor provideragnostic [sic!]. This has led to the problem that users cannot rely on consistent protection standards across the digital market even when using comparable services.

As the argument also contains the key word 'market' it simultaneously signals the use of an economic frame. ETNO (2016) argues that "[t]he coexistence of two different set of rules creates legal uncertainty and confusion, undermining the coherence and trust on the online Consumer Policy, as European citizens cannot rely on consistent protection of their personal data and privacy." Thus, updating the ePrivacy rules would have the opposite effect and would rather weaken consumer protection. With respect to the proposal's security implications, organizations representing telecommunication providers also consider a separate ePrivacy regulation to be superfluous. ETNO (2016) argues that

> [i]n 2009 the ePD introduced for the first time obligations on security for telecom operators; the GDPR has extended the scope of the new rules on security to all sectors seeking a comprehensive, technologically neutral set of rules on security of processing and data breach notifications. Therefore, it does not make sense to maintain dissimilar data breach notifications rules under the ePD.

Thereby, using the key word 'security' implicates the use of crime and security frame. While both organisations share the same opinion and argue similarly on many aspects of ePrivacy, only ETNO provides arguments that contain the key words 'human rights' which indicate the use of a human rights frame. Nevertheless, based on counting the number of provided economic arguments, ETNO still focuses more on the economic implications of the proposal while GSMA presents as many public goods as economic arguments. It stresses the drawbacks of keeping two separate legal instruments. "As long as the ePD coexists with the new GDPR, there will be no level playing field" (ETNO, 2016). The use of key expressions including 'level playing field' thereby indicate the use of an economic frame. ETNO further adds that "[g]enerally, in cases where a competitive market can solve the required objectives through self-regulation, any unnecessary legislation leads to legislative burden and disproportionate costs" (GSMA, 2016a). Using the key words 'competitive', 'market' and 'costs' signals the use of an economic frame.

Overall, organizations representing the telecommunications sector advocate for establishing a viable regulatory framework which allows them to compete with digital communication providers and does not hamper innovation. Both organizations relied on an economic frame, as the number of economic arguments is higher (or as high) as the number of

public goods arguments. However, as GSMA employs as many public goods arguments (13) as economic (13), which derives from the occurrence of the key words (Table 3), it simultaneously relied on a public frame.

Digital communication

The digital communications providers presented an opposing view to the traditional telecommunication companies. They were inter alia represented by EuroISPA. EuroISPA does not see a necessity in keeping a separate ePrivacy regulation. In fact, indicating the use of a human rights frame by using the key words 'Charter of Fundamental Rights', it argues that "the EU Treaty, EU Charter of Fundamental Rights, GDPR Directive and Member States' constitutions all already protect the secrecy of communication (…). New European legislation is not needed to ensure this already existing right" (EuroISPA, 2016). Indicating the use of a consumer protection frame, it argues that, "individuals should always be able to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, but more importantly no law should restrict that ability" (EuroISPA, 2016). Although EuroISPA reflects on public goods aspects, its argumentation on economic aspects is more elaborate. Most importantly, it argues that

> [r]egulation should not unduly interfere with companies freedom to choose and develop innovative business models where there is clear consumer demand. This would be contrary to the fundamental principle that regulation should only be enacted where it is necessary to address a clear issue in the market, and that any regulation should be proportionate and technologically neutral, so as not to favour certain business models or technology over others (EuroISPA, 2016).

Using words such as 'company', 'innovative', 'business' and 'market' thereby clearly characterize an economic frame.

As the number of economic arguments (10) exceeds the number of public goods arguments (7), EuroISPA overall employs an economic frame.

Publisher

The publishers' lobby, including the organizations EMMA/ENPA and EPC representing newspaper and magazine publishers, has been among the most active and vociferous of industry lobbies in the ePrivacy debate. As print media circulations decrease, online advertising has become increasingly important to publishers. Their business model is based on monetising

people's data to generate advertising revenue. Therefore, it is reasonable that they do not welcome the Commission's ePrivacy draft considering that it foresees to change the way personal data can be legally used. All three organizations highlight in particular economic aspects of the proposal, which are highlighted by signal words such as 'innovative', 'companies' and 'business'. ENPA/EMMA (2016b) are concerned that "[a] general consent requirement for the setting of cookies only favours large international companies (…), which base their business models on log-in systems." Thus, they see their members disadvantaged as opposed to the big players. EPC (2016) advocates for minimum intervention in the market as "[c]ontractual freedom is paramount in the free economy and should have as little interference as possible." Additionally, "[i]ndustry has shown responsibility by setting up a self-regulatory program providing simple information to users, but also providing them with the tools to exercise effective choices and control" (European Publishers Council, 2016). These examples of their argumentation clearly indicate the application of an economic frame. Although the business perspective prevails, the publisher's lobby still reflects on the prospective implications for consumer protection, security and human rights. ECP (2016) stresses that "legislation should keep the right balance protecting the privacy of consumers on the one hand and business interests on the other." Using the key word 'protecting' in combination with 'consumer' thereby signals the use of a consumer protection frame. EMMA/ENPA in contrast, only briefly touch upon the aspects of consumer protection and do not provide any crime and security or human rights arguments.

As both organizations provide more economic than public goods arguments which is manifested in their use of the corresponding key words (ECP provided 14 economic and 7 public goods arguments, EMMA/ENPA 12 economic and 2 public goods arguments), they overall rely on an economic frame when approaching the Commission.

Other sectors

Alongside the dominant lobbies of telecos, digital communication providers and publishers, a variety of other organizations lobbied for their members which are affected by the proposal. The Application Developers Alliance, which represents software developers, does not welcome the Commission's proposal in its current form and provides in particular economic justification for it.

> The Apps Alliance believes that none of the actions (…) will help to achieve the objectives of both the Digital Single Market Strategy and the Commission Better Regulation Agenda: increasing consumer trust and creating a competitive market and

> high quality legislation. In fact, while a binding instrument guarantees maximum harmonisation, it also risks to overburden digital industries (Application Developers Alliance, 2016).

Incorporating key words such as ‘market’, ‘competitive’ and ‘industries’ in its argumentation, signals the use of an economic frame. In addition, with respect to its implications for consumers, the Alliance (2017) expresses its concerns: “[W]e are also dubious that the proposed regulation will help achieve better consumer satisfaction or protection” ‘Consumer’ in combination with ‘protection’ thereby indicates the use of a consumer protection frame.

As the leading trade association for digitally transforming industries, DIGITALEUROPE was also involved in the debate on the new ePrivacy rules. It advocates for simplifying the existing legal framework and repealing legislation in case it overlaps with other legislation and represents a burden for businesses. It elaborates on aspects referring to public goods to a greater extent than on economic aspects. By highlighting its concerns that “the ePD creates an unnecessary overlay that could lead to different security requirements and certainly gives rise to different enforcement bodies having the right to issue instructions to service providers, quite possibly in different Member States (…)” (DIGITALEUROPE, 2016b) and in particular using the key word ‘security’, the use of a crime and security frame is indicated. While it “welcomes the European Commission’s suggestion to streamline security requirements and align these with the GDPR”(DIGITALEUROPE, 2018b), it questions the envisaged consent rules. “[C]onsent simply does not make sense. Asking a fraudster’s consent for the purpose of detecting fraudulent activities would hardly be a practical solution” (DIGITALEUROPE, 2018b). Here again the use of a crime and security frame is signaled through addressing the key word ‘fraudster’.

Furthermore, the digital commerce sector was represented by Ecommerce Europe. It overall supports the Commission’s plan to update the existing ePrivacy rules. It argues that there is a need for harmonized European rules as it would profit its members’ businesses. “Ecommerce Europe endorses uniform regulation all over Europe and in that view, it does not favor a choice for national legislators to diverge, which could end up hampering cross-border trade” (Ecommerce, 2016). By addressing the key word ‘trade’, evidence for the use of an economic frame is provided. It furthermore stresses that “[a]s the national provisions are the base for traders in protecting the privacy and personal data of consumers, they certainly have contributed to the increase of consumer trust” (Ecommerce, 2016). This statement simultaneously indicates the use of an economic frame through using the key word ‘trade’ as

well as the use of a consumer protection frame by referring to ‘protecting’ in combination with ‘consumer’.

Overall, the Application Developers Alliance as well as Ecommerce Europe relied on an economic frame for their argumentation vis-à-vis the Commission (making use of 19 economic arguments and ten public goods arguments and 18 economic arguments and five public goods arguments respectively), while DIGITALEUROPE provided more public goods arguments (51) than economic arguments (41) and thus relied on a public frame.

7.1.2.3. Firms

Telecommunication

The telecommunications firms[7], represented by Cisco, Nokia, Orange, Telefónica and Vodafone in this study, have been among the most active lobbyists on the ePrivacy regulation. A key demand has been to ensure that the OTTs are brought within the remit of the new ePrivacy rules. The arguments provided overall indicate that they welcome the Commission’s proposal in the regard that it envisages to cover OTTs. However, in its current form and with regard to the newly reformed GDPR, they would recommend withdrawing from the current proposal as they do not see any added value in it. The imbalances that exist between telecommunication firms and OTTs as well as the unfair competition that results from it, are two recurring arguments made by the telecommunication firms. Nokia (2016b) elaborates that “[i]t is not appropriate to impose different data protection obligations on providers of functionally equivalent services depending on whether they are OTT and other information society providers or traditional telecommunications companies (…). This may impede innovation and hinder future legitimate uses of these data”. Orange (2016) states that

> unlike telcos, OTT are global players that are allowed to commercially exploit the traffic data and the location data they collect. However, there is no technical or legal reason to consider that traffic and location data collected from telcos and OTT should be treated differently by regulators and competition authorities.

Telefónica (2016) emphazises that “[t]he uneven application of privacy and data protection rules for equivalent services destroys the ability for these players [telecommunication firms] to compete on equal footing in a single market.” As these arguments include key words such as ‘companies’, ‘innovation’ or ‘competition’, they point to the use of an economic frame.

[7] The telecommunications firms include telecommunication operators as well as network hard- and soft-ware providers

Simultaneously, referring to 'exploit" characterizes a crime and security frame. The telecommunication firms are also concerned that it would not improve consumer's protection while benefiting the dominant players in the data economy. They do not only believe that the unequal treatment of communication providers harms competition, but it also negatively affects security and consumer protection. Orange (2016) stresses that "European citizens cannot rely on European rules to consistently protect their privacy." As this argument contains they key word 'protect' in combination with 'citizens' it signals the use of a consumer protection frame. Highlighting aspects of 'security', these firms outline that a separate legal instrument is not necessary. In contrast, Cisco (2016a) argues that "the ePD creates an unnecessary overlay that could lead to different security requirements" (Cisco Systems, 2016b). In line with this argumentation, Nokia (2016b) emphazises that "[s]ecurity provisions in European legislation should be consistent, complimentary and not duplicate or overlap with each other". The recurring key word 'security' indicates the emplyoment of a crime and security frame. Whereas the telecommunication firms do not specifically discuss that the protection of communication and privacy is a legal right that individuals have, they naturally refer to it in their argumentation. Telefónica states that "there is no need for complementing the right of confidentiality of communications with additional legal provisions on encryption regarding the communication between individuals, especially as they cannot keep pace of technology developments". The 'right of confidentiality of communications' thereby signifies the use of a human rights frame. Overall, the telecommunication firms agreed that OTTs need to be covered by the new legislation in order to create a level playing field for all business. However, they call for a review of the Commission's proposal.

Four of the five analyzed telecommunication firms provided more public goods arguments than economic arguments, which can be determined by the occurrence of the corresponding signal words. Thus, they employed a public frame. Nokia is the only of these firms that relied on an economic frame as it provided twice as many economic arguments (10) as public goods arguments (5).

Digital communication

Digital communication providers, represented by Facebook, Google, and Microsoft in this study, whose business models rely to some extent on making money from online advertising, have an interest in rejecting the new ePrivacy rules, or making them as weak as possible. These firms opposed to the adoption of new ePrivacy rules and articulated shared industry concerns about the damage to their business models. Facebook (2016) elaborates that

"[i]n a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to decide their business models, as long as the privacy rights of the users are cared for and safeguarded." Using the key words 'economy', 'growth', 'companies' and 'business' thereby suggests the use of an economic frame, while 'privacy rights' indicates the simultaneous use of a human rights frame. The firms are concerned about ensuring their market dominance and even propose that "regulators should perhaps consider removing telecoms regulations where no longer necessary to protect consumers or competition" (Facebook, 2016a). This argument simultaneously indicates the use of a consumer protection and economic frame as the key words 'protect consumers' and 'competition' respectively are used. Microsoft's view on the impact of the proposal for its business model is less strict. The firm elaborates that "[w]e believe that innovation and competition flourish best when companies can freely choose how to structure their business" (Microsoft, 2016). This argument is a prime example for the use of an economic frame as it contains even multiple signal words: 'innovation' 'competition' and 'companies'. Although the firms do not discuss aspects of security and consumer protection in equal detail, they share their stance that a separate legal instrument for consumer protection and safety is not necessary. Google (2016) argues that "[t]he GDPRs security and personal data breach notification obligations are built on the ePDs rules, turning these into a general obligation for all data controllers". 'Security' and 'breach' therby signal the use of a crime and security frame. Remarkably, they also highlight that data protection and privacy are fundamental rights that every individual possesses. Facebook (2016a) refers to "[t]he Charter of Fundamental Rights [which] states [that] everyone has the right to respect for his or her private and family life, home and communications. Confidentiality of communication is guaranteed as a fundamental right under Art. 7 (Respect for private and family life) of the Charter". Google (2016) equally acknowledges this right and expresses that "[t]he right to privacy and confidentiality are important fundamental rights" and Microsoft (2016) specifically states that "[d]ata protection is a human right." Thus, including key words such as 'Charter of Fundamental Rights' or 'fundamental right' signify the use of a human rights frame.

Overall, all three digital communication providers use more economic arguments than public goods arguments and thus relied on an economic frame.

Other sectors

Mozilla was the only analyzed firm which neither belonged to the group of telecommunication operators nor to the group of digital communication providers. Light on its

argumentation will thus be shed individually. Mozilla is generally supportive of the proposal and confirms the need to update ePrivacy rules. It argued that "[r]ules of the road that provide a baseline level of protection of user privacy and the increasing amount of data that can be collected, shared, and stored via the internet of things are demonstrably useful" (Mozilla, 2016). As this argument contains the key words 'protection' in combination with 'consumer' it is an indicator for a consumer protection frame. The firm also acknowledges that the protection of the confidentiality of communication is a human right. It emphazises that "Article 7 of the Charter of Fundamental Rights establishes the right of individuals to secure their communication" (Mozilla, 2016). Reflecting on the proposal's economic implications, Mozilla most prominently argues that there is a need for harmonizing and aligning regulations in order to facilitate cross border- business and compliance with it. "For technology companies hoping to do business across the EU, this provides compliance difficulty and risk" (Mozilla, 2016). The use of the signal words 'business' and 'industry' therby characterizes an economic frame. In contrast to other firms, however, Mozilla prioritizes aspects of consumer protection over economic aspects and overall employed a public frame. This is manifested by the greater quantity of counted public goods arguments (21) as opposed to economic arguments (18).

7.2. European Parliament

The EP, more specifically the responsible LIBE Committee held a hearing on 11 April 2017. It was organized to discuss three overarching issues of the proposed ePrivacy regulation. The first session dealt with institutional aspects, the second focused on the aspect of legal consistency with other legal instruments as well as the creation of a level playing field and the last session centered around the issue of confidentiality and security of communications (Committee on Civil Liberties, Justice and Home Affairs, 2017).

7.2.1. Identification of involved interest groups

Overall, ten stakeholders were invited to share their point of view on the proposed ePrivacy regulation with members of the EP. However, speakers' notes of two of the participating stakeholders were not publicly available and could not be obtained through directly contacting them. On written request, Bureau Européen des Unions de Consommateurs (BEUC) stated that no document had been submitted and was also not archived internally. No reply was received from Telefónica. Attempts to request the missing documents by telephone were also unsuccessful, as nobody could be reached. They were thus excluded from the sample.

As four stakeholders could not be classified as either of the three predefined types of interest groups, they were also excluded from the sample. Overall, eight interest groups were subject to the analysis (Table 5).

Table 5:

Overview of involved interest groups in the EP hearing

Name	Description	Type of interest group according to their organizational form (see theoretical framework)	Selected for analysis
European Data Protection Supervisor	EU independent data protection authority		No
Institute for Information Law, University of Amsterdam	Academia		No
Telefónica	Telecom industry	firm	No[a]
Schibsted Sverige	Advertising/publisher sector	firm	Yes
Access now	NGO	cause group	Yes
Goethe University Frankfurt	Academia		No
Symantec	Industry	firm	Yes
Bureau Européen des Unions de Consommateurs (BEUC)	Umbrella group defending Europe‘s consumer views	cause group	No[a]
Garante per la Protezione dei dati personali	Italian national data protection authority		No
Facebook	Social networking website	firm	Yes
Total included		**3 firms** **1 cause group**	**4**

a Data was not publicly available on the EP’s website and could also not be acquired through additional intensive desk research, directly contacting via mail and LinkedIn or calling.

7.2.2. Frame usage

7.2.2.1. Cause group

Two cause groups testified in the hearing before the LIBE Committee, namely Access Now and Bureau Européen des Unions de Consommateurs (BEUC).

Defending individual’s digital rights

Access Now defends and extends the digital rights of users at risk around the world (Access Now, 2020). It most strongly highlights that “[t]o respect the fundamental rights of

privacy and data protection is not a favor, it is a legal obligation" (Hidvegi, 2017, May 17). Furthermore, it argues that "in order to meet the requirements of the EU Charter of Fundamental Rights and achieve legal consistency with the General Data Protection Regulation we must indeed level the playing field" (Hidvegi, 2017, May 17). By drawing attention to 'fundamental rights of privacy and data protection' and the 'Charter of Fundamental Rights' the usage of a human rights frame is indicated. According to the frame classification, the use of the expression 'level playing field' typically highlights the use of an economic frame (Table 3). This argument is, however, a prime example that underlines the importance of neighboring words and sentences. In fact, in this case the context changed the classification of argument type. Access Now explains that the playing field must not be levelled between telecommunication companies and OTT service providers but between businesses and consumer who do not have sufficient control of their personal information and lack access to information.

> "The playing field must be levelled to protect users because the field is uneven: telcos and online service providers are both in a dominant position compared to the users due to the lack of information and transparency. A level playing field for users would address this information asymmetry (Hidvegi, 2017, May 17).

Thus, in this case, 'level playing field' does not highlight an economic argument. In combination with 'levelled to protect users' the use of a consumer protection frame is signalled. Furthermore, Access Now addresses some economic aspects. However, these mostly serve to strengthen consumer protection arguments. It outlines for instance that "[t]he primary public interest is the legal and technical protection of people and not cementing semi- or fully unlawful business practices" (Hidvegi, 2017, May 17). And further, "[t]he European Union has taken the first steps to create the Digital Single Market which can only be successful if the trust of European citizens is regained" (Hidvegi, 2017, May 17). Still, using the key words 'business' and 'market' indicate the use of an economic frame.

Overall, consumer protection is clearly the center of attention of Access Now's argumentation. As it uses six arguments related to public goods and four economic arguments, it overall employs a public frame.

7.2.2.2. Firms

Overall four firms were invited to the EP's hearing. Due to data unavailability of Telefónica's speech, the analysis will focus on Schibsted Sverige, Symantec and Facebook.

Advertising

Schibsted Sverige was invited to the EP's hearing to represent advertising companies. It unites international digital consumer brands and provides digital services that empower consumers (Schibsted, 2020). Schibsted considers the regulation to be of great importance due to the fact that it strengthens consumers' protection and helps European companies to "compete with the global players to ensure independent, pluralistic, and accessible European press" (Grünthal, 2017, May 17). The occurrence of the key word 'compete' thereby signals the use of an economic frame. The proposal's impact on the free press and data driven advertising in particular was emphasized. The European free press depends on its ability to deliver effective advertising to generate revenue from it. However, this has become challenging as the big players, such as Google and Facebook, possess much larger volumes of data as compared to smaller companies. Schibsted's main argument focuses on the discrimination of smaller firms as compared to the big players which would be enhanced by the new ePrivacy regulation. Looking more closely at Schibsted's presentation (Appendix B), it becomes clear that it outlines the characteristics of the current advertising landscape in great detail while expressing its own position concerning the new ePrivacy regulation only briefly. It refers to the "[n]eed for flexible rules to promote user empowerment and transparency; to secure a level playing field; and to allow for innovation" (Grünthal, 2017, May 17). Referring to 'level playing field' and the need for flexible rules that "allow for innovation […] to compete with the global players" (Grünthal, 2017, May 17) indicate the use of an economic frame.

As Schibsted Sverige only used three economic and no other arguments, it overall employed an economic frame.

Digital communication

Facebook, which represents digital communication providers, elaborates extensively on its position concerning the new privacy regulation. On the one hand, Facebook highlights the need for adequate security instruments. It stresses that "[b]ad actors won't consent. Think about the spam, malware, and child exploitation cases I mentioned above. If you were a bad actor, why would you agree to such processing?" (Strahs, 2017, May 17). As this argument contains the key words 'malware' and 'exploitation', the employment of a crime and security frame is indicated. Moreover, it provides multiple examples contributing to strengthening consumer protection: "I wanted to talk to you today about the services we and others are working on to help people express themselves and stay connected with their loved ones in a safe and secure way" (Strahs, 2017, May 17). 'Loved ones' which are 'consumers' in combination with 'safe

and secure' indicate the use of a consumer protection frame. On the other hand, Facebook also reflects on potential obstacles to new innovation and growth resulting from the revision of the ePrivacy directive. "[A]s currently drafted, [it] threatens to hold back the artificial intelligence and big data innovation" (Strahs, 2017, May 17). 'Innovation' is the key word that identifies an economic frame. Facebook urges the Commission to adapt it proposal stating, "[w]e believe the Parliament has an opportunity to reform the proposal so that it does more to encourage growth in these services while also protecting privacy" (Strahs, 2017, May 17).

As Facebook uses five public good arguments and four economic arguments determined by the use of the corresponding key words, it overall employed a public frame.

Other sectors

Symantec Corp. engages in the provision of security and systems management solutions (Forbes, 2020). Symantec predominantly focuses on the security aspect of the proposed ePrivacy regulation. As discussed, it can be difficult to differentiate between individual security and collective security. From the context, which does not refer to consumers or users at any point, it can be assumed that collective security is the center of attention in Symantec's argumentation. It argues that ePrivacy is an important component of the security landscape. However, in its current format, the "[n]ew ePrivacy Regulation (...) weakens security" (Chantzos, 2017, May 17). The "[f]ocus needs to be on capabilities to be achieved to deliver security as opposed to a generic obligation to deliver a confidential environment" (Chantzos, 2017, May 17). There will be "[l]ess protection because fewer organisations can collect security relevant info (…)" (Chantzos, 2017, May 17). Thus 'security' clearly indicates the use of a crime and security frame. Additionally, Symantec also discusses its potential economic impact. It highlights aspects of 'growth' and 'competitiveness' which signals the use of an economic frame. More precisely, Symantec argues that "[t]he more restrictive the framework is for metadata the less likely is for EU businesses to grow in new/big data sectors [and] [l]ess growth = less jobs, less innovation, less competitiveness" (Chantzos, 2017, May 17). According to Symantec there is also a "need for harmonized approach for doing business in Europe" (Chantzos, 2017, May 17).

Counting the number of arguments, Symantec refers to four security arguments while addressing three economic arguments. Thus, it employs a public frame.

Overall, two firms employed public frames (Facebook, Symantec) while one firm employed an economic frame (Schibsted Sverige). Facebook and Symantec used a public frame as the number of arguments related to public goods exceeds the number of economic arguments.

8. Discussion of findings

Based on the theory of 'two logics of interest groups', two hypotheses have been formulated. These will be tested against the findings of the analysis.

8.1. The logic of membership

To recall, the first hypothesis states that frame choice varies systematically across the types of interest groups. Cause groups will employ public frames, sectional groups economic frames and firms will show a great diversity of frames. In order to test this hypothesis, the argumentation of six cause groups, eight sectional groups and nine firms (Commission) and one cause group and three firms (EP) have been analyzed and compared with respect to the ePrivacy regulation.

8.1.1. Frame choice approaching the Commission

Table 6 illustrates that frame choice varies significantly across type of interest group. It is important to highlight that the total number of arguments made by interest groups does not play a major role as only the ratio between public goods and economic arguments is decisive for the identification of frames.

Overall, five of the six cause groups used a public frame which reflects the position of their members. In addition, most of these cause groups, with one exception, used at least twice as many public goods arguments as economic arguments. Within the category of public frames, all three types, consumer protection, crime and security and human rights, were roughly equally popular. The only outlier among cause groups is the Center for Democracy and Technology (CDT) which used twice as many economic arguments as public goods arguments. Based on the organization's name and its mission one can to some extent explain its reliance on an economic frame. CDT describes itself as "a champion of global online civil liberties and human rights, driving policy outcomes that keep the internet open, innovative, and free" (Center for Democracy and Technology, 2020a). This statement clearly shows the organization's dual focus on both public goods aspects and economic aspects. Therefore, it could even be questioned whether, strictly speaking, CDT is a cause group. None of the other analyzed cause groups is so obviously also committed to an economic purpose. In addition, the organization consists of staff, a Board and an Advisory Council. The Board, which serves as the CDT's

governing body, consists of leading representatives from a variety of firms including tech firms such as Microsoft and Mozilla Corporation, law firms, lobbying and communication firms as well as public institutions including George Washington University. The Advisory Council provides CDT with expertise knowledge. Although employees from tech companies like Facebook and Twitter are members of the Council, it is specifically stated that they only "serve in their personal capacity" (Center for Democracy and Technology, 2020b). Therefore, as CDT does not have a formal membership structure representing very specific interests, it does not need to adhere to members position but can act more freely.

In contrast, nearly all sectional groups relied on an economic frame. Digital Europe is the only outlier and employed a public frame. Its members are exclusively corporate members and national trade associations which clearly represent private interests. Thus, its membership structure cannot explain why the result deviates from the hypothesis. Its mission and policies, which focus on topics concerning the digital transformation, including Artificial Intelligence and Cybersecurity, also do not offer an explanation. Therefore, an explanation for their reliance on a public frame cannot be adequately provided. Additionally, GSMA, representing the global mobile communications industry, was the only sectional group that provided the same number of public goods and economic arguments and therefore simultaneously relied on a public and an economic frame. GSMA members include "handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors" (GSMA, 2020). They "work towards common goals, around hot topics such as 5G, RCS, IoT, Roaming, Security and SIM Technology" (GSMA, 2020). Thus, alongside pursuing economic goals that are related to new technological developments, it is concerned with the public goods aspects of security. Therefore, its equal elaboration on both economic and public goods aspects reflects its goals.

The firms that have been subject to the analysis did not employ a specific type of frame preferentially. They showed the greatest flexibility with regard to their frame choice, as they are not constrained by any members. Both types of frames, public and economic frames, were used to an equal extent. More specifically, five firms relied on public frames while four firms employed an economic frame. Comparing the number of public goods and economic arguments for each firm revealed, however, that the frame choice was not always as clear as for cause groups. For instance, Google employed eight public goods arguments and nine economic arguments. It was noticeable that those companies already subject to the current ePrivacy Directive, namely the traditional telecommunication providers such as Orange, Telefónica and Vodafone, relied mostly on public frames. In contrast, most digital communications firms

employed an economic frame, which is reasonable as they try to convince the Commission of the negative influence it would have for their business models. Thus, in this case, interest groups' frame choice corresponded to their actual preferences which is not necessarily the case for all interest groups.

Overall, despite minor outliers, the first hypothesis can be confirmed for all three types of interest groups. Thus, frame choice varies systematically across type of interest group. While cause groups predominantly relied on public frames and sectional groups on economic frames, firms employed both types of frames. This also suggests that the logic of membership influences interest group frame choice.

Table 6:

Frame choice by interest group type (number of frames) vis-à-vis the Commission

Interest group	Type of frame				Sum
	Public frame			Economic frame	
	Consumer protection frame	Crime and security frame	Human rights frame		
Cause groups					
Access Now	23	13	21	19	**76**
		57			
BEUC	9	0	7	4	**20**
		16			
Bits of freedom	4	3	15	5	**27**
		22			
CDT	1	5	5	22	**33**
		11			
EDRi	2	8	6	14	**30**
		16			
Open Rights Group	2	4	5	4	**15**
		11			
Sum		133		68	**201**
Sectional groups					
Application Developed Alliance	5	5	0	19	**29**
		10			
DIGITALEUROPE	14	28	9	41	**92**
		51			
Ecommerce Europe	3	1	1	18	**23**
		5			
ETNO	10	4	5	30	**49**
		19			
EuroISPA	3	1	3	10	**17**
		7			
EMMA/ENPA	2	0	0	12	**14**
		2			
European Publishers Council	3	2	2	14	**21**
		7			
GSMA	7	6	0	13	**26**

Interest group	Type of frame				Sum
	Public frame			Economic frame	
	Consumer protection frame	Crime and security frame	Human rights frame		
		13			
Sum		114		158	**272**
Firms					
Cisco Systems	6	13	5	16	**40**
		24			
Facebook	8	3	2	16	**29**
		13			
Google	3	1	4	9	**17**
		8			
Microsoft	1	6	3	19	**29**
		10			
Mozilla	8	10	3	18	**39**
		21			
Nokia	1	2	2	10	**15**
		5			
Orange	12	4	4	15	**35**
		20			
Telefónica	9	4	5	17	**35**
		18			
Vodafone	7	7	3	15	**32**
		17			
Sum		136		135	**271**

Note. The grey fields highlight the highest number of arguments per interest group and thus indicates its overall frame usage.

Source: Own illustration of the research findings

8.1.2. Frame choice approaching the European Parliament

Due to the limited number of interest groups that have been analyzed, it is more difficult to assess whether frame choice varies systematically across type of interest group when approaching the EP. However, even the few interest groups' argumentations should then be consistent with the hypothesis. In line with the first hypothesis, the only cause group that has been subject to the analysis, employed a public frame. As hypothesized, firms also showed variation in frame employment. Two firms relied on a public frame while one firm relied on an economic frame. No statement can be made about sectional groups, as these were not part of the analysis (Table 6).

For the European Parliament, the first hypothesis can therefore also be confirmed with reservation. The interest groups at stake employed frames that correspond to their constituency structure. As the only cause group, Access Now, employed a public frame which reflects its

objective to fight for a public good, namely to defend and extend users' digital rights. Among the firms, which do not have any members, variation in frame employment could be identified.

Table 7:

Frame choice by interest group type (number of frames) vis-à-vis the EP

Interest group	Type of frame				Sum
	Public frame			Economic frame	
	Consumer protection frame	Crime and security frame	Human rights frame		
Cause groups					
Access Now	3	0	3	4	**10**
	6				
Firms					
Facebook	2	3	0	4	**9**
	5				
Schibsted Sverige	0	0	0	3	**3**
	0				
Symantec	0	4	0	3	**7**
	4				
Sum	16			14	**30**

Note. The grey fields highlight the highest number of arguments per interest group and thus indicates its overall frame usage.

Source: Own illustration of the research findings

8.2. The logic of influence

8.2.1. Frame choice approaching the Commission

It was expected that the *logic of influence* has an effect on interest groups' frame choice. According to this logic, interest groups should tailor their frames towards the decision-makers and the corresponding characteristics of the institution in order to influence them (Klüver, Mahoney & Opper, 2008). More specifically, the second hypothesis states that frames that interest groups employ are specifically tailored towards the DG in charge of drafting the proposal. In this case, the Directorate General Communications Networks, Content and Technology (DG CONNECT) took the lead in drafting the legislative proposal of the ePrivacy regulation. Its work focuses on developing "a digital single market to generate smart, sustainable and inclusive growth in Europe" (Directorate-General CONNECT, 2020). As this DG clearly focuses on economic aspects, interest groups were expected to primarily rely on the use of economic frames. However, deriving from the analysis, this link cannot be clearly

confirmed. The interest groups at stake did not seem to have adopted their frames specifically to the preferences and beliefs of the primarily responsible DG. In fact, almost all cause groups and every second firm relied on employing a public frame. Only sectional groups made most use of economic frames and thus are consistent with the second hypothesis. Therefore, H2.1 cannot be fully confirmed, thus interest groups did not specifically tailor their frames towards the DG in charge of drafting the proposal. Noteworthy is, that especially the large tech companies, including Facebook, Google and Microsoft, which are amongst the most powerful players in the field of digitization worldwide, relied on economic frames and were thus in line with the DG's orientation.

8.2.2. Frame choice when approaching the European Parliament

Applying the logic of influence to the EP, interest groups were expected to adapt their framing strategy to the characteristics of the EP committee responsible for handling the revision of the ePrivacy directive. Hypothesis 2 states that frames that interest groups employ are tailored towards the EP committee in charge. The responsible committee was the Civil Liberties, Justice and Home Affairs (LIBE) Committee, which "is in charge of most of the legislation and democratic oversight for policies enabling the European Union to offer its citizens an area of freedom, security and justice (Article 3 TEU)" (López Aguilar, 2019). The committee clearly focuses on public goods matters including "the fight against international crime and terrorism, the protection of the rule of law and fundamental rights [and] ensuring data protection and privacy in a digital age" (López Aguilar, 2019). Accordingly, interest groups were expected to rely on public frames. The only cause group that has been subject to the analysis, Access Now, employed a public frame. However, as its membership structure and overall mission also indicate the use of a public frame, it is difficult to assess whether or to what extent the addressee played a role in the organization's choice of arguments. Additionally, two of the three analyzed firms (Facebook and Symantec) employed a public frame, while the other firm (Schibsted Sverige) employed an economic frame. Due to the limited number of analyzed interest groups, it is difficult to assess whether H2.2 can be confirmed, thus whether interest groups tailor their frames towards the EP committee in charge. One of the four interest groups did not employ a frame that matches the beliefs and interests of the LIBE committee. Furthermore, there is still some uncertainty whether and to what extent other factors, such as the organization's or firm's own mission and orientation as well as its membership structure might have been the dominant factor influencing interest group frame choice.

As two interest groups, namely Access Now and Facebook participated in both the Commission's questionnaire and the EP's hearing, these were compared individually. It

allowed to draw more reliable conclusions on whether frame choice is affected by the institutional properties of the European Commission and the European Parliament accordingly. Whereas Access Now employed a public frame vis-à-vis both EU institutions, Facebook employed an economic frame when approaching DG CONNECT and a public frame when approaching the EP Committee LIBE. This suggests, that Facebook tailored its argumentation towards the interests and beliefs of the responsible DG and EP committee in order to influence the policy outcome in contrast to Access Now which strictly adhered to its orientation on public goods.

9. Conclusion

This final chapter is dedicated to the conclusion. It serves to answer the central research question by reflecting on the two hypotheses. It will further elaborate on the study's limitations and practical implicatins.

9.1. Answering the central research question

This study pursued to answer the central research question "*To what extent do the types of interest groups and European institution affect interest group frame selection in case of the ePrivacy regulation?"* The theory of the two logics of interest groups developed by Klüver, Mahoney and Opper (2015) served as the study's theoretical basis. A qualitative content analysis of interest groups' responses to the Commission's public consultation, supplementary position papers and speaker's notes for the EP hearing has been conducted. Choosing a qualitative approach allowed to unveil important mechanisms that drive frame selection, which would not have been possible using a quantitative approach.

In order to systemtically organize the textual data of this study and increase the reliability of the research findings, hand-coding has been complemented by using the qualitative content analysis software MAXQDA. MAXQDA facilitated a clear and thorough analysis and enabled to reliably code and analyze the data with its word frequencies and word combinations tools. For qualitative research in general, MAXQDA further allows to explore and analyze a wide variety of data types ranging from text documents to survey data (Kuckartz, Rädiker, 2019, p.1).

The study's findings suggest that frame choice varies systematically across type of interest group. When lobbying the Commission, almost all cause groups employed a public frame, almost all sectional groups employed an economic frame and firms employed both types of frames to an equal extent. H1, which states that *frame choice varies systematically across type of interest group* was thus confirmed and suggests that the membership structure has an impact

on interest groups' frame choice. Additionally, the findings also suggest that frame choice is not necessarily affected by the institutional characteristics of the Commission and the EP accordingly. Not all types of interest groups necessarily adapted their frames towards the DG CONNECT which has been lobbied. They did not preferentially employ an economic frame that matches the DG's orientation. In fact, only sectional groups predominantly relied on an economic frame. Within the groups of firms, it was noticeable that the digital communications providers employed an economic frame while most of the traditional telecom companies employed a public frame. Vis-à-vis the LIBE Committee in the EP, which focuses on public goods, three out of four interest groups employed a public frame. While this indicates that they tailored their frames towards the responsible Committee, it cannot be disregarded that other factors may have had an influence on their frame selection. The assigned topics of each of the hearing's sessions for instance steered the interest groups' argumentation. Whether the logic of influence really holds true for the analyzed sample, could be best assessed by comparing the frame choice of those interest groups that participated both in the Commission's consultation and the EP's hearing. While Access Now employed a public frame approaching both institutions, Facebook adapted its frames towards the venue that has been lobbied. It employed an economic frame vis-à-vis the Commission and a public frame vis-á-vis the EP. Thus, the findings of the analysis suggest that the logic of influence only holds true for Facebook which changed its frame in order to influence the responsible institution the best possible way. H2, claiming that *frame choice is affected by the institutional properties of the European Commission and the European Parliament accordingly*, could thus overall not be fully confirmed.

9.2. Limitations of the research

One of the most obvious limitations of the study is the small number of interest groups in the case of the EP, which did not allow to draw trustworthy conclusions from it. In particular, as none of the interest groups that testified in the EP's hearing could be classified as a sectional group, this group was not part of the analysis of frame choice when approaching the EP, which also limited the possibility of comparison with the Commission. Secondly, data inconsistencies occurred. Data for some interest groups were not accessible. Thirdly, it should also be noted that interest groups were not entirely free to elaborate on their positions, since they were responding to the Commission's questions or were invited to the EP's hearing which discussed a specific aspect of the proposal. Fourthly, as the classification of frames was only based on the occurrence of key words and word combinations it did not take the strength of arguments into consideration. An expression might have only been a side note but due to the occurrence of a

key word and word combination it is treated as a full standing argument. Fifthly, this study has specifically analyzed public and economic frames. This inherently means that other arguments which could not be classified as such were ignored. In the case of the ePrivacy regulation, interest groups also elaborated quite extensively on the relevance and necessity of a separate ePrivacy regulation considering that the newly revised GDPR already covers digital communication. Reflections on these 'other frames' have thus not been made, although they were also important integral parts of the Commission's consultation. Lastly, with regard to the substantive focus on the ePrivacy regulation, it is noticeable that the topic is closely related to the GDPR and thus also some provided arguments did not exclusively address the ePrivacy regulation.

9.3. Recommendations for future research and practical implications

The identification of frames in this study was not exhaustive and research could be extended by taking other types of frames (Table 1) into consideration. Additionally, the study's scope could be further increased by including the Council and taking a look at the different member state's stances towards the proposal. This would, however, require more time and resources. Policy debates in other fields could also be examined qualitatively. This would not only allow to get an equally detailed insight into the interest groups' framing strategies of other debates, but it would also enable to compare framing strategies across different policy fields.

This research has revealed that analyzing interest group frame selection has important practical implications. The process of highlighting certain aspects while ignoring others is a strategic choice. Analyzing framing strategies is particularly relevant because they are expected to influence the course of public policy. As this study has identified that interest groups' organizational structures influence their choice of frames, decision makers are provided with empirical proof that consulting different types of interest groups makes sense in order to make sound decisions that are informed by multifaceted accounts of arguments regarding the policy proposal at stake. Additionally, while it is commonly believed that interest groups adapt their argumentation towards their targets, this study could not confirm this assumption. Interest groups might in fact work more objectively than people think. Thus, this research encourages citizens to broaden their perception of interest groups. More generally, EU citizens' as well as policy-makers' knowledge about lobbying strategies could furthermore be expanded. Lastly, considering that the analyzed policy debate has attracted many lobbyists who highlighted different aspects of the policy proposal on the ePrivacy regulation, it has become clear how impactful but also controverse the topic is.

10. Reference List

Access Now. (2016a). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://www.accessnow.org/cms/assets/uploads/2016/07/ePRIVACY-Review-Access-Now.pdf.

Access Now. (2016b). Review of the e-Privacy Directive. Retrieved from https://www.accessnow.org/cms/assets/uploads/2016/07/ePrivacy-Review-Policy-Paper-1.pdf.

Access Now. (2020). Our mission. Retrieved from https://www.accessnow.org.

Application Developers Alliance. (2016a). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Application Developers Alliance. (2016b). Position paper on the Proposal for an E-Privacy Regulation. Retrieved from https://static1.squarespace.com/static/53864718e4b07a1635424cdd/t/592798b217bffcf51487afa7/1495767220070/Developers+Alliance_PositionPaperePrivacyRegulation_May+2017.pdf.

Atikcan, E. Ö, & Chalmers, A. W. (2019). Choosing lobbying sides: The general data protection regulation of the European Union. *Journal of Public Policy, 39*(4), 543-564. doi: 10.1017/S0143814X18000223.

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis, Educational Research, 45(2), 143-154, doi: 10.1080/0013188032000133548.

Baumgartner, F. R. (2007). EU lobbying: A view from the US. *Journal of European Public Policy, 14*(3), 482-488. doi: 10.1080/13501760701243830.

Baumgartner, F. R., Berry, J. M., Hojnacki, M., Kimball, D. C & Leech, B. L. (2009). Lobbying and policy change: Who wins, who loses, and why. *University of Chicago Press*.

Baumgartner, F.R., De Boef, S.L. and Boydstun, A.E. (2008) The Decline of the Death Penalty and the Discovery of Innocence, Cambridge: Cambridge University Press.

Baumgartner, F. R., & Mahoney, C. (2008). Forum Section: The two faces of framing. *European Union Politics, 9*(3), 435-449. doi:10.1177/1465116508093492.

Bernhagen, P., Dür, A., & Marshall, D. (2015). Information or context: What accounts for positional proximity between the European Commission and Lobbyists? *Journal of European Public Policy, 22*(4), 570-587. doi: 10.1080/13501763.2015.1008556.

Beyers, J. & Braun, C. (2014). Ties that count: Explaining interest group access to policymakers. *Journal of Public Policy, 34*(1), 93-121. doi:10.1017/S0143814X13000263.

Beyers, J., Eising, R., & Maloney, W. (2008). Researching Interest Group Politics in Europe and Elsewhere: Much we study, little we know? *West European Politics, 31*(6), 1103-1128. doi: 10.1080/01402380802370443.

Biliouri, D. (1999). Environmental NGOs in Brussels: How powerful are their lobbying activities? *Environmental Politics, 8*(2), 173-182. doi: 10.1080/09644019908414472.

Binderkrantz, A. S. (2019). Interest group framing in Denmark and the UK: Membership representation or public appeal? Journal of European Public Policy,1-21. doi:10.1080/13501763.2019.1599041.

Bits of Freedom. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-civil-society-and-consumer-associations-public-consultation-evaluation.

Bits of Freedom. (2020). About bits of freedom. Retrieved from https://www.bitsoffreedom.nl/english/.

Blatter, J., & Blume, T. (2008). In search of co-variance, causal mechanisms or congruence? towards a plural understanding of case studies. *Swiss Political Science Review, 14*(2), 315-356. doi:10.1002/j.1662-6370.2008.tb00105.x.

Blatter, J. & Haverland, M. (2014). *Designing case studies. Explanatory approaches in small-N research* (2nd ed.). Basingstoke, Hampshire, England: Palgrave Macmillan.

Boräng, F. & Naurin, D. (2015). Try to see it my way! Frame congruence between lobbyists and European Commission officials, Journal of European Public Policy, 22(4), 499-515, doi: 10.1080/13501763.2015.1008555.

Bouwen, P. (2002). A comparative study of business lobbying in the European Parliament, the European Commission and the Council of Ministers. Retrieved from https://www.mpifg.de/pu/mpifg_dp/dp02-7.pdf.

Bouwen, P. (2004). 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. doi:10.1111/j.1475-6765.2004.00157.x.

Brandsma, G.J. (2019). Transparency of EU informal trilogues through public feedback in the European Parliament: promise unfulfilled, *Journal of European Public Policy, 26*(10), 1464-1483, doi: 10.1080/13501763.2018.1528295.

Bryman, A. (Ed.). *Social research methods* (5th ed.). Oxford, United Kingdom: 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. doi:10.1080/13501763.2014.936483.

Bunea, A., & Ibenskas, R. (2015). Quantitative text analysis and the study of EU lobbying and interest groups. *European Union Politics, 16*(3), 429-455. doi:10.1177/1465116515577821.

Bureau Européen des Unions de Consommateurs. (2016). Consultation on the review of the e-Privacy Directive. Summary of BEUC Response. Retrieved from https://www.beuc.eu/publications/beuc-x-2016-073_summary_of_eprivacy_response.pdf.

Bureau Européen des Unions de Consommateurs. (2020). Who we are. Retrieved from http://www.beuc.eu/about-beuc/who-we-are.

Buttarelli, G. (2018). The urgent case for a new ePrivacy law. Retrieved from https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

Cacciatore, M. A., Scheufele, D. A., & Iyengar, S. (2016). The end of framing as we know it… and the future of media effects. *Mass Communication and Society*, *19*(1), 7-23. doi:10.1080/15205436.2015.1068811.

Center for Democracy and Technology. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-civil-society-and-consumer-associations-public-consultation-evaluation.

Center for Democracy and Technology. (2017). Analysis of the proposed ePrivacy Regulation. Retrieved from https://cdt.org/wp-content/uploads/2017/05/2017-May-CDT-EPR.pdf.

Center for Democracy and Technology. (2020a). About. Retrieved from https://cdt.org/about/.

Center for Democracy and Technology. (2020b). Advisory council. Retrieved from https://cdt.org/about/advisory-council/.

Center for Democracy and Technology. (2020c). Who we are. Retrieved from https://cdt.org/who-we-are/.

Chalmers. A.W. (2013). Trading information for access: informational lobbying strategies and interest group access to the European Union, *Journal of European Public Policy*, *20*(1), 39-58, doi: 10.1080/13501763.2012.693411.

Chantzos, I. (2017, May 17). European ePrivacy Reform Security considerations EP, LIBE hearing, 11th April. In C. Moraes (Chair), *The proposed rules for the respect for private life and the protection of personal data in the electronic communications in the EU* [Title Hearing] The e-privacy proposal: confidentiality and security of communications. https://www.europarl.europa.eu/cmsdata/116948/symantec.pdf.

Cisco Systems. (2016a). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Cisco Systems. (2016b). Cisco response to the evaluation and review of the ePrivacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Cisco Systems Inc. (2020). Who is Cisco. Retrieved from https://www.cisco.com/c/en_au/about/who-is-head.html.

Coen, D., & Richardson, J. (2009). *Lobbying the European Union: Institutions, actors, and issues*. Oxford: Oxford University Press. Retrieved from https://eur.on.worldcat.org/oclc/294885646.

Committee on Civil Liberties, Justice and Home Affairs. (2017). *Programme hearing on ePrivacy*.

Corporate Europe Observatory. (2018). Shutting down ePrivacy: Lobby bandwagon targets council. Retrieved from https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council.

Council of Europe. (1952). *The European Convention on Human Rights*.

Daviter, F. (2007). Policy framing in the European Union. Journal of European Public Policy, 14(4), 654-666. doi:10.1080/13501760701314474.

De Bruycker, I. (2017). Framing and advocacy: A research agenda for interest group studies. *Journal of European Public Policy, 24*(5), 775-787. doi:10.1080/13501763.2016.1149208.

De Bruycker, I., & Beyers, J. (2019). Lobbying strategies and success: Inside and outside lobbying in European Union legislative politics. *European Political Science Review, 11*(1), 37-56. doi: 10.1017/S1755773918000218.

DG CONNECT. (2016). Contributions to the public consultation on the Evaluation and Review of the ePrivacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-public-consultation-evaluation-and-review-eprivacy-directive.

DIGITALEUROPE. (2016a). DIGITALEUROPE views on the Review of the ePrivacy Directive. Retrieved from https://www.digitaleurope.org/wp/wp-

content/uploads/2019/01/DIGITALEUROPE%20views%20on%20the%20Review%20of%20the%20ePrivacy%20Directive.pdf.

DIGITALEUROPE. (2016b). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

DIGITALEUROPE. (2018). DIGITALEUROPE's comments on the ePrivacy Regulation proposal. Retrieved from https://www.digitaleurope.org/resources/digitaleuropes-comments-on-the-eprivacy-regulation-proposal/.

DIGITALEUROPE. (2018). DIGITALEUROPE's consolidated position on ePrivacy Regulation. Retrieved from https://www.digitaleurope.org/resources/digitaleuropes-consolidated-position-on-eprivacy-regulation/.

DIGITALEUROPE. (2020). About us. Retrieved from https://www.digitaleurope.org/about-us/.

Directorate-General CONNECT (2020). Communications networks, content and technology. Retrieved from https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en.

Directorate-General for Research. (2003). *Lobbying in the European Union: Current rules and practices.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/etudes/join/2003/329438/DG-4-AFCO_ET%282003%29329438_EN.pdf.

Directorate General Internal Policies of the Union (2007). Lobbying in the European Union. Briefing paper. Retrieved from http://www.eurosfaire.prd.fr/7pc/doc/1211469722_lobbying_eu.pdf.

Druckman, J. N. (2004). Political preference formation: Competition, deliberation, and the (ir)relevance of framing effects. *American Political Science Review, 98*(4), 671-686. doi:10.1017/S0003055404041413.

Dür, A., Bernhagen, P., & Marshall, D. (2015). Interest group success in the European Union: When (and why) does business lose? *Comparative Political Studies, 48*(8), 951-983. doi: 10.1177/0010414014565890

Dür, A. & De Bièvre, B. (2007). The question of interest group influence. *Journal of Public Policy, 27*(1), 1-12. doi: 10.1017/S0143814X07000591.

Dür, A., & Mateo, G. (2013). Gaining access or going public? interest group strategies in five european countries. *European Journal of Political Research, 52*(5), 660-686. doi:10.1111/1475-6765.12012.

Ecommerce Europe. (2016). European Commission consultation on the review of the e-Privacy Directive: Position of European press publishers. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Ecommerce Europe. (2017). Ecommerce Europe Position Paper. Policy recommendations for a better Regulation on Privacy and Electronic Communications. Retrieved from https://www.ecommerce-europe.eu/wp-content/uploads/2017/07/Ecommerce-Europe-Position-Paper-ePrivacy-July-2017-1.pdf.

Ecommerce Europe. (2020). About Ecommerce Europe. Retrieved from https://www.ecommerce-europe.eu/about-ecommerce-europe/.

Eising, R. (2007). Institutional context, organizational resources and strategic choices: Explaining interest group access in the European Union. *European Union Politics, 8*(3), 329-362. doi: 10.1177/1465116507079542.

Eising, R., Rasch, D., & Rozbicka, P. (2015). Institutions, policies, and arguments: Context and strategy in EU policy framing. Journal of European Public Policy, 22(4), 516-533. doi:10.1080/13501763.2015.1008552.

Eising, R., & Spohr, F. (2017). The more, the merrier? interest groups and legislative change in the public hearings of the German parliamentary committees. *German Politics, 26*(2), 314-333. doi:10.1080/09644008.2016.1213244.

EMMA/ENPA. (2016a). European Commission consultation on the review of the e-Privacy Directive: Position of European press publishers. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

EMMA/ENPA. (2016b). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51-58. doi:10.1111/j.1460-2466.1993.tb01304.x.

ETNO. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

ETNO. (2017). ETNO's views on the Proposal for an ePrivacy Regulation. Retrieved from https://etno.eu/datas//positions-papers/2017/RD440_ETNO_views_eprivacy/RD440_ETNO_views_eprivacy.pdf.

ETNO. (2019). Joint industry statement on the ePrivacy regulation. Retrieved from https://www.etno.eu/news/all-news/651:industry-statement-eprivacy-19.html.

EuroISPA. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

EuroISPA. (2020). A few words about us. Retrieved from https://www.euroispa.org/.

European Commission. (2002). *Towards a reinforced culture of consultation and dialogue - general principles and minimum standards for consultation of interested parties by the Commission.* Retrieved from https://ec.europa.eu/governance/docs/comm_standards_en.pdf.

European Commission. (n.d.) Shaping Europe's digital future. Digital Privacy. Retrieved from https://ec.europa.eu/digital-single-market/en/online-privacy.

European Digital Rights. (2016a). EDRi's position on the proposal of an e-Privacy regulation. Retrieved from https://edri.org/files/epd-revision/ePR_EDRi_position_20170309.pdf.

European Digital Rights. (2016b). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-civil-society-and-consumer-associations-public-consultation-evaluation.

European Digital Rights. (2020). About EDRi. Retrieved from https://edri.org/about/.

European Parliament. (2017a). Bye bye cookies? MEPs consider new e-privacy rules. Retrieved from https://www.europarl.europa.eu/news/en/headlines/society/20170602STO76619/bye-bye-cookies-meps-consider-new-e-privacy-rules.

European Parliament. (2017b). Legislative Observatory. 2017/0003(COD). Respect for private life and the protection of personal data in electronic communications. Retrieved from https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en.

European Parliament. (2019a). European Parliament approves more transparency and efficiency in its internal rules. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20190123IPR24128/ep-approves-more-transparency-and-efficiency-in-its-internal-rules.

European Parliament. (2019b). Legislative train schedule connected digital single market. Retrieved from https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform.

European Parliament. (n.d.). Committee. Introduction. Retrieved from https://www.europarl.europa.eu/committees/en/about/introduction.

European Publishers Council. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

European Publishers Council. (2020). What is the European Publishers Council? Retrieved from https://www.epceurope.eu/what-is-the-epc.

European Union. (n.d.). *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02.

Facebook. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Facebook. (2020). Our mission. Retrieved from https://about.fb.com/company-info/.

Forbes. (2020). Symantec. Retrieved from https://www.forbes.com/companies/symantec/#3f2368ab2f98.

Gerring, J. (2004). What is a case study and what is it good for? *The American Political Science Review, 98*(2), 341-354. Retrieved from https://www.jstor.org/stable/4145316.

Google. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Google. (2020). From the garage to the googleplex. Retrieved from https://about.google/intl/com/our-story/.

Goyens, M. (2016). Letter on the revision of the E-Privacy Directive. Retrieved from https://www.beuc.eu/publications/beuc-x-2019-082_consumer_mission_letter_to_commissioner_reynders.pdf.

Greenwood, J. (2019). *Interest Organizations and European Union Politics* Oxford University Press. doi:10.1093/acrefore/9780190228637.013.1162.

Grünthal, R. (2017, May 17). Hearing on ePrivacy, EU Parliament, In C. Moraes (Chair), *The proposed rules for the respect for private life and the protection of personal data in the electronic communications in the EU* [Title Hearing] The e-privacy proposal: legal consistency with other legal instruments; level playing field, Brussels, European Union. https://www.europarl.europa.eu/cmsdata/116943/grunthal.pdf.

GSMA. (2016a). 5th July 2016 - GSMA Full response to Question 6A. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

GSMA. (2016b). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

GSMA. (2020). Membership. Retrieved from https://www.gsma.com/aboutus/.

Hidvedi, F. (2017, May 17). Testimony by Access Now on 11 April 2017 before the LIBE Committee on the proposed ePrivacy Regulation presented by the EU Commission on 10 January 2017. In C. Moraes (Chair), *The proposed rules for the respect for private life and the protection of personal data in the electronic communications in the EU* [Title Hearing] The e-privacy proposal: legal consistency with other legal instruments; level playing field, Brussels, European Union. https://www.accessnow.org/europes-eprivacy-regulation-must-level-playing-field-users/.

Hix, S., & Høyland, B. (2011). *The political system of the European Union* (3rd ed. ed.). Basingstoke: Palgrave Macmillan.

Jensen, C., & Seeberg, H. B. (2019). On the enemy's turf: Exploring the link between macro- and micro-framing in interest group communication. *Journal of European Public Policy*, 1-20. doi: 10.1080/13501763.2019.1659845.

Kellstedt, P. M. & Whitten G. D. (2013). *Field research in political science* (2nd ed.) Cambridge University Press. doi: 10.1017/CBO9780511794551.

Klüver, H. (2012). Biasing politics? interest group participation in European policy-making. *West European Politics, 35*(5), 1114-1133. doi: 10.1080/01402382.2012.706413.

Klüver, H. (2013). Lobbying as a collective enterprise: winners and losers of policy formulation in the European Union, *Journal of European Public Policy, 20*(1), 59-76, doi: 10.1080/13501763.2012.699661.

Klüver, H., Mahoney, C., & Opper, M. (2015). Framing in context: How interest groups employ framing to lobby the european commission. *Journal of European Public Policy, 22(4),* 481-498. doi:10.1080/13501763.2015.1008550.

Kononenko, V., & Parise, R. (2017). Briefing initial appraisal of a European Commission impact assessment. Respect for private life and protection of personal data in electronic communications. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf

Kuckartz, U., & Rädiker, S. (2019). *Analyzing qualitative data with MAXQDA*. Springer.

Lehnert M., Miller B., Wonka A. (2007). Increasing the Relevance of Research Questions: Considerations on Theoretical and Social Relevance in Political Science. In: Gschwend T., Schimmelfennig F. (eds) Research Design in Political Science. Palgrave Macmillan, London.

López Aguilar, J. F. (2019). LIBE. About. Welcome words. Retrieved from https://www.europarl.europa.eu/committees/en/libe/about.

Mahoney, C. (2007). Lobbying success in the united states and the European Union. *Journal of Public Policy, 27*(1), 35-56. doi: 10.1017/S0143814X07000608.

Maxwell, J.A. (2010). Using Numbers in Qualitative Research. Sage Journals, 16 (6), 475-482. doi:10.1177/1077800410364740.

Michalowitz, I. (2007). What determines influence? assessing conditions for decision-making influence of interest groups in the EU. *Journal of European Public Policy, 14*(1), 132-151. doi:10.1080/13501760601072719.

Microsoft. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Microsoft. (2020). Facts about Microsoft. Retrieved from https://news.microsoft.com/facts-about-microsoft/.

Monteleone, S. (2017). *Briefing. reform of the e-privacy directive*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf.

Morth, U. (2000). Competing frames in the European Commission-the case of the defence industry and equipment issue. *Journal of European Public Policy, 7*(2), 173-189. doi:10.1080/135017600343151.

Mozilla. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Mozilla. (2017). Mozilla position paper on the European Commission's draft e-Privacy Regulation. Retrieved from https://blog.mozilla.org/netpolicy/files/2017/10/ePrivacy-position-paper-_-FINAL.pdf.

Mozilla. (2020). The Mozilla manifesto addendum. Pledge for a healthy internet. Retrieved from https://www.mozilla.org/en-US/about/manifesto/.

Negreiro, M., & Madiega, T. (2019). Digital transformation. *European Parliamentary Research Service*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/633171/EPRS_BRI(2019)633171_EN.pdf?utm_source=e-mailnieuwsbrief&utm_medium=email&utm_campaign=AWTI+e-mail+alert.

Neuhold, C. (2001). The 'Legislative Backbone' Keeping the Institution Upright? The Role of European Parliament Committees in the EU Policy-Making Process. European Integration online Papers (EIoP), 5(10), 1-27, doi.org/10.2139/ssrn.302785.

Nokia. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Nokia. (2020). What we do. Retrieved from https://www.nokia.com/about-us/what-we-do/.

Open Rights Group. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-civil-society-and-consumer-associations-public-consultation-evaluation.

Open Rights Group. (2020). Who we are. Retrieved from https://www.openrightsgroup.org/who-we-are/.

Orange. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Orange. (2020). Key facts. Orange at a glance. Retrieved from https://www.orange.com/en/Group/Key-facts/Discover-Orange-s-key-facts.

Rasch, D. (2018). *Lobbying success in the European Union. The role of information and frames*. New York: Routledge.

Ravenhill, J. (2017). *Global political economy.* Oxford University Press.

Saldaña, J. (2015). *The coding manual for qualitative researchers*. Sage.

Salisbury, R. H. (1969). An exchange theory of interest groups. *Midwest Journal of Political Science*, *13*(1), 1. Retrieved from https://search.proquest.com/docview/1301259783.

Saurugger, S. (2008). Democracy and interest group studies in the EU: Towards a sociological research agenda. Retrieved from https://halshs.archives-ouvertes.fr/halshs-00321276/document.

Schibsted. (2020). Who we are. Retrieved from https://schibsted.com/about/who-we-are/.

Schrefler, L. (2017). *Review of the ePrivacy Directive*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/587347/EPRS_BRI(2017)587347_EN.pdf.

Strahs, B. (2017, May 17). Speech by Benjamin Strahs, Software Engineer at Facebook. In C. Moraes (Chair), *The proposed rules for the respect for private life and the protection of personal data in the electronic communications in the EU* [Title Hearing] The e-privacy proposal: confidentiality and security of communications. https://www.europarl.europa.eu/cmsdata/116941/benjamin-strahs-facebook.pdf.

Stolton, S. (2019). Commission to present revamped ePrivacy proposal. Retrieved from https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/.

Telefónica. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Telefónica. (2020a). Digital confidence. Retrieved from https://www.telefonica.com/en/web/public-policy/digital-confidence?p_l_id=341414&p_p_id=101_INSTANCE_IpJfX5zuYTix&p_p_lifecycle=0&p_p_state=normal&_101_INSTANCE_IpJfX5zuYTix_resetCur=true&_101_INSTANCE_IpJfX5zuYTix_categoryId=348332.

Telefónica. (2020b). In brief. Retrieved from https://www.telefonica.com/en/web/about_telefonica/in-brief.

Vodafone. (2016). Response to the questionnaire for the public consultation on the evaluation and review of the E-Privacy Directive. Retrieved from https://ec.europa.eu/digital-single-market/en/news/contributions-received-industry-public-consultation-evaluation-and-review-eprivacy-directive.

Vodafone. (2020). What we do. Retrieved from https://www.vodafone.com/what-we-do.

Voltolini, B. (2016). Framing processes and lobbying in EU foreign policy: Case study and process-tracing methods. doi: 10.1057/eps.2016.18.

Vreese, C. H. (2005). News framing: Theory and typology. *Information Design Journal, 13*(1), 51-62. doi:10.1075/idjdd.13.1.06vre.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks: Sage Publications.

Appendix A: In-depth analysis of interest group frame choice (Commission)

The tables contain direct quotes from the interest groups responses to the Commission's questionnaire as well as from their position papers if provided. These were subject to the in-depth analysis of frame choice vis-à-vis the Commission.

Cause Groups

Table 1:

In-depth analysis of frame choice by Access Now (Commission)

Type of frame	Arguments by Access Now	Key words/word combinations
Public frame		
Consumer protection frame	Furthermore, the differences in the implementation of the rules by each Member State results in unequal protections and safeguards for users across the EU as well as complexity for cross-border businesses	protections safeguards users
	According to the 2015 EuroBarometer, more than half of the respondents reported concerns about mobile services or applications providers recording their everyday activities. These concerns highlight the need for robust and clear safeguards for the protection of users' data and confidentiality, which will lead to increased trust in services.	safeguards protection users
	Overall, the future e-Privacy legislation should promote the development, spread, and use of technologies that protect the confidentiality of communications – both content and metadata - and safeguard user anonymity.	protect safeguard user
	To that end, the legislators should refrain from establishing specific technical standards or requirements as those could hinder security and create vulnerabilities that negatively impact users' rights and ultimately undermine the objective of the e-Privacy	security user
	The e-Privacy Regulation will seek to protect user privacy by complementing and particularising the GDPR.	protect user
	While implementation of a single set of rules agreed under a Regulation will facilitate harmonised enforcement and help users seek redress of privacy violations, further safeguards for an efficient right to remedy must also be put in place.	users safeguards
	The findings of the 2015 EuroBarometer highlights the need for stronger rules in protecting user privacy, anonymity and confidentiality of communications in the future e-Privacy legislation, while strengthening users' access to remedy for violations of these protections.	protecting user protection
	Any compliance costs associated with the privacy and security obligations of the e-Privacy Directive are at least mitigated by the benefits produced by the same privacy and security obligations in regard to increased user trust and networks' protection.	user protection
	Legislation, and in particular the upcoming e-Privacy legislation, should ensure the right of individuals to secure their communications.	individuals secure
	Legislators should not erode the security of devices or applications by either introducing a legal requirement for vulnerabilities or backdoors into products or service or by pressuring companies to keep and allow law enforcement access to data, or have disproportionate access to the encryption keys to private data.	
	The more privacy-invasive the tracking, the stricter the user protections should be.	user protections

Type of frame	Arguments by Access Now	Key words/word combinations
	As provided for in the GDPR, consent should be informed and freely given. Not only it is the fundamental right of users to have their personal information protected, which means that this information should be used on the basis of their consent as established by Article 8.2 of the EU Charter of Fundamental Rights, but it is also what users want, according to the result of the 2015 EuroBarometer: 67% of users indicated concern about not having complete control over the information they provide online.	users protected
	The differences in the implementation of the rules by each member state have resulted in unequal protections and safeguards for users across the EU and an unnecessary complexity for cross-border businesses.	protection safeguards users
	To provide the legal certainty and clarity needed by the private sector, and to protect users effectively, we must learn from the GDPR experience and refrain from adopting a "Regulective" - half Regulation, half Directive.	protect users
	Overall, the future e-Privacy legislation should promote the development, spread, and use of technologies that protect the confidentiality of communications – both content and metadata - and safeguard user anonymity.	protect safeguard user
	Improving security for users when surfing the web and ensuring digital privacy are in general high on the European Commission's list of priorities. The e-Privacy Directive is a key instrument to achieve these objectives.	security users
	The future e-Privacy Regulation should include a positive obligation for providers of electronic communications, including providers of OTT services, to protect users' anonymity and the confidentiality of their electronic communications - both content and metadata - thus reaffirming the objective of this legislative instrument.	protect users
	Both the metadata and the content of these communications can reveal highly sensitive information about users, and this information must therefore be protected with the highest legal standard for processing: the user must give explicit consent, which must be informed, affirmative, and specific to a clearly defined purpose.	user protected
	The protection of user metadata has often been overlooked and its impact on privacy downplayed. However, in recent years, its relevance has been clearly established.	protection user
	The Open Rights Group, the UK-based NGO, recently published a report on how phone companies use personal data which addresses the caveats for anonymised data under the e-Privacy Directive. Findings indicate that in the UK, implementing the e-Privacy Directive's provision on data anonymisation has not provided sufficient safeguards for users, as in many cases personal attributes such as names were replaced by a code that still enabled identification of individual users.	safeguards users
	The more privacy-invasive the tracking, the stricter the user protections should be.	user protections
	By extending the scope of the future e-Privacy Regulation, increasing the promotion of privacy-by-design tools, and promulgating rules on confidentiality of communications, we have the opportunity to make products and services more resilient, help protect users against surveillance, and push back on the technical level against state's desire to undermine products.	protect users
	To further advance safeguards for the confidentiality of communications - both content and metadata - the future e-Privacy Regulation should promote the general use of privacy-enhancing technologies as well as tools which protect users' anonymity.	protect users
	Access Now supports the EU Commission's efforts in the reform of the e-Privacy Directive and looks forward to engaging with the	protection users

Type of frame	Arguments by Access Now	Key words/word combinations
	legislators and all stakeholders to achieve a high-level of protection for users' right to privacy and confidentiality of communications	
Crime and security frame	While data breach notification is covered by the GDPR, other issues remain to be tackled. The e-Privacy review should specifically ensure protection of traffic and locations data and the principles of data minimisation, purpose limitation, and data protection by design defined under the GDPR.	data breach
	To that end, the issue of data breach notification is sufficiently covered under the GDPR and need not be re-addressed under e-Privacy.	data breach
	The referenced legal instruments establish security obligations and requirements that broadly correspond to the objectives of the e-Privacy Directive. To avoid duplication, administrative burden and uncertainty, the security obligations set under the e-Privacy Directive should re-assessed against those instruments. While the requirement set under the Telecoms Framework and the Radio Equipment Directive appear to complement each other, the Network and Information Security Directive specifically refers to the security requirements set under the GDPR.	security
	The issue of data breach notification is sufficiently covered under the GDPR and need not be re-addressed under e-Privacy.	data breach
	To that end, legislators should refrain from establishing specific technical standards or requirements, as those could hinder security and create vulnerabilities that negatively impact users' rights and ultimately undermine the objective of the e-Privacy legislation.	security
	Security and privacy are crucial to ensure trust in the digital economy and the digital single market, which in turn is key for business development, revenues, and growth.	security
	However, regardless of the e-Privacy Directive review process, states are currently pushing for a way to circumvent encryption, either through exploiting vulnerabilities or through hacking.	exploiting hacking
	To that end, legislators should not erode the security of devices or applications, either by introducing a legal requirement for vulnerabilities or by mandating backdoors into products or services.	security
	Member states' surveillance of, and unlawful access to, personal data pose serious risks for the rights to privacy and data protection.	unlawful
	We recognise the need for member states to ensure the security of people living the EU; this goal can only be achieved if the foreseen cooperation with providers of electronic communications does not lead to the establishment of vulnerabilities in networks or devices, and if we prevent unlawful access to information. Such measures would put all users at risks. There is no secure way to provide authorities with a "magic key" or other form of exceptional access. Any deliberate vulnerabilities or backdoors in our technology would inevitably pave the way for exploitation.	security unlawful secure exploitation
	Transparency reporting is a pathway for technology companies to disclose threats to users' privacy and freedom of expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, internet shutdowns, content restrictions, and a host of other practices that impact users' fundamental rights.	abuse
	Furthermore, while the implementation of a single set of rules agreed under a Regulation will facilitate harmonised enforcement and help users seek redress of privacy violations, further safeguards for an efficient right to remedy must also be put in place.	violations
	Measures on data breaches and the compliance and enforcement mechanism should be aligned with the GDPR.	data breaches

Type of frame	Arguments by Access Now	Key words/word combinations
Human rights frame	At the time of its adoption, the legislators did not adequately capture the impact that smartphone applications, online tracking, javascript, social media services, or behavioural advertising would have on internet users' right to privacy and confidentiality of communications.	right to privacy and confidentiality of communications
	The GDPR does not specifically cover the right to private life enshrined in Article 7 of the EU Charter of Fundamental Rights, and specific protections will have to be articulated in the future revised e-Privacy.	right to private life Charter of Fundamental Rights
	Member States have taken advantage of the current uncertainty under EU law to enact data retention mandates, which have a deleterious impact on human rights, the environment, and the digital economy.	human rights
	While the costs of data retention have been demonstrated and highlighted in the EU Commission impact assessment on the Data Retention Directive (DRD), the necessity and proportionality of data protections measures remains to be proven. In Joined Cases C-293/12 and C-594/12, the EU Court has highlighted the severe impact on the right to privacy of this highly intrusive scheme.	right to privacy
	Legislation, and in particular the upcoming e-Privacy legislation, should ensure the right of individuals to secure their communications.	right to secure communications
	Any attempt to undermine the development or use of encryption or other tools and technologies protecting the confidentiality of communication would also undermine the fundamental right to privacy as well as the integrity of communications and systems	fundamental right to privacy
	Finally, introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent, would be a welcome development to strengthen user's right to privacy.	right to privacy
	User opt-in consent guarantees individual's retain control over his or her personal information. As provided for in the GDPR, consent should be informed and freely given. Not only it is the fundamental right of users to have their personal information protected, which means that this information should be used on the basis of their consent as established by Article 8.2 of the EU Charter of Fundamental Rights, but it is also what users want, according to the result of the 2015 EuroBarometer: 67% of users indicated concern about not having complete control over the information they provide online.	fundamental right
	Please find attached our Transparency Reporting Index, a resource that contributes to important efforts tracking how well companies across the globe are meeting their responsibility to respect human rights in the digital age.	human rights
	Similarly, the future framework will complete the recently adopted General Data Protection Regulation and provide protection for the right to private life as enshrined in Article 7 of the EU Charter of Fundamental Rights, which is not specifically covered by the scope of the GDPR.	Charter of Fundamental Rights
	Aligning the e-Privacy reform with the GDPR will be crucial in order to avoid a conflict of laws, uncertainty for users' rights, and undue administrative burden for industry.	users' rights
	When the e-Privacy Directive was adopted in 2002, legislators were unable to sufficiently anticipate the impact that smartphone applications, online tracking, javascript, social media services, or behavioural advertising would have on internet users' right to privacy and confidentiality of communications.	right to privacy and confidentiality of communications.
	Member states have taken advantage of the current uncertainty under EU law to enact data retention mandates which have a deleterious impact on human rights, the environment, and the digital economy	human rights
	the Court of Justice of the EU has established in Joined Cases C-293/12 and C-594/12 that data retention schemes have a severe impact on the user's right to privacy.	right to privacy

Type of frame	Arguments by Access Now	Key words/word combinations
	Echoing the United Nations 2016 resolution on privacy, we calls upon governments to "refrain from requiring business enterprises to take steps that interfere with the right to privacy." The UN also encourages companies "to work towards enabling secure communication and the protection of individual users against arbitrary or unlawful interference of their privacy, including by developing technical solutions."	right to privacy
	Member states' surveillance of, and unlawful access to, personal data pose serious risks for the rights to privacy and data protection	right to privacy
	Any attempt to undermine the development or use of encryption or other tools and technologies to protect the confidentiality of communication would also undermine the fundamental right to privacy as well as the integrity of our systems, and therefore stands at odds with the objective of the e-Privacy legislation.	fundamental right to privacy
	It is important to note that regardless of the member states' competence under the public security exemption, the requirements for proportionality and necessity under the EU Charter for Fundamental Rights still apply. Access Now is keen to challenge laws and policies that violate the right to privacy, in collaboration with other stakeholders	Charter for Fundamental Rights right to privacy
	Transparency reporting is a pathway for technology companies to disclose threats to users' privacy and freedom of expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, internet shutdowns, content restrictions, and a host of other practices that impact users' fundamental rights.	fundamental rights
	Access Now supports the EU Commission's efforts in the reform of the e-Privacy Directive and looks forward to engaging with the legislators and all stakeholders to achieve a high-level of protection for users' right to privacy and confidentiality of communications	right to privacy and confidentiality of communications
	The new e-Privacy Regulation must contain rules that protects the right to privacy of users from member states to avoid the creation of loopholes for government access to data related to either telecoms operators, OTTs, or information society services.	right to privacy
Economic frame		
	The Directive's market oriented objectives on the free movement of data and equipment were somewhat successful, as reflected by the development of Big Data and Internet of Things products and services in the last decade.	market
	Furthermore, the differences in the implementation of the rules by each Member State results in unequal protections and safeguards for users across the EU as well as complexity for cross-border businesses.	businesses
	Alignment with the GDPR will be crucial to avoid conflict of laws, uncertainty for users' rights, and administrative burden for the industry.	industry
	While the costs of data retention have been demonstrated and highlighted in the EU Commission impact assessment on the Data Retention Directive (DRD), the necessity and proportionality of data protections measures remains to be proven.	costs
	Any compliance costs associated with the privacy and security obligations of the e-Privacy Directive are at least mitigated by the benefits produced by the same privacy and security obligations in regard to increased user trust and networks' protection. These compliance and related administrative costs can be further mitigated by changing the nature of the e-Privacy instrument from a Directive to a Regulation, free of national exceptions or derogations.	costs
	Legislators should not erode the security of devices or applications by either introducing a legal requirement for vulnerabilities or backdoors into products or service or by pressuring companies to keep and allow	companies

Type of frame	Arguments by Access Now	Key words/word combinations
	law enforcement access to data, or have disproportionate access to the encryption keys to private data.	
	Under Article 16 of the EU Charter of Fundamental Rights, companies enjoy the freedom to conduct a business and should therefore not be "required to make paying services available."	companies business paying
	The differences in the implementation of the rules by each member state have resulted in unequal protections and safeguards for users across the EU and an unnecessary complexity for cross-border businesses.	businesses
	Aligning the e-Privacy reform with the GDPR will be crucial in order to avoid a conflict of laws, uncertainty for users' rights, and undue administrative burden for industry.	industry
	Security and privacy are crucial to ensure trust in the digital economy and the digital single market, which in turn is key for business development, revenues, and growth.	economy market business revenues growth
	While avoiding creating burdens for users and businesses, law makers must develop measures for a future e-Privacy Regulation that are technologically neutral and focused on addressing the impact of privacy-intrusive technologies, rather than regulating or prescribing the development of specific applications.	businesses
	Article 23 of the GDPR covers the content of Article 15 of the e-Privacy Directive, which includes a provision authorising the use of data retention schemes. This Article should be removed from the update as it is redundant with Article 23 in the GDPR. Member states have taken advantage of the current uncertainty under EU law to enact data retention mandates which have a deleterious impact on human rights, the environment, and the digital economy.	economy
	We acknowledge that there are risks that the legislation could be weakened during the reform process, given that some member states are pushing for circumvention of encryption, and industry has continually attacked the ePrivacy Directive as a whole.	industry
	The e-Privacy Directive is the best instrument to help businesses resist the pressure of developments like these, protect their products and infrastructure, and shield their users from privacy violations.	businesses
	To further advance safeguards for the confidentiality of communications - both content and metadata - the future e-Privacy Regulation should promote the general use of privacy-enhancing technologies as well as tools which protect users' anonymity. Those rules must be technologically neutral and not request the industry or users to use a specific standards, as such criteria would make it easier for external actors to undermine the selected tools and trump their potential benefits.	industry
	They [legislators] should not pressure companies into keeping private data, allow law enforcement to access to it, or retain encryption keys to decrypt the data.	companies
	Echoing the United Nations 2016 resolution on privacy, we calls upon governments to "refrain from requiring business enterprises to take steps that interfere with the right to privacy." The UN also encourages companies "to work towards enabling secure communication and the protection of individual users against arbitrary or unlawful interference of their privacy, including by developing technical solutions."	business enterprises
	Transparency reporting is a pathway for technology companies to disclose threats to users' privacy and freedom of expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, internet	companies

Type of frame	Arguments by Access Now	Key words/word combinations
	shutdowns, content restrictions, and a host of other practices that impact users' fundamental rights.	
	Increased promotion and general rules on the protection of privacy by design tools and techniques such as encryption should be added. Those rules must be technologically neutral and not request the industry or users to use specific standards.	industry

Table 2:

In-depth analysis of frame choice by Bits of Freedom (Commission)

Type of frame	Arguments by Bits of Freedom	Key words/word combinations
Public frame		
Consumer protection frame	At the time of the ePD's adoption, many elements of current technologies were not yet fully developed (e.g. communicating through over the top (hereinafter OTT) services, smart phone apps, new monitoring and profiling techniques). These developments are not fully accounted for in the ePD. This has created arbitrary differences in the protection of users between different but functionally equivalent services.	protection users
	Many new communications services are not subject to the same confidentiality requirements and specific obligations when processing traffic and location data, that users expect from traditional telecommunications providers. This arbitrary difference in the protection of end users' rights and interests undermines the legitimacy and effectiveness of the ePD.	protection users
	The first statement unjustly puts a monetary value on the level of privacy protection afforded to individuals. Privacy protection should not be commodified, leading to different levels of protection depending on how much an individual could afford.	protection individuals
	GDPR as a minimum. The new instrument should provide protections to users when communicating (online) that are more specific and complementary to the GDPR.	protections user
Crime and security frame	Although law enforcement authorities should be able to perform their tasks in accordance with the law, legislation mandating the creation of back doors or the weakening of encryption or other security measures, should be avoided at all costs. The second part of this question, which opens up the possibility of back doors and mandating weaker security, is therefore unacceptable and could undermine the right to privacy, private property rights and other fundamental rights right of individuals.	security
	Informed consent should be required for identifiers collected/placed by third parties tracking your behavior, whether this is for behavioral advertising, website analytics, fraud detection or frequency capping purposes. Consent would not necessarily be required for identifiers collected/placed by the website owner itself for website analytics or fraud detection (first party cookies), provided that it has no or little impact on the end user's privacy rights and clearly falls within the scope of the privacy policy of the website.	fraud
	Third party ads are often served automatically without any human oversight. This creates ideal conditions for malware to spread.	malware
Human rights frame	The e-Privacy Directive (hereinafter "ePD") has failed to achieve full protection of the individual's right to privacy, confidentiality of communications and freedom to seek information without being continuously profiled and monitored online.	right to privacy

Type of frame	Arguments by Bits of Freedom	Key words/word combinations
	The lack of substantive protection of fundamental rights is further exacerbated by the lack of privacy by design and security measures implemented in the terminal equipment (hardware and software) of end users.	fundamental rights
	The processing of traffic or location data should fall under the protection of the Charter rights to data protection and confidentiality of communications, in addition to any requirements under the GDPR or successor to the ePD. It should be clarified that any restriction to such rights by Union law or national law (such as data retention laws) must comply with the requirements of these Charter rights.	Charter rights
	Since the GDPR does not specifically address matters such as the confidentiality of communications, or the right to freedom of expression (including the freedom to communicate more generally) in an online environment, having specific rules particularizing and complementing the general regulatory framework of the GDPR, will provide the added value that the ePD (partly) offered in the past.	right to freedom of expression
	Finally, the new legal instrument must ensure full communications confidentiality and integrity on fundamental rights grounds. It is key that end users are protected against fundamental rights interferences, irrespective of the type of communications provider or services involved.	fundamental rights
	The protection of fundamental rights should not depend on an economic cost/benefit analysis. Fundamental rights are inherently valuable, deserving full legal protection.	fundamental rights
	The new instrument should be aligned with the GDPR where possible, and should put more emphasis on relevant values protected by the fundamental right to freedom of expression. Confidentiality of communications can be seen as an auxiliary right safeguarding freedom of expression.	fundamental right to freedom of expression
	We agree with what the first half of this question states about the right of individuals to secure their communications. This is a right individuals have.	right of individuals to secure their communications
	The second part of this question, which opens up the possibility of back doors and mandating weaker security, is therefore unacceptable and could undermine the right to privacy, private property rights and other fundamental rights right of individuals .	right to privacy, private property rights fundamental rights
	Private parties not offering public services should not be prohibited from denying access to their non-subscription based services if users refuse the storage of identifiers in their terminal equipment. Such a general prohibition would be a disproportionate limitation of their freedom to conduct business. However, this does not exclude providers to protect users' privacy rights and personal data. Limitations on (third party) tracking technologies interfering with end user's rights, including liability arrangements, should be part of the new instrument.	privacy rights
	Consent would not necessarily be required for identifiers collected/placed by the website owner itself for website analytics or fraud detection (first party cookies), provided that it has no or little impact on the end user's privacy rights and clearly falls within the scope of the privacy policy of the website.	privacy rights
	Traffic and location data carry a high risk to give away a very detailed and intimate picture of an individual's day to day life, social interactions, and personal preferences. The protection of such data is essential for an individuals right to privacy and confidentiality of communications.	right to privacy and confidentiality of communications.
	The principle of "purpose limitation" applies and should not be weakened for statistical purposes or "traffic control" or similar processing that does not override the fundamental rights and freedoms of the data subject.	fundamental rights

Type of frame	Arguments by Bits of Freedom	Key words/word combinations
	In addition to the right to privacy and data protection, issues related to the right to freedom of expression and related communications freedoms that are impacted by electronic communications should also be specifically addressed by the successor to the ePD.	right to privacy and data protection
	Private parties not offering public services should not be prohibited from denying access to their non-subscription based services if users refuse the storage of identifiers in their terminal equipment. Such a general prohibition would be a disproportionate limitation of their freedom to conduct business. However, this does not exclude providers to protect users' privacy rights and personal data.	privacy rights
Economic frame		
	The market oriented goals of the ePD the free movement of personal data and of electronic communications equipment seem to have been achieved quite successfully since the adoption of the ePD, given the rapid market growth of data driven (new) market players which heavily rely on the processing of personal data. Whether the ePD has played any causal role in this rapid development, is uncertain and hard to determine.	market growth
	The protection of fundamental rights should not depend on an economic cost/benefit analysis. Fundamental rights are inherently valuable, deserving full legal protection. When offering communications services, providers inevitably have to use resources in order to ensure the confidentiality thereof. The quantity of the resources needed cannot in itself be a justification for offering less protection to the confidentiality of communications. The potential costs of compliance will likely be substantially lower if the successor to the ePD is a Regulation instead of a Directive. By choosing for a Regulation, the additional costs of compliance with national implementations of the ePD could be avoided, since one uniform regulatory framework would apply directly in all Member States.	economic cost
	The first statement unjustly puts a monetary value on the level of privacy protection afforded to individuals. Privacy protection should not be commodified, leading to different levels of protection depending on how much an individual could afford.	monetary
	Private parties not offering public services should not be prohibited from denying access to their non-subscription based services if users refuse the storage of identifiers in their terminal equipment. Such a general prohibition would be a disproportionate limitation of their freedom to conduct business.	business
	An opt-in regime minimizes undesired communications which are not beneficial for both individuals and businesses. The commercial interests of a small group of telemarketing companies do not outweigh the interests of the general public and businesses to not be exposed to undesired communications at their homes or offices.	businesses commercial companies

Table 3:

In-depth analysis of frame choice by BEUC (Commission)

Type of frame	Arguments by BEUC	Key words/word combinations
Public frame		
Consumer protection frame	The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy.	consumers protection

Type of frame	Arguments by BEUC	Key words/word combinations
	It is essential to protect the confidentiality of communications and guarantee a high level of consumer privacy protection across all services.	consumer protection
	Moreover, the emergence of over-the-top ("OTTs") online communication services (like Voice over IP or instant messaging applications) and other means of communication via information society services, has exposed limitations and gaps in the current rules. These new services are massively used by European consumers but they currently fall outside the scope of the Directive. This means for example that a consumer sending a message over an OTT service like WhatsApp does not enjoy the same legal protection as when sending an SMS over a traditional telecoms operator. Consumers are not aware and do not understand these differences in protection.	consumers protection
	The e-Privacy directive, as transposed at national level, has somewhat helped to create a safer environment for users' privacy.	safer user
	Users should always have the right to secure their networks, equipment and communications with the best available techniques.	users secure
	Also, consumers need to continue to be able to control whether their personal data is made publicly available or not. They should also be able to protect their anonymity when calling and be able to block automatic call forwarding by a third party to their terminals.	consumer protect
	The ePD is a fundamental piece of legislation for the protection of consumers' privacy. The General Data Protection Regulation (GDPR) represents a significant step forward in the right direction. Once it becomes applicable, the GDPR will bring great improvements for consumers. However, the GDPR does not address all the elements that are essential to protect consumers' privacy in digital communications. Strong e-Privacy legislation is also necessary.	protection consumer protect
	In the absence of the ePD, issues of concern such as data mining and tracking/profiling of users would grow even larger in scale and the confidentiality of our communications would be unprotected. It is of utmost importance that the Commission comes up with an ambitious proposal that puts citizens/consumers privacy protection at the forefront.	citizens/consumers protection
	A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services.	protects consumers
Crime and security frame	-	
Human rights frame	A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services.	fundamental rights to privacy and data protection
	The e-Privacy Directive is the only legal instrument that crystallises Article 7 of the European Charter of Fundamental Rights (on the protection of private life and communication) into secondary EU law and specifically protects the confidentiality of communications.	Charter of Fundamental Rights
	Therefore, more needs to be done to guarantee the full respect of consumers' fundamental rights to privacy and data protection.	fundamental rights to privacy and data protection
	Where appropriate, the scope should go beyond OTT communication services and cover all information society services in general, complementing the rules of GDPR and particularising them to ensure a high level of data protection and privacy in the online environment, in line with articles 7 and 8 of the European Charter of Fundamental Rights.	Charter of Fundamental Rights
	It is essential to ensure the protection of the confidentiality of communications and that 'privacy by design' and 'privacy by default' become fundamental guiding principles in the online environment.	right to secure communications

Type of frame	Arguments by BEUC	Key words/word combinations
	The legislation should also ensure the right of individuals to secure their communications.	
	On the other hand, this does not mean that every website should be forced to offer a paying service alternative. Such an obligation could foster social/economic discrimination (i.e. the rich, who can pay to protect their privacy, and the poor, who cannot) which would run against the universal nature of the fundamental rights to privacy and data protection. Forcing websites to offer a paid subscription service could also interfere with the development of new innovative business models which might be advantageous to consumers.	fundamental rights to privacy and data protection
	The ePD is the only legal instrument that translates Article 7 of the European Charter of Fundamental Rights on the protection of private life and communication into specific secondary EU law. It provides an additional layer for the protection of personal data, complementing and particularising the general data protection rules.	Charter of Fundamental Rights
Economic frame		
	Public surveys, such as the latest Data Protection Eurobarometer, show that a majority of citizens do not trust landline or mobile phone companies and internet service providers, or online businesses.	companies business
	The 2015 Data Protection Eurobarometer shows that a majority of Europeans is uncomfortable with internet companies using information about their online activity to tailor advertisements. Consumers should have the possibility to use online services without being under constant commercial surveillance.	companies commercial
	On the other hand, this does not mean that every website should be forced to offer a paying service alternative. Such an obligation could foster social/economic discrimination (i.e. the rich, who can pay to protect their privacy, and the poor, who cannot) which would run against the universal nature of the fundamental rights to privacy and data protection. Forcing websites to offer a paid subscription service could also interfere with the development of new innovative business models which might be advantageous to consumers.	paying economic pay paid innovative business
	We strongly welcome the Commission's determination to revise and update the e-Privacy Directive (ePD), despite continuous calls for repeal coming from different industry sectors.	industry

Table 4:

In-depth analysis of frame choice by CDT (Commission)

Type of frame	Arguments by Center for Democracy and Technology	Key words/word combinations
Public frame		
Consumer protection frame	Rapid advancement in tracking technology has highlighted the need for consumer protection in this area. While consumers likely understand firstparty tracking, in which the service provider saves information in order to enhance user experience, third party tracking remains less understood. Third party tracking is also more pervasive.	consumer protection
Crime and security frame	There should be legal protection against unwarranted intrusion into private communications by third parties, regardless of the underlying technology	unwarranted
	In the 2002 ePD, Article 15 allows Member States to adopt legislation that limits the ePD's protections for certain purposes. These purposes are: "defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". The ePD makes reference to	security criminal unauthorized

Type of frame	Arguments by Center for Democracy and Technology	Key words/word combinations
	these purposes, set out in the corresponding Article 13(1) of Directive 95/46/EC.	
	Where the ePD provision was narrowly focused on law enforcement, criminal investigations and public security, the ePR allows public authorities access to data for any "other important objectives of general public interest". This could enable public sector agencies to access a far broader range of personal data than permitted under the ePD.	criminal security
	It is crucial that these issues are dealt with in a manner that do not undermine protection of communications data, while at the same time enabling law enforcement to access data necessary for criminal investigations, and give legal certainty to service providers.	criminal
	The ePR should also include a general prohibition on providers from decrypting, reverse engineering, or monitoring communications protected by encryption. It should specify that service providers are not permitted to degrade the security of systems.	security
Human rights frame	A new legislative should be targeted at problems that are not covered effectively in other EU legislation. A compelling argument for proposing a new instrument to replace the E-Privacy Directive is the fact that the GDPR is not based on Article 7 of the Charter of Fundamental Rights of the EU on the right to privacy and confidentiality of communications. EU Member States are bound by Article 8 of the European Convention on Human Rights, but in the absence of EU legislation, there is arguably a risk of fragmented implementation.	Charter of Fundamental Rights European Convention on Human Rights
	A legislative instrument could possibly be used to ensure that access by law enforcement agencies to data is subject to the safeguards that have established in EU law and by the Court of Justice of the EU, and in the European Convention on Human Rights.	European Convention on Human Rights
	A compelling argument for a new instrument would be that whereas the EPD is based on Art 7 of the Charter of Fundamental Rights, GDPR is based on Art. 8. A new instrument should focus narrowly on addressing identified 'gaps' in protection, rather than import concepts from the EPD into the GDPR framework	Charter of Fundamental Rights
	we argued that a new instrument should primarily target the areas not covered by the General Data Protection Regulation (GDPR). In particular, it should provide for the protection of the right to confidentiality of communications. This Article is not covered by GDPR, which implements Article 8 of the Charter of Fundamental Rights.	right to confidentiality of communications Charter of Fundamental Rights
	The legitimate interest is set out in GDPR Article 6(1)(f) and allows processing of data without consent if this interest is not found to override the fundamental right to privacy and data protection.	fundamental right to privacy
Economic frame		
	As is the case with other utilities policy makers have a legitimate interest and responsibility in making sure that ECS perform to the benefit of society and the economy as a whole.	economy
	We do not have particular insights to offer on this question. It appears that the types of marketing mentioned in Article 13.1 are no longer particularly relevant for today's market place. Online advertising has changed significantly since the adoption of the Directive, and further dramatic shifts can be expected as technology evolves.	market
	In terms of substance, a new instrument should be conducive to the provision of a wide range of communications services, built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes.	business innovation
	Both measures seem disproportionate in their interference in the freedom of a service provider to develop its business model. Their practical impact might be to shut down successful services that	business

Type of frame	Arguments by Center for Democracy and Technology	Key words/word combinations
	consumers appreciate and stop European businesses from getting off the ground.	
	At the same time, the greater the market power of the service provider in question, the stronger the argument for regulatory interference in its business practices. If the provider of a service that is all but indispensable for consumers enjoys such market power that no alternative provider exists, the case for intervention is strengthened.	market business
	There may be a case for specific obligations on providers of Internet Access Services on this issue, depending on specific market conditions.	market
	There is no reason why consent rules and requirements for notices should be different for a communications service provider than for any other business (data processor or controller under the GDPR).	business
	Overall, there would seem to be a strong case for deferring to the GDPR on traffic and location data. This could create a more flexible and innovation-friendly regime, and would be preferable to broadening the legacy EPD provisions to a potentially broad set of services.	innovation
	There does not seem to be a need to carry over the concept of value-added services to a new instrument. Different bundles of services can be envisaged, including ones in which a communications service is provided as an additional feature to another service. For example, a travel agent may offer a chat service as part of its business. A connected car will transmit data over an electronic communications network, but transport is the main service being offered.	business
	It should result in a regime is conducive to the provision of a broad range of communications services, built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes.	business innovation development pricing
	We agree with the need to update the ePD in light of the adoption of the GDPR and developments in communications technology and business models.	business
	Communications confidentiality is also fundamentally important for companies (legal persons) of all descriptions that need to transmit sensitive and confidential data using electronic communications networks.	companies
	As more and more technologies are interconnected and communicate with each other and end users, it becomes difficult to envision a company or service that does not transmit or process data in electronic form using communications networks. Logically, all such data would then be covered by the ePR.	company
	It is sensible to attempt to future-proof the ePR, and the existence of a separate set of rules for communications services outside of the explicit scope of the ePD was one reason put forward by industry for largely repealing ePrivacy rules altogether. Rules governing the confidentiality of communication remain necessary, but we note that language in the draft ePR captures a vast array of different business models and services.	industry business
	Today, a significant portion of digital services and products are provided without fees charged to users, and funded by advertising. Under this business model, the use of websites and digital applications are tracked by first and third parties that measure usage and aim to deliver advertising that is targeted or otherwise tailored to users. Addressing the privacy implications of this model provided the impetus for the revision of the ePD in 2009 and subsequent introduction of the controversial cookie provisions.	business
	The rules should enable transparency and control for end users and at the same time enable provision of a broad range of innovative communications and other digital services and products.	innovative

Type of frame	Arguments by Center for Democracy and Technology	Key words/word combinations
	More flexibility is needed in the underlying legal text; this can be accomplished by further empowering data protection authorities (DPAs) to make decisions as and when market and technology developments require it.	market
	Specifically, the ePR could provide for a larger role for the European Data Protection Board (EDPB) established under the GDPR. Under the GDPR, member states DPAs, via the EDPB, may issue guidance and opinions interpreting the Regulation on issues and questions as they arise with changing technologies and business models. Tracking will remain a priority for DPAs for the foreseeable future. They will need to monitor market developments, business models, technologies, and user behaviours	business market
	Absent centralized controls, the Commission insists that entities will be able to obtain user consent by means of individual requests to end users, but this only encourages industry to engage in the sorts of practices and pop-up banners that generated consent fatigue with the existing ePD. To the extent the ePR is designed to address tracking concerns with respect to advertising business models, it is also worth emphasizing that the GDPR arguably already provides detailed obligations and safeguards for processing of data for advertising and/or profiling purposes.	business
	There is a great need for continuing technical and process innovation in this area, and it is important that the legal language on notice and consent is flexible enough to accommodate new and improved solutions	innovation
	The question is whether the ePR approach will be conducive to the sorts of innovative solutions that will be needed going forward.	innovative
	Encryption technology is an essential tool to enable secure transactions, communications and storage of data. Without these technologies, Europe's digital economy and society would not be able to function.	economy

Table 5:

In-depth analysis of frame choice by EDRi (Commission)

Type of frame	Arguments by European Digital Rights (EDRi)	Key words/word combinations
Public frame		
Consumer protection frame	The evergrowing connectedness of devices will increase the need for clear rules on protection of the confidentiality of communications, both for individuals and for businesses.	protection individuals
	What is lacking is the obligation for hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices.	protect users
Crime and security frame	Notification of personal data breaches: The text related to data breaches should be in line with the one in the GDPR.	data breach
	All of these legal instruments include security obligations which are, in one way or another, in the spirit of the text of the ePD. However, given the divergencies in the different instruments, we believe that the framework stated in the GDPR concerning security requirements should be set as the standard and be applied to the future legal instrument substituting the ePD.	security
	The position which empowers citizens the most in this case would be to require consent. Given such an intrusive marketing technique, the only way to prevent abuses and to avoid overloading the supervisory authorities (DPAs or Telecom Regulators) with objections which have not being taken into consideration adequately would be requiring users to consent to that type of marketing.	abuses

Type of frame	Arguments by European Digital Rights (EDRi)	Key words/word combinations
	Fraud detection must be strictly limited to that activity.	fraud
	However, extending the scope of application of the new rules should not lead to national (telecommunications) laws allowing law enforcement and intelligence agencies to undermine the effectiveness of any security technology, such as end-to-end encryption.	security
	What is lacking is the obligation for hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices. It is baffling and contradictory that unauthorised access to a computer system is a crime under EU legislation (Directive 2013/40/EC) while, under this proposal, unauthorised access to an individual's computer system could be permitted by default.	unauthorized
	Article 11 of the proposal allows Member States to restrict Articles 5 to 8 the proposal to the extent that these restrictions and exceptions are "necessary, appropriate and proportionate" to safeguard major public interests such as national security or the fight against crime.	security crime
	Consequently, these exception clauses in the regulations again leave these matters first and foremost to be determined by Member States' laws – meaning that in these areas, the national laws will be different, allowing for more or less intrusive actions by national security-, defence and law enforcement agencies in the different Member States.	security
Human rights frame	First option: The e-Privacy law should be in line with the GDPR, to achieve legal certainty for consumers and businesses, and compliance with data protection and privacy rights.	privacy rights
	EDRi underlines the necessity of the proposed Regulation. Firstly, it is of utmost importance that internet users can rely on the confidentiality of their communications and the integrity of their devices. Their communications deserve protection in order to give effect to the fundamental rights to privacy, personal data protection and freedom of expression	fundamental rights to privacy
	If websites start checking whether third party cookies are enabled, similar to current checks for certain advertising and tracking blockers, and display an annoying banner asking the end-user to allow cookies in order to access the site, end-users will for all practical purposes be coerced into accepting cross-website tracking. This will have severe negative implications for the fundamental rights of citizens	fundamental rights
	This provision is similar to, and cross-refers to, article 23 in the GDPR. Similar exception clauses are also contained in the Data Protection Directive and the e-Privacy Directive. The clauses in the GDPR and this proposal are an improvement, in that they expressly add that such exceptions must "respect the essence" of the fundamental rights affected; a clear reflection of the wording of the European Charter of Fundamental Rights and recent CJEU case-law	fundamental rights
	Although the intentions of the Commission are laudable, the current text will need thorough work to ensure that the privacy, data protection and other fundamental rights of citizens are fully respected in the digital environment, especially also by providers of e-communication networks and -services and OTT providers.	fundamental rights
	The European institutions need to make an extra effort to ensure that privacy and confidentiality of communications of European citizens are not considered as a tradeable asset, but as a right to be strongly protected.	privacy and confidentiality of communications right
Economic frame		
	On the other hand, market oriented goals (free movement of personal data and of electronic communications equipment) were successfully developed. The development of companies working on Big Data and Internet of Things has continued in the last decade. The movement of personal data is due to some of the norms in the 95 Directive on Data Protection and the ePD, while the free movement of equipment may	market companies

Type of frame	Arguments by European Digital Rights (EDRi)	Key words/word combinations
	rather be a consequence of the freedom of movement of goods and services.	
	Finally, standardisation pushed by the ePD and other regulatory frameworks have undoubtedly helped companies to distribute their products to the EU market.	companies market
	Although we do not comment on the costs that the ePD had for businesses, we believe that by making the new instrument a Regulation instead of a Directive, the potential costs of compliance with the new instrument could be substantially lower than the costs of compliance with the different national implementations of the ePD.	costs businesses
	Furthermore, not only businesses had costs: spam and wild direct marketing calls can generate a cost for consumers too. The ePD has certainly helped with that.	businesses costs
	The e-Privacy law should be in line with the GDPR, to achieve legal certainty for consumers and businesses, and compliance with data protection and privacy rights.	businesses
	Generally, an opt-in regime avoids undesired communications which are not beneficial for neither businesses nor individual citizens. The cost of communications is dropping rapidly (which is central to the growth of the email spam problem) and it is both time-consuming and often risky to "opt out". For both businesses and citizens, the only realistic option is opt-in.	businesses costs
	The notion that privacy should be the preserve of either those that can afford to pay for it or those who have the capacity to foresee the potential risks is a deeply troubling one. The solution to entirely nontransparent, unpredictable (indeed unpredictable for the providers themselves) harvesting and monetisation of personal data, profiling, reselling of data cannot be allowing an elite to avoid this. Ultimately, the solution to people paying an unspecified amount of security and privacy is to implement meaningful transparency for products is to implement meaningful transparency and meaningful consent.	pay monetization
	The evergrowing connectedness of devices will increase the need for clear rules on protection of the confidentiality of communications, both for individuals and for businesses.	businesses
	Secondly, EDRi considers the proposed Regulation will be a boost for innovation and economic growth in Europe.	innovation economic growth
	Similarly, privacy by design and security by design requirements would prevent market failure in the area of the Internet of Things and connected devices.	market
	In addition, established telcos are purchasing ad targeting platforms and openly entering the data markets with a specific value proposition on bypassing devices and installed software, including browsers. It is unclear how the current proposals in the ePR focused on consent through the browser will deal with these developments.	markets
	Unlike the companies that offer such device tracking would like to make us believe, it is extremely difficult, if not impossible, to set up such a service in a way that the protection of privacy of bystanders is respected	companies
	Technical solutions based on local computation in the end-user's device should always be preferred over centralised tracking. Therefore, the broad powers in Article 8.2 provides the wrong incentives to service providers that depend on location input and force citizens to defend themselves by turning off WiFi, or similar defensive measures, to both their detriment and that of the economy. Instead, the ePR should provide an incentive to develop technical solutions where citizens can provide location data to services without any privacy risks (privacy by design).	economy
	A significant number of articles and recitals will have to be substantially modified if citizens' rights are to be appropriately	market businesses

Type of frame	Arguments by European Digital Rights (EDRi)	Key words/word combinations
	protected and citizens' trust in the digital environment – and thus in the Digital Single Market – is to be assured. We hope the co- legislators will not fail the citizens, with unforeseeable negative consequences for individuals and businesses alike.	

Table 6:

In-depth analysis of frame choice by Open Rights Group (Commission)

Type of frame	Arguments by Open Rights Group	Key words/word combinations
Public frame		
Consumer protection frame	The same research shows that mobile users are mainly concerned about the explosion of apps collecting information, and actually expect mobile operators to protect them.	user protect
	Individuals have a right to secure their communications, but companies also have an obligation and should not simply pass this responsibility on to the customer.	individuals secure
Crime and security frame	Government should not be able to undermine the overall security of products and services, but work on a targeted basis.	security
	The monetisation of privacy may provide a solution in certain contexts, but privacy is a social right and sometimes a personal gain of information disclosure may have wider negative social impacts that would make it undesirable. For example, the confidentiality of election voting is protected in various countries, including the UK, in such a way that it would be illegal to buy that information.	illegal
	Nobody fully understands the data flows involved and there is a need for clearer information and separation from functional tracking. We have ticked consent on fraud above, but this is a qualified response. We are concerned that fraud detection and financial surveillance in general are fast growing areas that may be escaping scrutiny. While there is a clear legitimate interest on fighting fraud we would like too see more transparency and believe that there is room for more information to be disclosed without enabling fraudsters. Fraud systems are not completely fool proof and in some cases can disable legitimate transactions and services.	fraud
	What data is retained for billing and for how long needs tightening. This is currently open to abuse, for example some operators keep detailed web history logs with the argument that they may be challenged on data charges. There is a need for more consistency and transparency over retention periods.	abuse
Human rights frame	Our findings suggest that at best, UK mobile companies are fulfilling the minimal legal requirements, and at worst could be breaking the law and breaching our right to privacy	right to privacy
	We do not have information on these aspects, but generally respect for fundamental rights should be a core aspects of any modern business, incorporated in their financial calculations.	fundamental rights

Type of frame	Arguments by Open Rights Group	Key words/word combinations
	Individuals have a right to secure their communications, but companies also have an obligation and should not simply pass this responsibility on to the customer.	right to secure their communications
	The monetisation of privacy may provide a solution in certain contexts, but privacy is a social right and sometimes a personal gain of information disclosure may have wider negative social impacts that would make it undesirable.	privacy right
	An additional aspect is that a monetary approach could lead to the people suffering economic deprivation enjoying lower levels of privacy – which ultimately is a human right.	human right
Economic frame		
	For consistency, E-privacy must be under the same authority as data protections and not telecoms regulators. The latter have very weak mechanisms to engage citizens and are mainly driven though industry links.	industry
	We do not have information on these aspects, but generally respect for fundamental rights should be a core aspects of any modern business, incorporated in their financial calculations. It is possible that a regulation would make it cheaper to comply than a directive.	business financial
	An additional aspect is that a monetary approach could lead to the people suffering economic deprivation enjoying lower levels of privacy – which ultimately is a human right.	monetary economic
	We have found that subscribers already have concerns about the use of their data by companies to provide statistics, research, traffic, etc. Weakening consent would be received very badly. Overriding consent is presented as necessary for public purposes as if they were accrued by the whole of society, while in fact these are businesses services provided by companies for profit, and customers do not necessarily see the benefits.	businesses companies profit

Sectional groups

Table 7:

In-depth analysis of frame choice by the Application Developers Alliance (Commission)

Type of frame	Arguments by Application Developers Alliance	Key words/word combinations
Public frame		
Consumer protection frame	Since privacy and protection of users' data remain a key objective, other legal instruments entered into force overtime are equally, if not more, effective in reaching the same objectives.	protection users
	The Apps Alliance recommends exploring a deregulatory approach which allows Authorities to include consumer protection provisions in more appropriate legal instruments	consumer protection
	When exploring the extension of the regulation, the Commission must consider whether there is clear economic evidence that regulation is proportionate and necessary to protect consumers from harm.	protect consumers
	On the contrary, whilst we fear that this proposal risks putting those principles in jeopardy, we are also dubious that the proposed regulation will help achieve better consumer satisfaction or protection.	consumer protection

Type of frame	Arguments by Application Developers Alliance	Key words/word combinations
	the prohibition of collection and processing of communication data and metadata: the provisions included in art. 6 would hamper the execution of basic communication services function and features, as well as put in jeopardy users' safety online	user safety
Crime and security frame	We encourage the Commission to consider deregulation of existing electronic communication services where this does not harm consumer interests or compromise national or public security, prevention, detection and prosecutionof (sic!) criminal offences.	security
	As a part of an effective deregulation strategy, the Apps Alliance supports the definition of industry standards for security and encryption.	security
	According to art.6, the processing of communication data is considered as an extraordinary action, only allowed in case the processing itself is strictly necessary for the performance of the service or for security purposes.	security
	In fact, the meaning of "necessary" is not universally clear and the court interpretation tends to define it very restrictively. Consent may also not always be practical as most of the updates for security purposes happen automatically.	security
	Therefore, it is hard to understand why a paid-for model should be a preferable or even a viable option. The cost of setting up an infrastructure for payment would be high. There are also increased liability exposure and security risks that are inherent to collecting users' credit card information. Not least, the average user is not willing to pay for apps.	security
Human rights frame	-	
Economic frame		
	Our membership is widely subject to rules concerning unsolicited marketing communications. Due to how these are currently written, they lack clarity and have an impact on our members' business models.	business
	From 2002 onward, the ePrivacy Directive has been relevant to ensure that some sectors complied with specific rules so as to achieve, especially, confidentiality of communication. On the other side, the section concerning location data and cookies raised more criticism and could have a broader impact if applied to other digital sector (especially mobile). However, the legal framework, business models and interactions between the electronic communications sector and digital technologies changed impressively.	business
	The Apps Alliance believes that none of the actions (also questions 16 17) will help to achieve the objectives of both the Digital Single Market Strategy and the Commission Better Regulation Agenda: increasing consumer trust and creating a competitive market and high quality legislation. In fact, while a binding instrument guarantees maximum harmonisation, it also risks to overburden digital industries; an extension of the scope of legislation to other OTT services will not automatically establish a transparent and competitive market.	competitive market industries
	The Apps Alliance recommends exploring a deregulatory approach which allows Authorities to include consumer protection provisions in more appropriate legal instruments; in addition, it will reduce the financial and regulatory burden on the telecoms industry at a time where the commission and Member States are looking for significant levels of investment in infrastructure and services.	financial industry investment
	When exploring the extension of the regulation, the Commission must consider whether there is clear economic evidence that regulation is proportionate and necessary to protect consumers from harm.	economic
	As a part of an effective deregulation strategy, the Apps Alliance supports the definition of industry standards for security and encryption.	industry
	Possible new rules concerning this matter should be technology neutral and should avoid to require any specific business model to be adopted.	business

Type of frame	Arguments by Application Developers Alliance	Key words/word combinations
	No new ePrivacy instruments should be adopted; instead, deregulation should be accompanied by the adoption of industry standards or Code of Conducts.	industry
	Proposed articles 8 and 10 would impose severe restrictions on service providers' ability to process data. In addition, these rules would limit the use of technologies (like cookies or analytics services) that are key for small and micro businesses, that rely on "free" business models (ads-based or freemium).	businesses
	A new discussion on issues such as profiling and advertising through article 10, already debated and regulated by the GDPR framework, would create confusion for small, dynamic businesses, especially those relying on ads-based business models.	businesses
	The Alliance observed that the impact assessment did not show a market failure big enough to justify stricter rules. More generally, the Alliance supports the Commission's Better Regulation agenda - which aims to reduce regulation, to the benefit especially of small industry players such as our members.	market industry
	In fact, the processing and aggregation of communication data enable software developers to create innovative products, including smart features, that are highly appreciated by the consumers.	innovative
	The current proposed rules would restrict and discourage the development of features based on content analysis, from the more traditional (such as spam-filtering or fraud detection software) to the most innovative (applied artificial intelligence). Some of the many examples of industry leaders collaborating to accelerate the growth of artificial intelligence	innovative industry growth
	Any laws or regulations relating to Artificial Intelligence should mirror the 'light-touch' approach that has allowed innovation to flourish, must take into account the challenges of regulating a burgeoning technology, and should be sensitive to additional compliance burdens placed on small- and medium-sized enterprises.	innovation enterprises
	Article 8.1 d) reduces the scope for data analysis provided by third parties, allows processing and storage capabilities of terminal equipment only when: - It is necessary for web audience measuring; - the measuring is carried out by (only) the provider of the information society service; - It is requested by the end-user. Such a narrow scope would severely impact small digital businesses that rely on third party providers for services supporting business models, going far beyond the simple "web-site measurement".	business
	In addition, art. 8.2 seems to add a further regulatory layer on the online advertising by imposing new obligations to request and offer information. We encourage policy makers to avoid adding new limiting provisions, provided the importance of an ads-based business model for the digital industry. We would like to underline the importance of the ads. 38% of worldwide developers base their business model on advertising, while only 21% are still profiting from downloads and 19% are looking for subscription revenue. On top of this, the trend of adopting mixed business model is growing: in many cases, paid app business models are integrated with alternative ads-based models.	business industry revenue
	Therefore, it is hard to understand why a paid-for model should be a preferable or even a viable option. The cost of setting up an infrastructure for payment would be high. There are also increased liability exposure and security risks that are inherent to collecting users' credit card information. Not least, the average user is not willing to pay for apps.	paid cost payment pay
	As the browsers provides the users with the privacy setting choices, relevant also for advertisement providers, the relation between the two players would need to be clarified further. Either through additional	businesses

Type of frame	Arguments by Application Developers Alliance	Key words/word combinations
	legislation or contractual agreements, this would translate into more obligations particularly burdensome for smaller businesses	
	The procedure established by art. 11 (2) of the current proposal might introduce unbearable notification procedures for software developers and publishers, especially for those with limited resources. The Developers Alliance worries that transparency requests, coming from all across the Union, would overwhelm smaller businesses. Therefore, we encourage policy makers to value the existence of one prevailing jurisdiction in order to ease the position of businesses and allow them to deal with any request efficiently.	businesses

Table 8:

In-depth analysis of frame choice by DIGITALEUROPE (Commission)

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
Public frame		
Consumer protection frame	To the extent consumer protection issues such as itemised billing, caller ID, call forwarding and directories are still relevant for the traditional telecoms sector, which is questionable, they are either sufficiently covered by existing legislation (e.g. eCommerce Directive) or should be transferred to other legal instruments.	consumer protection
	Under the Radio Equipment Directive, the Commission has the right to introduce additional requirements for certain equipment classes to safeguard user privacy and security of the data, but we have not yet seen whether this causes significant incoherence.	safeguard user security
	An essential element in the creation of user trust is how national data protection authorities shape market practices in their jurisdiction. These authorities have struggled with the implementation of the ePD. Trust cannot be built on a fragmented implementation of an EU rule, in particular when this fragmentation leads to complex local regimes that are not fully protective of the users.	protective users
	Self-regulation and co-regulation balances the protection and empowerment of users with fast-moving technologies. These solutions are also promoted by the GDPR.	protection users
	These provisions do not relate to privacy or data protection, but rather to commercial practices and consumer protection. Imposing these obligations under a set of privacy and data protection rules such as the ePD creates confusion for the users as to where their rights under EU data protection law start and end.	consumer protection
	Making sure the new ePR rules are clear and targeted to areas where there is a genuine legislative gap will both better protect Europeans' privacy and help organisations to comply.	protect Europeans
	DIGITALEUROPE has been particularly supportive of the inclusion of the legitimate interest legal basis for processing electronic communication data as well as for the use of storage and processing capacity of a device, as this would ease the pressure to try to enumerate all the possible exceptions that may be needed today and tomorrow, while ensuring accountability and high-level protection to the user.	protection user
	Scope – The potential extension of scope to cover OTTs, IoT devices, and M2M communications is not necessary to ensure the appropriate level of protection for consumers.	protection consumers
	The review of the ePD offers a unique opportunity to simplify and streamline legislation in line with the European Commission's Better Regulation Agenda; and to achieve a simple, consistent and	protect citizens

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	meaningful set of rules designed to protect citizens' privacy and personal data.	
	Further extending telecoms regulations to OTTs is not necessary to ensure the appropriate level of protection for consumers.	protection consumers
	Instead, given the already existing and appropriate safeguards achieving the desired protections for consumers and competition, regulators should repeal the telecoms and other provisions of the ePD, which are no longer necessary.	protections consumers
	We also strongly believe that no law should restrict an individual's ability to access and use the best possible technology/methods to secure and protect the confidentiality of the communications.	individual secure protect
	DIGITALEUROPE does not believe that maintaining Article 5(3) is necessary to achieve the high level protection of consumers privacy, already guaranteed by the GDPR.	protection consumers
	All provisions must be carefully considered as to whether they are relevant or bring any value to the protection of citizens.	protection citizens
Crime and security frame	Article 4 of the ePD requires that publically available electronic communication service providers adopt technical and organisational measures to safeguard the security of services appropriate to the risk. This is complementary to Article 13a in the Framework Directive and the NIS Directive insofar as the focus is on security of data processing as opposed to the integrity of the network (and continuity of services) found in the other two instruments. This could lead to a degree of overlap as security incidents impacting the provision of service could have a data security element, but it is at an acceptable level.	security security incidents
	Nevertheless, the ePD creates an unnecessary overlay that could lead to different security requirements and certainly gives rise to different enforcement bodies having the right to issue instructions to service providers, quite possibly in different Member States (given the OSS found under the GDPR).	security
	The examples the Commission brought up in ist Communication, such as the right to be forgotten on online social networking service, data breach notification and attacks on a gaming service clearly indicate that the entire review of the DPD was motivated to adjust to changes in the ICT sector.	data breach
	However, many proposed or existing national legislation pose a serious threat to the right to secure communications (e.g. proposals in Hungary to prohibit use of encryption software, or in France to increase sanctions on companies failing to decrypt data for terrorism investigations).	threat
	Law enforcement and national security agencies should be able to access data - subject of course to adequate safeguards. However, many proposed or existing national legislation pose a serious threat to the right to secure communications	security threat
	While DIGITALEUROPE recognises the sensitivity that some uses of terminal equipment data may have for consumers' private lives, we urge the co-legislators to consider and converge around a more flexible and granular approach. This would preserve organisations' ability to use terminal equipment data for worthy and non-privacy-invasive causes such as improving security, enabling technical functionalities and developing innovative products and services.	security
	Moreover, security plays an integral part in protecting users from malicious activity and generating trust in the reliability of devices and services. The Article 29 Working Party has consistently argued that processing for maintaining and managing technical security should fall under one explicit exception for the processing of terminal equipment data in the ePR. The European Parliament's report and the Council's Doc. 15333/17 have proposed an exception that only applies for security updates (i.e. downloads) to the device, but does not reflect the fact that detecting security vulnerabilities, with a view to creating	security malicious

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	patches, also requires an upload of data from devices. We therefore urge the co-legislators to adopt a more general security exception that is consistent for all type of data covered by the ePR.	
	A service provider may also store communications data for later analysis in order to protect its network from fraud and security threats as well as maintain and test the operation of its systems. Such practices will already be subject to the GDPR's limitations on the storage and later use of personal data.	fraud security threats
	DIGITALEUROPE welcomes the European Commission's suggestion to streamline security requirements and align these with the GDPR.	security
	Many processing activities, such as spam detection, the display or printing of an e-mail, providing automatic updates and back-ups, ensuring that devices are free from security vulnerabilities and many others happen seamlessly without representing a risk to users' fundamental rights and freedoms.	security
	In some situations, consent simply does not make sense. Asking a fraudster's consent for the purpose of detecting fraudulent activities would hardly be a practical solution. This is why the GDPR makes it clear that processing for the purposes of preventing fraud constitutes a legitimate interest of the data controller (see Recital 47 of the GDPR). Recital 19 of the Commission's text also conditions the 'scanning of e-mails to remove certain predefined material' to consent. This would mean that the removal of child abuse images, for example, would be subject to the abuser's consent.	fraudster fraudulent fraud abuse
	The same way the GDPR explicitly recognises that processing for the purposes of ensuring network and information security constitutes a legitimate interest of the controller; the ePR should also acknowledge that processing of communications data as well the use of processing and storage capabilities of terminal equipment for security purposes is allowed.	security
	We also welcomed additional flexibility suggested for Article 8 by the Parliament (Amendment 90). We would, nonetheless, ask for the security exemption to go further and be sufficiently flexible to ensure that users' devices as well as the broader ecosystem can be protected. For example, an infected device can distribute malicious software across the network and the user of the device may or may not be aware or want to stop this. The software / device provider should still be in the position to address this security threat.	security malicious
	More broadly, as we have argued on page 2, a security exception should recognise that detecting security threats requires an upload of data from devices, not just downloads of software updates to the device.	security
	DIGITALEUROPE welcomes the changes made by the Parliament to Article 11. The Parliament has helpfully clarified that any restrictions on the rights of individuals are only allowed in the areas of national security, defence and the prevention, investigation, detection and prosecution of criminal offences. We also very much welcome the clarification that the 'Union or Member States shall not impose any obligation on undertakings that would result in the weakening of the security and encryption of their networks and services'. We believe this is the right approach as it is not only fundamental for cybersecurity at large but also reaffirms the ePR's ambition to ensure that communications services and devices remain confidential and secure.	security criminal secure
	Security – The security provisions under the GDPR have the exact same objectives as the ePD. Keeping Article 4 or any version of this provision would only duplicate existing requirements.	security
	Confidentiality & Law Enforcement – The right to the confidentiality of communication should not only apply to the commercial context alone. The protection granted by the Charter is universal and should	security

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	also be ensured in the law enforcement and national security context. Any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures should be explicitly prohibited.	
	The new legal framework not only includes separate provisions and safeguards for sensitive data and risky processing (i.e. explicit consent, impact assessments and prior consultation), but also incorporated and expanded ePrivacy provisions on security, breach notification regime, and the processing of location and traffic data.	security breach
	Article 4 of the ePD requires that publicly available electronic communication service providers adopt technical and organisational measures to safeguard the security of services appropriate to the risk. This is complementary to Article 13a in the Framework Directive (new Article 40 of the Draft Code) and the NIS Directive insofar as the focus is on security of data processing as opposed to the integrity of the network (and continuity of services) found in the other two instruments	security
	However, it is important to underline that the security provisions under the GDPR have the exact same objectives as the ePD. As the Communication4 of the European Commission accompanying the release of the GDPR proposal underlines, the security provisions of the Regulation build on the ePD.	security
	Malware or other threat screening – Service providers routinely scan communications for malware, phishing and other attacks. Businesses need to be able to continuously scan incoming data packets for cybersecurity threats	malware security
	Filtering out illegal or unacceptable content – _Service providers often rely on automated tools to scan communications and files for illegal content, violent and graphic images, and other content that violates user policies and community guidelines. Businesses should be allowed to continue such activities.	illegal violates
	Preventing the loss of data and unauthorised access – Service providers (as well as government agencies) often rely on automated tools to scan communications to prevent data loss and detect unauthorised access to a closed internal network. These systems require the ability to inspect communications travelling within a network as well as those communications seeking to enter and exit a network.	unauthorized
	Whilst we understand the need for law enforcement and national security agencies to access data, subject of course to adequate safeguards and proper legal processes, a seemingly simple extension to cover all online communication services, M2M communications, etc., will in fact achieve an anti-privacy goal of potentially opening all of these services to national data retention and interception obligations. Many of these services are engineered to apply the best possible encryption technology to reinforce security and confidentiality of the communication. They were not designed to comply with many of the data retention and interception obligations, which would in fact have an adverse impact on the security of these services	security
	Finally, in addition to existing safeguards provided in Article 15 (1) (i.e. that measures need to be necessary, appropriate and proportionate), DIGITALEUROPE strongly recommends to ensure that any measures cannot result in a weakening of the security and integrity of the service.	security
	Indeed, storage and access are required for various different purposes, such as those i) aimed at maintaining and managing security and integrity; ii) aimed at obtaining information about the quality and/or effectiveness of a provided service; and iii) within the scope of legitimate interest under the GDPR.	security

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	Enforcement powers should be conferred on the public agency that is the most competent in the matter at hand. For the sake of consistency, and as far as information society services are concerned, matters related to personal data, including security measures related to the protection of personal data, should solely be dealt with by national data protection authorities, as per the GDPR.	security
	Given the central role of electronic communications in people's lives and the many uses which communications can serve, the ePR should be technology neutral and ensure legal flexibility to allow for data processing that has little or no impact on the right to privacy and confidentiality such as improving quality of service, providing automatic updates, ensuring that devices are free from security vulnerabilities and many others.	security
Human rights frame	No law should restrict individuals ability to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, a right enshrined in the Charter of Fundamental Rights.	Charter of Fundamental Rights
	However, many proposed or existing national legislation pose a serious threat to the right to secure communications (e.g. proposals in Hungary to prohibit use of encryption software, or in France to increase sanctions on companies failing to decrypt data for terrorism investigations).	right to secure communications
	A feebased service may work for certain business models, but would be in direct contradiction with a large number of others. In addition, such rules would be disproportionate to the objectives pursued and goes against the freedom to conduct a business, another fundamental right granted by the Charter (Article 16).	fundamental right
	As we have noted in Section 1 above, excluding non-personal data from the ePR's scope, bringing it in line with the GDPR, would solve this fundamental inconsistency. Similarly, a proper balance could be struck in the ePR by allowing the collection of information about technical quality or effectiveness that is limited by design to have little or no impact on the right to privacy and confidentiality, similar to the current Dutch implementation of the ePrivacy Directive.	right to privacy and confidentiality
	Many processing activities, such as spam detection, the display or printing of an e-mail, providing automatic updates and back-ups, ensuring that devices are free from security vulnerabilities and many others happen seamlessly without representing a risk to users' fundamental rights and freedoms.	fundamental rights and freedoms
	Confidentiality & Law Enforcement – The right to the confidentiality of communication should not only apply to the commercial context alone. The protection granted by the Charter is universal and should also be ensured in the law enforcement and national security context. Any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures should be explicitly prohibited.	right to the confidentiality of communication
	DIGITALEUROPE members support the fundamental right to the confidentiality of communications. Our strong stance on Better Regulation and simplification of the legal requirements does not call this commitment into question as we strongly believe that the two are perfectly in line.	fundamental right to the confidentiality of communication
	It seems that the only real reason for maintaining the current ePrivacy framework is to ensure that the fundamental right to private communications (as established in Article 7 of the European Charter of Fundamental Rights) is respected. Arguably a standalone legal instrument, such as the ePD, is not necessary to ensure that communications remain confidential. The right is fundamental in EU law and there is a wealth of EU national and case law where this right has been enforced and concretely implemented, even outside privacy legislation.	fundamental right to private communications Charter of Fundamental Rights

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	The right to the confidentiality of communication should not only apply to the commercial context alone. The protection granted by the Charter of Fundamental Rights is universal and should also be ensured in the law enforcement and national security context. The definition of ECS forms the basis of national data retention and interception laws. An extension of the scope would thus have an immediate impact on users' privacy.	right to the confidentiality of communication Charter of Fundamental Rights
	Given the central role of electronic communications in people's lives and the many uses which communications can serve, the ePR should be technology neutral and ensure legal flexibility to allow for data processing that has little or no impact on the right to privacy and confidentiality such as improving quality of service, providing automatic updates, ensuring that devices are free from security vulnerabilities and many others.	right to privacy and confidentiality
Economic frame		
	The provisions on confidentiality of electronic communications is one example where a lack of clarity has led to an intense debate among authorities, academics and businesses as to the exact meaning	businesses
	Nevertheless, national transposition in different legal frameworks often applicable to different industry sectors or contained in general data protection rules mean the lines around what qualifies as an electronic communication service covered by the ePD are blurry.	industry
	This inconsistency created additional costs for business and led to fragmentation in the internal market.	costs business market
	Moreover, as publically available is not subject to a consistent interpretation, questions arise in relation to certain enterprise-facing services.	enterprise
	We firmly believe that the mix between data protection authorities and telecom national regulatory authorities across the EU has proven detrimental to citizens and industry.	industry
	The GDPR not only improves consistency of enforcement, but also sets out a comprehensive regime for penalising companies that violate EU data protection rules.	companies
	An essential element in the creation of user trust is how national data protection authorities shape market practices in their jurisdiction.	market
	It is difficult to provide specific numbers regarding the costs for businesses to comply with the ePD requirements. It depends on the size of the company, the number of countries they are located in, and their data processing practices. However, as a general rule, it can be estimated that compliance costs range from several tens of thousands of euros to several hundreds of thousands euros; sometimes more for large multinational companies operating across the EU. In any event, the cost of compliance increases with the level of complexity of the rules, fragmentation in local implementation and overall legal uncertainty that is linked to each piece of legislation.	costs businesses company
	For the ePD, these factors can all be considered as high. This is particularly problematic for SMEs operating across the Single Market, which have faced in some cases an extreme administrative (and cost) burden to implement the cookie banner, which has failed to achieve its objective.	SMEs market cost
	Additional costs would include limitations of functionality of services based on the strict purposes under which traffic and location data can be used; delay in roll-out of services and cost of legal analysis based on the legal uncertainty surrounding covered services; and failure to integrate communication functionality in hybrid services in order to avoid being subject to both the ePD and the additional provisions under the Telecom Package that apply to publicly available electronic communication services.	costs
	We do not believe the compliance costs associated with the ePD are	costs

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	proportionate to the objectives pursued. Industry has been faced with conflicting provisions and an un-harmonised implementation across Member States. This has led to confusion and a negative impact for both industry and citizens.	industry
	Moreover, the compliance costs further overshadow the objectives of confidentiality when one considers the numerous Member State laws, which have created exceptions allowing national authorities to circumvent the confidentiality requirements placed on telecoms providers.	costs
	Companies should remain free to select, adjust and enhance the security measures appropriate to the risks presented by their data processing activities (a recognised principle of the EU acquis, see GDPR or NIS). It is not sustainable to only talk about securing communications in the commercial context.	companies commercial
	DIGITALEUROPE is very concerned about the proposal to prescribe business models and way of operation. One of the pillars of the ePD is its technology neutral approach outlined in Article 14, which should be the case for business models as well.	business
	Online services are too diverse to apply a one-size-fits all rule. A feebased service may work for certain business models, but would be in direct contradiction with a large number of others. In addition, such rules would be disproportionate to the objectives pursued and goes against the freedom to conduct a business, another fundamental right granted by the Charter (Article 16).	business
	An open market will allow companies to compete and users to rely on the services, which they believe constitute the best offerings.	market companies compete
	The guidance should be clear, reflect the years of experience with the cookies banner and allow for creative solutions and innovation so that companies can ensure the objective of Article 5(3), namely transparency and control, in consumer friendly ways.	innovation companies
	Moreover, in the B2B context, it is unlikely to make sense in any case for the individual user/employee to determine billing presentation as opposed to the business entity.	business
	By including non-personal data in its scope, the ePR effectively removes incentives for responsible companies to develop technologies and build services that are predicated upon anonymity and anonymisation, for instance through the use of data minimisation techniques.	companies
	DIGITALEUROPE therefore urges an alignment of the ePR with the GDPR's Recital 26 and Article 4, which explicitly excludes anonymous data from the scope of the GDPR. This should be reflected in the ePR's Article 2. The exception should not only be applicable to the process of anonymisation, but to anonymous data itself, i.e. where no further actions are needed to be taken for the data to be considered anonymous. As per our remarks above, this is the case today for the GDPR and strongly incentivises companies to rely on data that is not identifiable	companies
	While DIGITALEUROPE recognises the sensitivity that some uses of terminal equipment data may have for consumers' private lives, we urge the co-legislators to consider and converge around a more flexible and granular approach. This would preserve organisations' ability to use terminal equipment data for worthy and non-privacy-invasive causes such as improving security, enabling technical functionalities and developing innovative products and services.	innovative
	The development and improvement of device functionalities, better connectivity and innovative services hinges on the ability to collect information from users' terminal equipment on the part of a diverse number of parties in the technology value chain, including device makers (OEMs), component manufacturers and more	innovative

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	Today, many companies face the challenge that customers do not only request actions from their 'connected' machines, but also related services via 'M2M platforms'.	companies
	We welcome the intention of the European Commission to exclude closed user groups and corporate networks from the scope of the ePR. However, we would like this exemption to be clarified in an article.	corporate
	DIGITALEUROPE is concerned that previous interpretations of this term by the National Regulatory Authorities ('NRAs') have both included services offered to enterprises as a whole (as opposed to specific sectors) and considered the means of availability (e.g. purchase over the public internet) as the determining factor as opposed to who is being targeted by the service.	enterprises
	It is also important to remember that Recital 18 of the GDPR, on the other hand, does apply to 'controllers or processors which provide the means for processing personal data for such personal or household activity'. Thus, while the idea to offer more flexibility for companies to provide the above-mentioned services should clearly be reflected in the law, it should not be linked to these individual or household exceptions.	companies
	DIGITALEUROPE supports clarifications that would ensure that only services intended for the European market are covered by the scope of the legislation. People travel all the time with their devices in a way that is obviously not predictable for the provider.	market
	We would welcome further clarification that for terminal equipment to be covered, it should be 'placed on the market' and not just 'located' in the Union.	market
	The GDPR contains detailed rules on consent, which define when consent is valid, how it should be documented and users' rights regarding withdrawal and other areas. (See Annex for the provisions of the GDPR.) These rules nuance the existing requirements and companies are investing heavily in upgrading their infrastructure to reflect these.	companies
	As DIGITALEUROPE indicated in its response to the Article 29 Working Party consultation on the consent guidelines, companies should retain their freedom to define the services they provide and the conditions (including monetization) under which they make these services available.	companies
	However, DIGITALEUROPE is very concerned about suggestions that these should be limited to what is 'technically' or 'strictly' necessary. Such terminology could easily exclude processing activities that are needed to make a product or device functionality perform better and/or differentiate the various offerings on the market.	market
	Device Data (including "Cookies") – Any suggestions that would seek to prohibit businesses from preventing access to their services if the user refuses to accept a cookie must be avoided. This would not only disproportionately interfere with the freedom to conduct a business and the freedom of contract, but also undercut the EU's competitiveness in the data-driven and knowledge-based digital economy.	businesses economy
	Instead, given the already existing and appropriate safeguards achieving the desired protections for consumers and competition, regulators should repeal the telecoms and other provisions of the ePD, which are no longer necessary.	competition
	DIGITALEUROPE strongly believes that rejecting this double regulation would not lead to a decrease of the level of protection offered to users of communications services. On the contrary, clarity of the rules ensured by relying on the GDPR would benefit both consumers and businesses alike.	businesses
	SPAM detection – Service providers use a variety of automated tools to filter communications for spam or other undesired actions.	businesses

Type of frame	Arguments by DIGITALEUROPE	Key words/word combinations
	Furthermore, features for searching and archiving stored communications require access to communication content. Businesses need to continue to be able to execute such legitimate activities.	
	Filtering out illegal or unacceptable content – Service providers often rely on automated tools to scan communications and files for illegal content, violent and graphic images, and other content that violates user policies and community guidelines. Businesses should be allowed to continue such activities.	businesses
	Anonymisation – Service providers must be able to access communications to execute anonymisation techniques in line with privacy principles. This will help businesses improve their services and increase privacy protection.	businesses
	In much the same way, we oppose any suggestions that would seek to prohibit businesses conditioning access to their services to the acceptance of a cookie. This would not only disproportionately interfere with the freedom to conduct a business and the freedom of contract, but also undercut the EU's competitiveness in the data-driven and knowledge-based digital economy.	businesses economy
	It is important to recall that there are many applications and services that are offered free or low-cost to users due to the revenue gained through online advertising. Without this revenue, it would simply not be possible to offer free or low cost applications. It cannot be the objective of the European Commission to make each and every website on the web a paid-for service.	cost revenue paid
	It should be clear that, provided users are given clear, upfront information about access and storage of their personal data on their device (including for advertising purposes), as required by the GDPR, it is valid to obtain their consent by their accepting such access/storage as a condition of the installation of the free or low cost application or access to the website. Uninstallation of the application (or ceasing to access the website) should be equally accepted as the mechanism by which users withdraw their consent.	cost
	DIGITALEUROPE fears that free or low cost services will cease to exist if the EU follows an overly rigid interpretation of the consent requirements of the GDPR, let alone add further restrictions in a new law. This will have a very substantive detrimental effect on the app industry as well as consumer choice.	cost industry
	Allow sufficient time for implementation as companies would need to apply software changes to comply under the ePR and this, requires minimum 18 and preferable 24 months to implement.	companies

Table 9:

In-depth analysis of frame choice by Ecommerce Europe (Commission)

Type of frame	Arguments by Ecommerce Europe	Key words/word combinations
Public frame		
Consumer protection frame	Users are sometimes not fully aware of the national provisions implementing the e-Privacy Directive or the provisions of the e-Privacy Directive and sometimes they do not know how they (can) contribute to their trust in the protection of their (personal) data. However, most users trust their providers in taking the appropriate measures to protect their data when using electronic communication services and networks and being in compliance	user protection

Type of frame	Arguments by Ecommerce Europe	Key words/word combinations
	with the general data protection provisions of the e-Privacy Directive.	
	As the national provisions are the base for traders in protecting the privacy and personal data of consumers, they certainly have contributed to the increase of consumer trust.	protecting consumers
	the company/trader should only have an obligation to offer an opt-out mechanism in each commercial message sent to the consumer and not also at the moment of acquisition of the end-user's e-mail in the context of the sale of a product/service, as the latter is impractical and doesn't provide any more protection to the consumer	protection consumer
Crime and security frame	Moreover, Ecommerce Europe strongly recommends a new exception (subsection (e)) on behalf of repairing security, technical faults and/or errors in the functioning of information society services: *(e) it is necessary to maintain or restore the security of information society services, or detect technical faults and/or errors in the functioning of information society services, for the duration necessary for that purpose.*	security
Human rights frame	Instead of focusing on the processing of personal data and privacy aspects which are sufficiently covered by the GDPR also for electronic communications, the Regulation should focus on the right on confidentiality of electronic communications. This makes perfect sense given the fact that the main issues of the ePrivacy framework (confidentiality of electronic communication content and metadata, respect for the private sphere of the terminal equipment of the end-user and respect for a natural persons' electronic mailbox) are based on the fundamental right of respect for everyone's private and family life, home and communications, as laid down in Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) and not on the fundamental right to the protection of personal data, as laid down in Article 8 of the Charter and Article 16 of the Treaty on the functioning of the European Union.	right on confidentiality of electronic communications fundamental right of respect for everyone's private and family life, home and communications Charter of Fundamental Rights
Economic Frame		
	The various interpretations of a same provision created huge uncertainty among the numerous organisations which had to implement it, as well as important implementation costs.	costs
	Seen from a European level there is no uniformity in supervision because the national authorities in the Member States arrive at different interpretations and supervision of the provisions of the directive based on the minimum level of harmonization of the directive and the possibilities for national gold plating and the personal and financial resources they have available.	financial
	The same applies when, on national level, different authorities are competent. Practice shows that it is hard for the different competent bodies to come to a uniform and common interpretation and understanding of the directive. Especially in cross-border e-commerce relations this leads to confusion and extra compliance costs.	commerce costs
	Ecommerce Europe also supports co-regulation and soft-law in the digital sphere because technological developments and business models are evolving too fast in relation with the legislation which tends to lag behind.	business
	In the past, supervisory authorities also damaged the market because of a bad assessment of technical aspects and because they were too ideological.	market

Type of frame	Arguments by Ecommerce Europe	Key words/word combinations
	Ecommerce Europe endorses uniform regulation all over Europe and in that view it does not favor a choice for national legislators to diverge, which could end up hampering cross-border trade.	trade
	Especially the provisions for telemarketing calls (checking Robinson registers and revising all lists, offering text script on the right to object and registration in the Robinson register) did lead to costly adaptations in the processes of telemarketing.	costly
	Although we are convinced that e-commerce traders will never reject a customer and potential buyer for the reason of not accepting a cookie for which consent is needed, Ecommerce Europe basically supports entrepreneurial freedom on the two subjects. On the one hand, for a payment Ecommerce Europe admits that paying for the service in money could be a reasonable alternative for other counter-performance like being subject to advertising, personal data and accepting cookies, but it should be up to the provider of the service to choose such alternatives. As regards so-called cookie walls, especially providers that provide their electronic communication services for free should have the right to prevent access to their services in case users do not accept the storing of identifiers in their terminal equipment. Ecommerce Europe therefore rejects any mandatory regulation on both subjects.	traders payment paying money
	Non-itemised bills should be only on request and there should only be an obligation for the trader to grant the request when it is technically possible and financially reasonable.	trader financially
	A revision of the legislation is suggested in the sense that companies, which have acquired an end-user's e-mail address in the context of a sale of products/services, can send direct marketing by e-mail to advertise their own similar products/services, provided that the end-user is given the possibility to object (opt-out) on 3 aspects.	companies
	the company/trader should only have an obligation to offer an opt-out mechanism in each commercial message sent to the consumer and not also at the moment of acquisition of the end-user's e-mail in the context of the sale of a product/service, as the latter is impractical and doesn't provide any more protection to the consumer	company trader commercial
	web shops often offer a wide range of products and services which often cannot be seen as similar. The current provision only allows e-mail marketing on similar products and services, which is not logical in our opinion. It is obvious that the consumer provides an e-mail in order to enter into a relation and communication with the trader and not with the product or service bought. That's why we favor a revision of the provision that will allow the trader not only to do e-mail marketing on similar products or services, but also for the whole range of services and products offered in a web shop.	trader
	A revision of the scope of the future law in the sense that it will be limited to electronic communication services only and will not be applicable to traders selling goods/services as such and who only use electronic communication services to sell their products. It is unrealistic to see these traders as a service of the information society i.e. an electronic communication service.	traders
	A balance approach is needed: no unreasonable burdens on businesses.	businesses
	Ecommerce Europe also identifies some practical problems in the fact that the exception under d) is restricted to measuring carried out by the provider and is not extended to third parties. This is particularly problematic with regard to the current market for audience measurement.	market

Type of frame	Arguments by Ecommerce Europe	Key words/word combinations
	The major players that develop browsing software (Google Chrome, Microsoft Internet Explorer, Apple Safari) - all established outside of the European Union - would be able to regulate standard access to the terminal equipment by browser setting consent systems, not only for themselves but also for their competitors. This would in fact allow these players to have a very favorable position, permitting them to use cookies necessary for the operation of the browser itself for all the services they provide on the web (search, advertising, audience analysis, etc.) and preventing competitors to benefit in the same way from the browser settings. In that perspective, Ecommerce Europe asks European legislators to come up with provisions that prevent the major publishers of navigation software to abuse browser setting consent systems to have a competition advantage or not complying with the European standards required by the GDPR.	competitors competition
	As the consent mechanism for e-mail marketing in the proposed Regulation has not changed compared to the one in the current e-Privacy Directive, Ecommerce Europe strongly advocates that existing standards developed by industry that meet the criteria of the Directive (as for instance, UFMD appendix to code for the use of personal data in direct marketing by electronic communication) are recognized as also meeting the standards of the new Regulation, thus giving the industry the necessary comfort of not having to develop new consent standards.	industry
	Moreover, traders have to file which products or services they sold to assess every time they sent a new unsolicited marketing e-mail whether they are allowed to do so without consent. This highly impractical practice is not only opposite to the GDPR obligation of data minimization, but it is also not well understood by customers, as they have a relation with the retailer and not with the good or service subject to the contract they concluded with the trader and, thus, expecting unsolicited offers on all the traders' products or services.	trader

Table 10:

In-depth analysis of frame choice by ETNO (Commission)

Type of frame	Arguments by ETNO	Key words/word combinations
Public frame		
Consumer protection frame	The coexistence of two different set of rules creates legal uncertainty and confusion, undermining the coherence and trust on the online Consumer Policy, as European citizens cannot rely on consistent protection of their personal data and privacy.	citizens protection
	The scope of the recently adopted GDPR represents a decisive step to ensure a consistent level of protection to European citizens irrespective of the location of the provider.	protection citizens
	Europe needs to address the current patchwork of regulation, compromising the effective and consistent protection of consumers across the digital value chain.	protection consumers
	Maintaining two different set of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection.	consumer protection

Type of frame	Arguments by ETNO	Key words/word combinations
	In fact, users cannot rely on consistent protection standards across the digital market. In contrast to the GDPR, which applies horizontally, the ePD has thus done little to raise users trust.	users protection
	In this line, the Digital Single Market Strategy explicitly mentions that GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that offer their services on the European market.	protect individuals
	The new GDPR, together with the possibility to engage in ex-post antitrust actions (and the possibility of legal actions from national DPA), provide a comprehensive framework to monitor the commercial exploitation of users data by all kind of providers of digital services, regardless of the type of services provider at stake. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users.	safeguard individual users
	The GDPR provides for a higher level of protection for the processing of personal data than the former Directive: It equips consumers with improved rights and imposes upon controllers and processors to carefully evaluate the risks for individuals when processing personal data (with new impact assessment obligations in GDPR), including for other purposes (based on the newly introduced compatibility criteria for further processing), while considerably increasing user privacy through the introduction of safeguards like pseudonymisation and encryption.	protection consumer
	Trying to be even more protective for consumers, the future ePrivacy Regulation could actually have a negative effect on European consumers, reducing the ability for telecom operators in Europe to create the best in class products for them.	protective consumers
	European telcos want to be able to innovate whilst providing European citizens with high levels of privacy protection as in the GDPR and, at the same time, a wider range of choice of trustworthy high quality data driven services.	citizens protection
Crime and security frame	In 2009 the ePD introduced for the first time obligations on security for telecom operators; the GDPR has extended the scope of the new rules on security to all sectors seeking a comprehensive, technologically neutral set of rules on security of processing and data breach notifications. Therefore, it does not make sense to maintain dissimilar data breach notifications rules under the ePD.	security data breach
	The new GDPR, together with the possibility to engage in ex-post antitrust actions (and the possibility of legal actions from national DPA), provide a comprehensive framework to monitor the commercial exploitation of users data by all kind of providers of digital services, regardless of the type of services provider at stake. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users. As a result, there is no need to apply different tools than GDPR and Antitrust Law in order to monitor the commercial exploitation of traffic and location data by any provider of digital services.	antitrust exploitation abuse
	Identifiers placed to detect fraud, for frequency capping or those immediately anonymized so that it is impossible to identify the users device should not require prior consent.	fraud
	While we understand the willingness of the regulator to avoid abusive processing of interpersonal communications and of metadata, the proposed provisions are disproportionate and stand in the way of a range of legitimate data processing purposes	abusive
Human rights frame	Ensuring confidentiality of communications is a valuable objective. However, the costs of compliance have only encumbered a certain number of actors (ecommunications services providers) while other actors not covered by ePD should also ensure the confidentiality of communications and the fundamental right to privacy.	fundamental right to privacy

Type of frame	Arguments by ETNO	Key words/word combinations
	The discussions on the right of encryption in the post-Snowden era are primarily related to avoiding access to communications by Law Enforcement Authorities which is an issue that is not at stake in regard to the above question. Consequently there is no need for complementing the right of confidentiality of communications with details on encryption regarding the communication between individuals.	right of confidentiality of communications
	Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users fatigue without providing any enhanced level of protection to the right of confidentiality of the individual.	right of confidentiality
	Based on the GDPR, the data controller is asked to strike a balance between its legitimate interest and the fundamental rights and freedoms of the data subject. This is a big difference between GDPR and the ePR: the former allows/obliges the controller to undertake a thorough assessment, weighing in its interests with the interests and fundamental rights of the data subject. The controller will not be able to process the data if its interest is overridden by those of the data subject. In contrast, the ePR does not even allow any assessment on the legitimacy of interests.	fundamental rights
	If legislators decide to maintain a specific ePR in addition to the GDPR, the proposed Art. 6 ePR should be modified in order to align with Art. 6 GDPR incorporating the additional legal grounds: - processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.	fundamental rights
Economic frame		
	The ePrivacy Directive may have had an initial positive impact when it was first adopted. In light of new market developments and players and of the adoption of the GDPR, the directive is outdated and no longer necessary in a world of converged and globally connected online services.	market
	Regarding businesses, sectoral rules contribute to a substantial value migration from European operators to OTT players and device manufacturers mainly based outside Europe.	businesses
	The unequal application of rules for functionally equivalent services prevents telecommunications services providers from competing on equal footing in a single market.	competing market
	Consumers must be able to enjoy consistent privacy standards and experiences, irrespective of the technologies, infrastructure, business models, type or location of the service provider.	business
	Additionally, the lack of harmonisation has been critical for multinational companies.	companies
	As long as the ePD coexists with the new GDPR, there will be no level playing field, consumers will not experience comparable digital privacy online and operators will continue to face this dual compliance regime and their competitive position will be compromised.	level playing field competitive
	Both Directive 95/46/EC and ePrivacy Directive aimed at harmonising provisions on data protection at the EU level to avoid that national rules could become a barrier to the single market (both Directives were single market instruments).	market
	Being a Regulation, one of the objectives of GDPR is to achieve full harmonisation, which is absolutely necessary for both industry and citizens.	industry
	Maintaining two different set of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection.	market
	In fact, users cannot rely on consistent protection standards across the digital market.	market

Type of frame	Arguments by ETNO	Key words/word combinations
	The new GDPR will bring a more consistent and horizontal, sufficiently contributing to raise users trust and creating a level playing field. Sector specific regulation would thus only jeopardise this approach. In this line, the Digital Single Market Strategy explicitly mentions that GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that offer their services on the European market.	level playing field market companies
	Telecoms operators face considerable costs for implementing the provisions of the ePD at national level, such as requirements to provide itemised billing and printed directories and building performance features. These costs further increase with expenses for customer care and product development. However, the most significant costs are the opportunity costs, as traditional telecommunications operators have been prevented from offering new services demanded and broadly taken up by consumers, provided by other market players (eg.: geo-location based services).	costs expenses market
	Ensuring confidentiality of communications is a valuable objective. However, the costs of compliance have only encumbered a certain number of actors (ecommunications services providers) while other actors not covered by ePD should also ensure the confidentiality of communications and the fundamental right to privacy. This has put European telecommunications service providers at a competitive disadvantage vis-à-vis other players offering the same services, imposing a significant loss of competitiveness on the concerned organisations and a relevant impact on the innovation and on the time to market for new services.	costs competitive competitiveness innovation market
	Moreover, investments that would have been made in the absence of sector specific regulation are delayed of finally discarded.	investments
	The new GDPR makes specific sector specific regulation redundant. The recent CERRE study on Consumer Privacy in Network Industries (http://www.cerre.eu/publications/consumer-privacy-network-industries) states that a future proof regulation requires a common approach to all industries and that sectorspecific privacy regulations are inadequate in a dynamic environment and should be withdrawn.	industries
	Only in the unexpected case that provisions are still deemed relevant and necessary to be implemented in a specific ePrivacy instrument, such rules should be provided in the form of a Regulation and apply to all market players.	market
	Business and technological advances are able to provide suitable and user-friendly solutions and in practice do so already, even without further regulation. It is in the interest of industry to offer consumer-friendly solutions as a central differentiating factor in the competition between companies (race to the top). Thus, there is no need to further define security measures, especially as they cannot keep pace of technology developments.	business industry competition companies
	Generally, commercial services remunerated on the basis of end-users personal data have to fall under comparable rules as any other commercial service based on remuneration. End-users should be adequately informed, in line with what is prescribed in the Consumer Rights Directive. Currently, there is a loophole and providers of such commercial services do not inform end-users appropriately.	commercial
	In this line, ETNO would like to refer to the submission by the Danish Business Forum, which has called for the cookie regulation to be amended in a manner which will both decrease industry costs of implementation and raise awareness of privacy among users. Less intrusive types of cookies (for instance cookies used for website statistics) should be exempted and regulation should be reserved for websites using cookies that pose genuine risks of privacy intrusion. The benefits will be fewer burdens to businesses, more alertness to privacy issues among users, and the possibility of more effective and targeted enforcement.	industry costs businesses
	The telecommunication sector is highly competitive. Therefore, in case consumer demand still exists, the current consumer rights of the ePD	competitive market

Type of frame	Arguments by ETNO	Key words/word combinations
	(itemised billing, CLI, automated call forwarding, directories) can be left to the market itself.	
	For instance, rules on directories are redundant because they are outdated or already addressed by industry in practice. For instance, the development of powerful search engines and online services have changed the ability to search for professional services.	industry
	Therefore, the most important thing is to avoid this duplicity and allow the GDPR to create the necessary level playing field between all players irrespective of sector or geographic location.	level playing field
	In addition, the future ePrivacy Regulation should also recognize, in line with GDPR, the right to further process metadata for other purposes compatible with the initial purposes for which the data was initially collected, provided that appropriate safeguards like pseudonymisation are put in place. These principles are essential to ensure a level playing field in data protection, to encourage innovation in big data and to enable responsible e-communications providers to provide trusted and secure innovative data driven services in an accountable manner.	level playing field innovative
	GDPR will increase trust in digital services". ETNO therefore believes that the ongoing review of the ePrivacy Directive must be seized in order to at last move towards a consistent privacy framework for the benefit of businesses and consumers.	businesses
	Maintaining a double set of rules based on an old structure of sharing of competences will stand in the way of an equal level playing field, will continue to cause confusion for businesses and consumers and will finally hamper the possibility of European telco providers to develop innovative services.	level playing field businesses innovative
	Insufficient level playing field Based on the definition of electronic communication services as contained in the Electronic Communications Code, the Commission's initial proposal for the ePR expands its material scope of application to also include the so-called *over-the-top* players offering interpersonal communication services (e.g. Messenger, Gmail).	level playing field
	Art. 6.4. GDPR states that when the processing is not based on consent, further processing shall be allowed when compatible with the purpose for which the data was initially collected and appropriate safeguards like pseudonymisation have been taken. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. This is especially important for Big Data services, where enormous amounts of data from different sources are required, while it is sometimes impossible to determine the exact purpose for processing at the time of collection. Big Data analytics and innovative business models require possibilities to further process personal data for other purposes (without consent) once the compatibility test is fulfilled.	innovative business
	Introducing the same rule in the ePR would ensure enough flexibility to innovate and would eliminate a competitive disadvantage that in turn reduces consumer's choice. European telcos want to be able to innovate whilst providing European citizens with high levels of privacy protection as in the GDPR and, at the same time, a wider range of choice of trustworthy high quality data driven services.	innovate competitive
	ETNO calls for ePR to promote appropriate safeguards like pseudonymisation by aligning the rules for further processing of metadata with Art. 6.4. of the GDPR, including its strict compatibility criteria. GDPR encourages privacy-friendly techniques such as pseudonymisation "*to reap the benefits of big data innovation while protecting privacy*" as stated by the Commission itself when the political agreement on the GDRP was reached in December 2015	innovation
	If the above proposed changes would be considered unacceptable, achieving a level playing field focusing on the privacy risks associated to a specific kind of personal data (i. e. location data), then they should	level playing field

Type of frame	Arguments by ETNO	Key words/word combinations
	include all service providers processing the same type of data, irrespective of whether these services include electronic communications.	

Table 11:

In-depth analysis of frame choice by EuroISPA (Commission)

Type of frame	Arguments by EuroISPA	Key words/word combinations
Public frame		
Consumer protection frame	However, there are interesting studies, estimating only the cost of the implementation of the cookies requirements to $2.3 billion dollars [EUR 1.8 billion] per year (Castro/ McQuinn, The Economic Costs of the European Unions Cookie Notification Policy, ITIF, 2014, https://itif.org/publications/2014/11/06 /economic-cost-european-unions-cookie-notification-policy). These huge implementation efforts, often just bureaucratic burdens bear no relation to neither a consumer benefit in terms of better privacy protection, nor to the industry in terms of fair business models.	consumer protection
	This means that individuals should always be able to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, but more importantly no law should restrict that ability.	individuals secure protect
	Furthermore, Article 21 specifically states that individuals shall have the right not to be subject to a decision based on automated processing, such as profiling, which produces legal effects or similarly significant effects. These provisions provide a comprehensive protection for individuals, making any further regulation redundant.	protection individuals
Crime and security frame	Given the rapid evolution of communications services into platforms for commerce and money transfers such a weakening would not only affect the confidentiality of communications but also expose sensitive commercial data to hackers.	hackers
Human rights frame	the EU Treaty, EU Charter of Fundamental Rights, GDPR Directive and Member States' constitutions all already protect the secrecy of communication, thus allowing the use of encryption and other means of self protecting personal communication. New European legislation is not needed to ensure this already existing right.	Charter of Fundamental Rights
	Furthermore, there is a chance that legislating for such a right would actually result in a diminished right. This principle is enshrined as a fundamental right under Article 7 (Respect for private and family life) of the EU Charter of Fundamental Rights and has been further specified and applied through national and European case law.	fundamental right Charter of Fundamental Rights
	In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to define their business models, as long as the privacy rights of the users are protected	privacy rights
Economic frame		
	EuroISPA believes that we no longer need sector-specific privacy rules that govern the commercial use of personal data.	commercial
	The GDPR also sets out a comprehensive regime for penalizing companies that violate EU data protection law.	companies
	As the Commission noted in its press release, with the GDPR our work in creating first-rate data protection rules providing for the world's highest standard of protection is complete. Now we must work together to implement these new standards across the EU so citizens and businesses can enjoy the benefits as soon as possible.	businesses
	It is difficult for EuroISPA members to provide specific figures, as most companies did not track the costs of the implementation and as the	companies costs

Type of frame	Arguments by EuroISPA	Key words/word combinations
	implementation effort varied, depending on the business model and how it is affected by the respective ePrivacy provisions. However, there are interesting studies, estimating only the cost of the implementation of the cookies requirements to $2.3 billion dollars [EUR 1.8 billion] per year (Castro/ McQuinn, The Economic Costs of the European Unions Cookie Notification Policy, ITIF, 2014, https://itif.org/publications/2014/11/06 /economic-cost-european-unions-cookie-notification-policy) These huge implementation efforts, often just bureaucratic burdens bear no relation to neither a consumer benefit in terms of better privacy protection, nor to the industry in terms of fair business models.	business industry
	As outlined in Q11, we believe that costs exceeded the objectives.	costs
	Given the rapid evolution of communications services into platforms for commerce and money transfers such a weakening would not only affect the confidentiality of communications but also expose sensitive commercial data to hackers.	commerce money commercial
	This question dictates a technology and business model approach and would result in a radical change of the present business environment.	business
	Many information society services are based on free-advertising-funded business models that keep the services free of charge by allowing advertisers to show their advertisements to them. Regulation should not unduly interfere with companies freedom to choose and develop innovative business models where there is clear consumer demand. This would be contrary to the fundamental principle that regulation should only be enacted where it is necessary to address a clear issue in the market, and that any regulation should be proportionate and technologically neutral, so as not to favour certain business models or technology over others.	business companies innovative market
	In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to define their business models, as long as the privacy rights of the users are protected. This, however, falls into the remit of the GDPR.	economy growth companies business
	There is no necessity to treat traffic data any different than other kinds of data. This approach will result in redundant double regulation, that further restricts companies' opportunities to use such data and stifle innovation in Europe.	companies innovation

Table 12:

In-depth analysis of frame choice by EMMA/ENPA (Commission)

Type of frame	Arguments by EMMA/ENPA	Key words/word combinations
Public frame		
Consumer protection frame	As regards notification of personal data breaches, the GDPR already provides a comprehensive set of rules under Article 33, which does not require additional obligations to be created. The same applies to the issue of confidentiality of electronic communications as Article 6 of the GDPR already sets out a list of lawful grounds allowing data processing to be carried out with an enhanced protection of users privacy.	protection user
	It is therefore of utmost importance to clarify that, on the one hand, only providers of electronic communication service providers have to comply with the consent requirement of Article 5(3) for any 'information' stored or accessed; while, on the other hand, information society service providers can lawfully process personal data on the basis of 'informed opt-out', in line with what the new EU Data Protection Regulation (GDPR) provides. This clarification is urgently needed especially now that the GDPR grants	individual protection

Type of frame	Arguments by EMMA/ENPA	Key words/word combinations
	individuals comprehensive and enhanced protection of their personal data while acknowledging various legitimate legal bases for processing. ‘	
Crime and security frame	-	
Human rights frame	-	
Economic frame		
	As far as Article 5(3) and Article 13(3) have not only been applied to electronic communication service providers but to all information society service providers, including press publishers, this has led to substantial implementation costs, resulting, inter alia, from disproportionate and lengthy litigation procedures. According to our members, the initial cost of compliance can amount to 120.000 euros for a publisher (to set up the banner and all the technical settings). Once the maintenance costs are added, the total cost reaches between 200.00 and 250.000 euros for a single publisher.	costs
	A general consent requirement for the setting of cookies only favours large international companies such as free e-mail providers or social networks, which base their business models on log-in systems. For those companies it is relatively simple to obtain the required consent of their customers, due to the direct contact inherent in the system with their customers.	companies business
	Furthermore, it is and should remain the sole business decision of a publisher, whether or not to rely on paid subscription revenues only.	business paid revenues
	Ultimately, a publisher will choose a business model that is best suited to meet its customers demands.	business
	The abovementioned proposals are also out of touch with reality. In the very large majority of cases, a user who refuses cookies will still be given the opportunity to access the non-paid-for content because a publisher does not want his content not to be accessed. However, such a decision affects the relevance of ads, reducing the quality of the user experience, and ultimately impacts the publishers advertising revenues. Such repeated calls to ask content providers to give up ad-financed business models are a great source of concern for ENPA and EMMA members.	paid revenues financed business
	Newspaper and magazine publishers are facing many challenges as regards digitization and are investing in the development of digital business models to finance their editorial products across all platforms. They need to be able to interact easily with their readers, especially in the digital environment, to be able to adapt to their readers needs. Cookies are one of the most common and efficient tracking tools used by internet society service providers, including press publishers for a variety of purposes (interest-based advertising, statistics, personalised content, etc.). They allow publishers to develop innovative ways of reaching out to their readers online, for instance by matching their potential interests with tailored advertising offers. Misinterpretations of the scope and requirements of Article 5(3) have had detrimental consequences in some countries (including financial costs) and represent further obstacles to the development of data-driven business models online.	investing business finance innovative costs
	Newspaper and magazine publishers are facing various challenges in relation to the digitization of their industry but are making significant investments in order to develop their digital business models and be able to continue to finance high quality journalistic content.	industry investments business finance
	In addition, cookies enable better targeted advertising. Advertising revenues are a key component of today’s press publishers’ online business models and allow editorial content to be financed and made available at no cost for European citizens.	revenues business financed cost
	‘Informed opt-out’ in practice means that data subjects are provided with transparent and clear information about the processing of their personal	companies business

Type of frame	Arguments by EMMA/ENPA	Key words/word combinations
	data and can easily decide to object to such processing. At the same time, small and medium-sized companies, including the vast majority of press publishers, can justify their data processing on the basis of legitimate interests, in particular where relying on consent (which is eventually a business decision) is not possible or appropriate.	
	The European Commission should not propose legislation imposing a particular type of business model on private undertakings. This would infringe the fundamental freedom to conduct a business while not efficiently and proportionately addressing the issue at stake. There are many good reasons why a publisher may choose not to offer a paid-for service (e.g. because of the type of publication, or in order to create a large audience base, etc.). Ultimately, this is and should remain the sole decision of a publisher whose aim is to find a business model that best suits its consumers' demands.	business paid
	Furthermore, EMMA and ENPA are not aware of a significant number of cases where a user who has refused cookies being left on his terminal equipment is not afterwards given the possibility to access the non-paid-for content. However, it is true that such a decision affects the relevance of ads, reduces the quality of the user experience, and ultimately negatively affects publishers' advertising revenues.	paid revenue
	Finally, it must be reiterated here, that a general 'opt-in'- like consent requirement for the setting of cookies only favours those companies whose business model is inherently based on user log-in. Because such a log-in step is necessary for users to access the service, these companies do not have any difficulty with obtaining consent. Some degree of flexibility must therefore be ensured and this is why we would ask the Commission to clarify the scope and requirements of Article 5(3).	companies business

Table 13:

In-depth analysis of frame choice by EPC (Commission)

Type of frame	Arguments by EPC	Key words/word combinations
Public frame		
Consumer protection frame	HTML code sites need short term storage of information to the RAM memory of the computer in order to deliver extra and faster services to the user. However, this could be perceived as not strictly necessary as stated in the provision, which means that it is yet another element of online activity that would require users consent despite the fact that it does not have any impact on the users privacy. This broad wording of the article should be annulled as it is a source of great legal uncertainty for the operators, and frustrates subscribers and users rather than strengthening the protection given to them.	users protection
	Regarding the areas of interest to EPC membership, we believe that the additional protections of ePD afforded to subscribers and users are effectively non-existent.	protections users
	Legislation should keep the right balance protecting the privacy of consumers on the one hand and business interests on the other.	protecting consumers
Crime and security frame	Moreover, as the recent study on the implementation of the ePD showed, there is notification fatigue and an over use of the notion of consent with users ending up indiscriminately consenting to anything, which poses a bigger threat to their privacy.	threat

Type of frame	Arguments by EPC	Key words/word combinations
	Regarding abusive behavior as described in the background document, it should be noted that the user has given his/her consent or has activated a specific functionality that requires certain technical procedures in order to be functional.	abusive
Human rights frame	Many forget that in the Charter of Fundamental Rights Art 16 and 17 protect the freedom to conduct business and the right to property, therefore they should be taken equally into account when formulating policy proposals.	Charter of Fundamental Rights
	Many publishers choose to offer advertising funded services, free to consumers at the point of access, in order to reach as large an audience as possible, thereby providing the opportunity of access to knowledge, information and analysis to the less privileged members of our societies, offering them a window to the world and to facilitate consumers Charter Article 11 Right.	Charter Right
Economic frame		
	In all member states the Data Protection Directive is under the competence of the national DPAs. However, the ePD has more enforcers such as the National Regulators for Telecommunications or Consumer Protection authorities. This multitude of enforcers creates confusion to the citizens as much as to the operators, leading to duplication of compliance, and associated costs.	costs
	It would be beneficial in terms of legal certainty and compliance to have only one authority with whom to discuss privacy issues. Given the recent adoption of the GDPR this would seem even more important. However this role would need to be properly funded and resourced, and accompanied by transparency and duty of care requirements for the DPAs to ensure that they are more open to industry and engage in better and more constructive dialogue.	industry
	The ability to allow member states to choose between opt-in or opt-out system is paramount given the very national nature of the issue for different reasons. These include cultural reasons, language, and market access conditions etc.	market
	Furthermore, industry has undertaken efforts to create telemarketing preference services and Robinson lists in order to give consumers the choice to receive or not direct marketing. Market data shows that the opt-out mechanism works well and it is the preferred method of the majority of the member states.	industry market
	Industry has shown responsibility by setting up a self-regulatory program providing simple information to users, but also providing them with the tools to exercise effective choices and control by opting out of data collection via cookies for the purposes of online behavioral advertising techniques, which have been very well received by consumers.	industry
	Cost estimation (direct, indirect or opportunity costs) is very difficult. Of course, publishers have to prepare and maintain a Cookie Policy along with a website pop-up/banner. Obvoopusly (sic!) the size of the company (sic!) as well as the markets it is operational affects the above costs.	cost company markets
	Depending on the subject matter, it is true that Regulations can benefit businesses because of the harmonized, directly applicable nature of the rules and legal certainty they provide by comparison to Directives. In this case, we do not believe that we need a further legal instrument as the issues of privacy and personal data have been harmonized comprehensively under the GDPR.	businesses
	However, now that the Commission is operating under Better Regulation principles, we call on the Commission to look holistically at the area of privacy and confidentiality and see where regulatory burden can be reduced and not multiplied. Otherwise, if this Directive is revised and adopted (as either a Directive or Regulation) its implementation will follow immediately after a major duty and cost to companies to comply with the	cost company

Type of frame	Arguments by EPC	Key words/word combinations
	new GDPR. In our view this would be disproportionate to any benefit from a separate, additional instrument.	
	Legislation should keep the right balance protecting the privacy of consumers on the one hand and business interests on the other. Many forget that in the Charter of Fundamental Rights Art 16 and 17 protect the freedom to conduct business and the right to property, therefore they should be taken equally into account when formulating policy proposals.	business companies
	Any attempt for legislation that imposes business models on privately held companies should not even be considered by the European Commission as it goes beyond proportionate public policy objectives.	business companies
	Contractual freedom is paramount in the free economy and should have as little interference as possible.	economy
	For a number of reasons, almost all companies in the digital sphere operate under adhesion contracts, an essential part of doing business. In any case, informed users have always the ability to turn to alternative services if they think that the business model or the terms of an operator doesnt suit them.	companies business
	Given the global nature of the internet any attempt to produce only European standards would be a failure and disregard the reasonable expectations of a global industry.	industry
	Specifically on cookies, the industry has set up an effective self regulatory program, giving consumers simple information, effective choices and simple to use tools to opt-out of OBA cookies.	industry

Table 14:

In-depth analysis of frame choice by GSMA (Commission)

Type of frame	Arguments by GSMA	Key words/word combinations
Public frame		
Consumer protection frame	The ePDs current scope does not reflect the converging area of electronic telecommunications where functionally equivalent services are not subject to the same regulatory constraints. Accordingly the ePD is neither technology-agnostic nor provideragnostic. This has led to the problem that users cannot rely on consistent protection standards across the digital market even when using comparable services.	users protection
	As a consequence of the current outdated EU telecommunications framework, users cannot rely on consistent protection standards across the digital market even when using comparable services. This is especially the case for the provisions of the ePD that only apply sector specific to classic telecoms and thus ignore the converging area of telecommunications, where functionally equivalent services are not subject to the same regulatory constraints.	users protection
	As it is applied only to telco providers and not to other players supplying similar services, the consumer is not protected in an equal measure and telco operators have been put at a competitive disadvantage compared to other players offering similar services.	consumer protected
	These provisions refer more to consumer protection principles than to privacy principles. The first three items can be offered to subscribers on commercial basis to if demanded and the fourth may no longer be needed.	consumer protection
	It should be noted that even without explicit duties in law, there exists for organisations an inherent commercial and/or reputational imperative to keep their customers communications and data safe.	customers safe
	An overall consumer protection standard has to be established to ensure that consumers are protected regardless of their location. Unsolicited	consumer protected

Type of frame	Arguments by GSMA	Key words/word combinations
	marketing communication is not an electronic communications sector specific occurrence. Consequently, such provision should be regulated under a more horizontal framework applying to - at minimum - digital services in general.	
	General consumer protection, such as included in the current review of the Unfair Commercial Practices Directive, as well as in the GDPR (Recital 47, 70, Art. 21.2, 21.3), already sufficiently include applicable rules on marketing.	consumer protection
Crime and security frame	Telecommunications providers specifically encounter problems in regard to the notification of personal data breaches due to inconsistencies between the obligations under Directive 95/46 EC and the obligations set out in Directive 2002/58 EC specified by Regulation 611/2013. While a data breach subject to Directive 2002/58 EC has to be notified within 24 hours in accordance with Art. 2 of Regulation 611/2013, there is no general obligation on businesses to notify data breaches either to DPAs or to the affected data subjects under Directive 95/46 EC. In the meantime, several Member States have passed their own data breach notification duties and the GDPR will soon introduce a 72 hour notification period. The existence of more than one data breach notification regime leads to complexity for telecom operators who are forced to decide which regime they should notify incidents under or to notify under both. As there are no objective reasons to maintain such differences, Art. 4 of the ePD and Regulation 611/2013 should be entirely substituted by the corresponding articles of the GDPR.	data breach
	Additionally the divided interpretation and implementation of article 6 has led to many questions and concerns. In some Member States traffic data is only permitted to be processed for transmission of communication and for billing purposes. For example processing for fraud prevention would not be allowed even with consent.	fraud
	It should further be taken into account that the processing of traffic and location data can help protecting communications from the threat of malware and viruses.	threat malware
	Data breach notification is covered by GDPR. GDPR would also cover lawful use of location and traffic data which is increasingly important for innovation and growth in the context of the Digital Single Market	data breach
	All types of network listed whether public, private, closed or non-commercial WIFI) should apply a level of security that is appropriate to the circumstances.	security
	Risks to consumers from use of traffic and location data can be adequately dealt with under the GDPR and do not need to be addressed in a separate and sector specific piece of legislation. If specific rules are deemed necessary, they should provide that the legal grounds for processing personal data given by GDPR (art. 6) including protecting communications from the threat of malware and viruses also apply to traffic and location data.	threat malware
Human rights frame	-	
Economic frame		
	The objective of an equal protection is no longer achieved, since the ePD has not kept pace with an increasingly dynamic digital market.	market
	The ePDs current scope does not reflect the converging area of electronic telecommunications where functionally equivalent services are not subject to the same regulatory constraints. Accordingly the ePD is neither technology-agnostic nor provideragnostic. This has led to the problem that users cannot rely on consistent protection standards across the digital market even when using comparable services.	market

Type of frame	Arguments by GSMA	Key words/word combinations
	With the application of the GDPR, a more consistent and horizontal approach will be taken, which leads to a level playing field and thus contributes to raise users trust.	level playing field
	It is difficult to quantify the additional costs directly related to the measures included in a single legal instrument as data protection related implementation stems from different legal sources. Although precise costs are not available, it is well recognized that the costs of compliance with multiple and overlapping regulatory paradigms places a financial burden on service providers. By making it far more difficult for ISPs to do what edge providers such as Over-the-Top service providers and Operating System developers do use non-sensitive customer data to engage in socially productive first and third-party marketing the rules would reduce the profitability of broadband services, exert upward pressure on broadband prices, and depress incentives for broadband deployment. Thus, it is critical for the ePD to align with the GDPR in a way that facilitates the efficient growth of the DSM ecosystem to achieve the economic and social benefits that DSM can bring to consumers.	costs financial growth economic
	The costs of compliance are not proportionate in so far as the rules do not achieve the goal of ensuring confidentiality of communication to all consumers.	costs
	As it is applied only to telco providers and not to other players supplying similar services, the consumer is not protected in an equal measure and telco operators have been put at a competitive disadvantage compared to other players offering similar services.	competitive
	A harmonised approach across the EU is preferable and will help to establish a Digital Single Market.	market
	Sector-specific legislation like the ePD is therefore not the right tool to tackle privacy related issues in a harmonised and technology neutral approach towards all industries.	industries
	Only in the unexpected case that provisions are still deemed relevant and necessary to be implemented in a specific ePrivacy instrument, should such rules be provided in the form of a Regulation and apply to all market players.	market
	Key factors to facilitate users' ability to consent without disrupting the Internet experience are inter alia requiring manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings as well as to mandate European Standards Organisations to produce standards and the support of self-co regulation.	market
	These provisions refer more to consumer protection principles than to privacy principles. The first three items can be offered to subscribers on commercial basis to if demanded and the fourth may no longer be needed.	commercial
	Data breach notification is covered by GDPR. GDPR would also cover lawful use of location and traffic data which is increasingly important for innovation and growth in the context of the Digital Single Market	innovation growth market
	Further, due to the telecommunication sector’s nature of being highly competitive, related consumer provisions will be dealt with by the market itself, if user demand calls for it. Generally, in cases where a competitive market can solve the required objectives through self-regulation, any unnecessary legislation leads to legislative burden and disproportionate costs.	competitive market costs

Firms

Table 15:

In-depth analysis of frame choice by Cisco (Commission)

Type of frame	Arguments by Cisco	Key words/word combinations
Public frame		
Consumer protection	Under the Radio Equipment Directive, the Commission has the right to introduce additional requirements for certain equipment classes to safeguard user privacy and security of the data but we have not yet had occasion to see whether this causes significant incoherence.	safeguard user security
	As mentioned above, the DPD provides the overall protection of individual's data in the EU, soon to be surpassed by the GDPR.	protection individual
	While tracking cookies may allow the build up of a user profile that we consider important to know about, control and protect, it is not immediately obvious why we need to consent in the same way to cookies that allow the information society service provider to know when the user is logged in or offer content in the user's preferred language.	user protect
	Consumer protection issues in this context are adequately addressed by the eCommerce Directive.	consumer protection
	As should be apparent from the analysis above, we believe that the most appropriate path would be repeal of the ePD and transfer of the provisions categorised as consumer protection issues to other legal instruments to the extent they are still relevant for publicly available electronic communication service providers.	consumer protection
	To the extent provisions characterised above as 13 consumer protection issues should be maintained for publicly available electronic communication services, we hold that they should be transferred to other legal instruments.	consumer protection
Crime and security frame	Article 4 of the ePD requires publicly available electronic communication service providers to adopt technical and organisational measures to safeguard the security of services appropriate to the risk. It is complementary to Article 13a in the Framework Directive and the NIS Directive insofar as the focus is on security of data processing as opposed to the integrity of the network (and continuity of services) found in the other two instruments. This could still lead to a degree of overlap as security incidents impacting the provision of the service could have a data security element but it is at an acceptable level.	security
	The security provisions under the GDPR, on the other hand, have the exact same objective as under the ePD.	security
	Nevertheless, the ePD creates an unnecessary overlay that could lead to different security requirements (especially as the GDPR requirements are somewhat broader) and certainly gives rise to different enforcement bodies having the right to issue instructions to service providers, quite possibly in different countries (given the one stop shop found under the GDPR).	security
	The Directive on Attacks against Information Systems criminalises the illegal interception of information systems, data controllers and processors are subject to specific rules as to when they can process personal data (including accessing data) in the GDPR and the new Data Protection Directive for the police and criminal justice sector includes similar safeguards.	criminalises illegal criminal
	Indeed, the GDPR includes separate provisions for perceived risky data and processing scenarios. This includes special categories of data (such as ethnic origin or health data) and data on criminal offences, decisions	criminal

Type of frame	Arguments by Cisco	Key words/word combinations
	based on automated processing and impact assessments and prior consultation of data protection authorities for high-risk processing.	
	The equivalent provisions in the GDPR are in Article 32. This also requires technical and security measures to ensure a level of security appropriate to the risk. It is somewhat broader, however, insofar as it covers confidentiality, integrity, availability and resilience of systems and services, as well as a testing and evaluation process.	security
	The public consultation on the review of the ePD raises additional questions as to whether security measures should be extended to cover 1) software used in combination with the provision of the communication service (such as the operating system of the terminal equipment) 2) Internet of Things (IoT) devices and 3) network components, such as SIM cards, switches and routers. It is not clear whether the intention is for the responsibility for such security to lie with software or hardware manufacturer or their owner/ operator.	security
	Under the GDPR, the controller of the processed personal data, or the entity that processes it on their behalf, is responsible for ensuring the security measures are undertaken in each of the outlined three cases. This makes sense given that they determine the use case (and hence the level of security appropriate to risk), actually handle the data being processed and have the scope to implement the full range of security measures (e.g. access by authorised personnel). To the extent such devices are used for critical services, where the risk of a security incident would have a higher impact on the economy or society, it is also worth noting that they are subject to security measures under the Network and Information Society Directive. We do not see the need to extend the security measures given this coverage in other legislation.	security
	As a result of the arguments above, there is no need to maintain or extend security measures or maintain data breach requirements under the ePD.	security data breach
	Moreover, the restrictions identified under Article 15(1) of the ePD are repeated in Article 23 of the GDPR, such as necessary and proportionate restrictions for the purposes of national security, defence, public security and processing relating to criminal offences. Points 3) and 4) could be construed as examples of legitimate interest (Article 6.1(f) of the GDPR) or in certain circumstances, necessary for the performance of a contract (Article 6.1(b)).	security
	Moreover, additional legitimate interests, such as network and information security, should also apply.	security
	There is a strong case to be made that certain cookies are necessary for the use of the site, such as authentication or security and site integrity cookies. Others are necessary for full functionality, such as site features and services or localisation cookies.	security
	This difference in privacy expectations can be seen in relation to the other provisions. Storage or access to the terminal equipment of an employee is necessary for a range of purposes in the workplace, such as provisioning the device in the first instance, updating enterprise software or security. Keeping logs on communications could be necessary for legal or myriad business purposes. Workers location may need to be tracked for physical security, logistics or workplace resource management.	security
Human rights frame	Individuals should have the right to secure their communications but we are not convinced that the ePD, or its potential successor, is needed to achieve this end. The right to secure communications is expressed in legislation in terms of actors who may have the possibility to access communications being required to abide by rules governing such access.	right to secure communications
	While we recognise the needs of law enforcement and national security agencies to access data subject to adequate safeguards, it is worth noting that national proposed or existing legislation that could undermine the right to secure communications is usually framed in relation to the objectives of such agencies (e.g. proposals in Hungary to prohibit use of	right to secure communications

Type of frame	Arguments by Cisco	Key words/word combinations
	encryption software, proposals to increase sanctions on companies failing to decrypt data for terrorism investigations in France, potential changes to decryption powers under the UK's Investigatory Powers Bill).	
	The right to private communications is established in Article 7 of the European Charter of Fundamental Rights. As a result, it is important that this fundamental right is adequately reflected in Community law.	right to private communications Charter of Fundamental Rights
	For example, there may be other legitimate interests that would allow such processing, Article 6.1(d) allows for processing in the vital interest of the data subject and Article 6.1(e) for tasks carried out in the public interest. It is worth noting, however, that the fundamental rights of the data subject, including private communications, take precedence over legitimate interest, so they are in any way protected and use will be limited.	fundamental rights
	In terms of confidentiality, even under the ePD which applies to publicly available networks, the drafters felt the need to provide an exception for recording communications in the ordinary course of business for certain purposes. In January 2016, the European Court of Human Rights held in the case Barbulescu v. Romania that monitoring of an employee's communications for reasonable and proportionate ends did not breach Article 8 of the European Convention on Human Rights (right to private life). This clearly differs from monitoring in the private sphere.	European Convention on Human Rights right to private life
Economic frame		
	Nevertheless, national transpositions in different legal frameworks – often applying to different industry sectors or contained in general data protection rules - mean the lines around what qualifies as an electronic communication service covered by the Directive are blurry.	industry
	Moreover, as "publicly available" is not subject to a consistent interpretation, questions arise in relation to certain enterprise-facing services.	enterprise
	We have not conducted an holistic analysis but it is worth noting that an ITIF study put the cost of compliance with the cookie notification provision alone at $2.3 billion a year in Europe. Additional costs would include limitations of functionality of services based on the strict purposes under which traffic and location data can be used; delay in roll-out of services and cost of legal analysis based on the legal uncertainty surrounding covered services; and failure to integrate communication functionality in hybrid services in order to avoid being subject to both the Directive and the additional provisions under the Telecom Package that apply to publicly available electronic communication services.	costs
	According to our understanding, the ePD adds little in terms of protection related to the risks presented but brings significant additional costs.	costs
	Independent of these concerns, it does not seem proportionate to interfere with the business model of such services if consumers clearly see the benefit of the service in question and are happy to pay with their data.	business pay
	The mandate of expensive new services is not commensurate with the return in terms of public good, particularly in a competitive market.	expensive competitive market
	To the extent consent would be required and this could be achieved through alternatives to cookie notification, this is best achieved through an industry-led approach.	industry
	There are four exceptions to this: 1) where the users have provided their consent 2) legal authorisation in accordance with Article 15(1) 3) technical storage necessary for the conveyance of a communication 4) legally authorised recording carried out in the course of business for the purpose of providing evidence of a commercial transaction or other business communication.	business

Type of frame	Arguments by Cisco	Key words/word combinations
	If the confidentiality provision is nevertheless maintained or extended to cover other communication providers, Article 5.2 of the ePD should be amended to recognize that the recording of the content of communications is for legitimate business reasons as opposed to providing evidence of business communications per se.	business
	In relation to the possible extension of the ePD to non-traditional communication services, it is not always clear how the requirement for only persons acting under the authority of the communications provider to process the data would apply. Particularly for enterprise solutions, the communications service provider may share the data back with the enterprise customer about their user group.	enterprise
	It could also relate to types of functionality, like the ability to record sessions or share documents. For consumer services, the services are often not subject to direct payment – the only monetary payment may be to the underlying provider of the electronic communication service as opposed to the communication application provider. In the business-to-business context, it is unlikely to make sense in any case for the individual user/ employee to determine billing presentation as opposed to the business entity.	payment monetary business
	Given how many different kinds of communications services users have available to them, they should be allowed to choose whether they want ones that support anonymous calling or not. Expanding this requirement to all services would constrain the market for those services, potentially eliminating services targeting uses by small or trusted communities of users.	market
	If you take the popular What's App application, for example, you already need to have the contact details of an individual on your device before they become visible to you in order to add them to your network. In the business-to-business space, such a right can actually be obtrusive. In a corporate directory, it could be disadvantageous to make the decision maker on inclusion of work contact details the individual as opposed to the entity.	business
	Independent of these concerns, it does not seem proportionate to interfere with the business model of such services if consumers clearly see the benefit of the service in question and are happy to pay with their data. The mandate of expensive new services is not commensurate with the return in terms of public good, particularly in a competitive market.	business competitive market
	In terms of confidentiality, even under the ePD which applies to publicly available networks, the drafters felt the need to provide an exception for recording communications in the ordinary course of business for certain purposes.	business
	This difference in privacy expectations can be seen in relation to the other provisions. Storage or access to the terminal equipment of an employee is necessary for a range of purposes in the workplace, such as provisioning the device in the first instance, updating enterprise software or security. Keeping logs on communications could be necessary for legal or myriad business purposes. Workers location may need to be tracked for physical security, logistics or workplace resource management.	enterprise business

Table 16:

In-depth analysis of frame choice by Facebook (Commission)

Type of frame	Arguments used by Facebook	Key words/word combinations
Public frame		
Consumer protection	Accordingly, where privacy regulations applied to traditional telecommunications operators are no longer needed to protect consumers, because they are adequately covered in the GDPR or other legislation, they should be eliminated.	protect consumers
	Extending regulation out to Online Services risks undermining the existing protections in place and could stymie innovation in this area to the detriment of consumers who wish to have a high level of security for their communications. With regard to broader consumer protection issues, these can all be dealt with under the existing body of consumer protection law at EU level (e.g., such as the Unfair Commercial Practices Directive, digital content rules etc).	protection consumer
	Where the provisions are no longer needed to protect consumers because they are adequately covered in the GDPR or other legislation, they should be eliminated.	protect consumers
	Furthermore, in any event, there is no need to extend provisions of the ePD to Online Services, which are already sufficiently regulated by existing EU privacy and consumer protection provisions.	consumer protection
	Extending telecoms type regulations to Online Services is not necessary to ensure the appropriate level of protection for consumers, as Online Services are already subject to a variety of European Union directives that ensure this protection in the digital space. Instead, given appropriate safeguards, regulators should perhaps consider removing telecoms regulations where no longer necessary to protect consumers or competition. This approach would be consistent with the fact that regulation should only be applied where there is a clearly identified issue that can only be addressed through regulation, and any rules imposed are proportionate and non-discriminatory. For the reasons cited, this is not the case here. In fact, Online Services often provide higher levels of privacy and security protections for users (e.g., through E2E encryption) than is the case under traditional telecoms services.	protection consumers security users
	In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to decide their business models, as long as the privacy rights of the users are cared for and safeguarded.	users safeguard
	The provisions aimed at regulating the use of cookies do not serve users' interests as they make the experience burdensome for users, and overall services become less attractive and relevant for users. This is in conflict with the objective of providing users with meaningful information to enable them to protect privacy and confidentiality of their communications.	user protect
	Consumer related issues can be addressed under the body of consumer protection law that exists at EU level (e.g., the Unfair Commercial Practices Directive which is under review) and/or in specific instruments that form part of the EU telco regulatory framework (which is also under review).	consumer protection
Security and crime	From our perspective, we consider that including measures on security in the ePD is unnecessary. Measures aimed at ensuring sufficient security (whether in terms of security of networks, security of equipment) already exist in a number of other legislative instruments such as GDPR, the EU telecoms regulatory framework (for example the Framework Directive) and more recently the NIS Directive. There is therefore no regulatory gap that needs to be filled by including security measures in the ePD.	security

Type of frame	Arguments used by Facebook	Key words/word combinations
	Building in a "secret" opening for law enforcement to unlock encryption also creates an opening for other actors to exploit it. Criminals and oppressive regimes could use a "backdoor" to achieve their own ends.	exploit criminals oppressive
	E2E encryption guarantees the security and confidentially of the communication to its users. Building backdoors undermines this security for everyone.	security
Human rights frame	The Charter of Fundamental Rights states everyone has the right to respect for his or her private and family life, home and communications. Confidentiality of communication is guaranteed as a fundamental right under Art. 7 (Respect for private and family life) of the Charter and is further specified and applied through a number of national and European case law. This allows users to access and use the best possible technology/methods to secure and protect the confidentiality of their communications.	Charter of Fundamental Rights fundamental right
	In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to decide their business models, as long as the privacy rights of the users are cared for and safeguarded.	privacy rights of the users
Economic frame		
	Extending regulation out to Online Services risks undermining the existing protections in place and could stymie innovation in this area to the detriment of consumers who wish to have a high level of security for their communications.	innovation
	The differences in treatment in Member States regarding implementation of rules on unsolicited marketing has also led to a not insignificant degree of regulatory uncertainty for businesses, and contributed to a general lack of transparency for users.	businesses
	Instead, given appropriate safeguards, regulators should perhaps consider removing telecoms regulations where no longer necessary to protect consumers or competition.	competition
	At a practical level, the market has separately sought to improve user trust in security networks e.g., through encryption.	market
	From our perspective we consider that the ePD has led to increase in compliance costs for businesses which cannot readily be justified	costs businesses
	For example, while we do not have specific figures that we point to here, we understand that the costs to businesses in complying with the current rules on cookies - exacerbated by the often very different approaches taken by Member States in implementing these rules - are not insignificant.	costs businesses
	Although we do not have exact figures that we point to here, as a matter of principle, it is reasonable to assume that the costs of complying with multiple frameworks which, while in many areas overlap, in other areas adopt contradictory approaches, will be burdensome on business and ultimately risks leading to higher costs for users.	costs business
	Duplication of rules will be burdensome for business, and will lead to an increase in costs of compliance - that is unnecessary and disproportionate - and ultimately risks leading to higher costs for users.	business costs
	Regulation should not be enacted unless there is a clear and specific need for regulation, and even where such regulation is enacted it should be proportionate and non-discriminatory and applied in a technologically neutral manner so as not to stymie innovation in this area.	innovation
	Setting hard and fast standards around security could restrict users' ability to seek out and take advantage of such services that are E2E encrypted and force the market to develop in a specific manner, contrary to the principle that regulation should be technology neutral.	market
	Many companies and industries use encryption and it is not limited to one particular product or service.	companies industries
	Many information society services today are based on free-advertising-funded business models that keep the services free of charge for the user by allowing advertisers to show their advertisements to them.	business

Type of frame	Arguments used by Facebook	Key words/word combinations
	Regulation should not unduly interfere with or stymie entities' freedom to choose and develop innovative business models where there is clear consumer demand for these models.	innovative business
	This would be contrary to the fundamental principle that regulation should only be enacted where it is necessary to address a clear issue in the market, and that any regulation should be proportionate and technologically neutral so as to not to favour certain business models / technology over others.	market business
	In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to decide their business models, as long as the privacy rights of the users are cared for and safeguarded.	costs businesses
	Also, this approach will result in redundant double regulation, that further restricts companies' opportunities to use such data and stifle innovation in Europe, which already faces heavy burdens by the GDPR.	companies innovation

Table 17:

In-depth analysis of frame choice by Google (Commission)

Type of frame	Arguments used by Google Inc.	Key words/word combinations
Public frame		
Consumer protection	Legislators should carefully consider the various use cases, currently not covered by these provisions, which exist to protect the technical systems and hence the user; provide the service itself; or add value the user desires.	protect user
	As we noted above, the e-Privacy Directive is only one of the legislative instruments that was put in place to provide protection of personal data as well as to increase users trust in such protection.	user protection
	Google provides both tools and assistance to its users to help them stay safe and secure online (see for example myaccount.google.com). This includes advice on passwords and login methods, device authentication and others.	users safe secure
Crime and security frame	The GDPRs security and personal data breach notification obligations are built on the ePDs rules, turning these into a general obligation for all data controllers - both the Commissions impact assessment as well as the Communication accompanying the release of the GDPR make this clear.	data breach
Human rights frame	The right to privacy and confidentiality are important fundamental rights. The EU Regulatory Framework for Electronic Communications (e-Privacy Directive or ePD) is one, but not the only legislative instrument that was put in place to ensure the implementation of these rights by EU Member States.	fundamental rights
	Regarding the confidentiality of communications, it is important to find a workable and practically implementable solution to achieve the fundamental objective of this right, namely to protect the privacy of the communications from other individuals. This right should also complement, not duplicate or overlap with data protection regulation.	confidentiality of communications right
	The stated objective of the data protection reform was to benefit individuals by strengthening their data protection rights and their trust in the digital environment. (COM (2012) 9 final). The Commission declared this goal fulfilled, underlining that the data protection reform will strengthen the right to data protection (...) and allow them to have trust when they give their personal data. The new rules address these	data protection rights/ right to data protection

Type of frame	Arguments used by Google Inc.	Key words/word combinations
	concerns by strengthening the existing rights of empowering individuals with more control over their personal data. (See Press Statement of 15 December 2015). The GDPR thus fulfills this objective of raising users trust.	
	As noted above, the General Data Protection Regulation was clearly adopted with the digital and online environment in mind, with the aim to strengthen data protection rights and user trust in the digital environment and to stimulate development of the digital economy across the EUs Single Market and beyond, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe (see COM (2012) 9 final among others).	data protection rights
Economic frame		
	As the Time.lex/Spark (SMART 2013/0071) study demonstrated, its implementation varies significantly among Member States, creating challenges for businesses trying to participate in the Digital Single Market.	business market
	Years after the Directives adoption, there is still intense debate, both at European and national level, amongst authorities, academics and businesses about the interpretation of its rules, in particular of Article 5 on the confidentiality of communications.	businesses
	The implementation of the e-Privacy Directive has proven challenging and resource intensive to many in industry.	industry
	On the other hand, as the Time.lex/Spark (SMART 2013/0071) study assessing the e-Privacy Directive points out, whether the objective of, for example, the cookie provision have been reached is ambiguous, casting some doubts over the effectiveness of the resources invested in this by businesses.	business
	As noted above, the General Data Protection Regulation was clearly adopted with the digital and online environment in mind, with the aim to strengthen data protection rights and user trust in the digital environment and to stimulate development of the digital economy across the EUs Single Market and beyond, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe (see COM (2012) 9 final among others).	economy market
	As its rules overlap with the privacy provisions of the e-Privacy Directive, it provides the level playing field advocated for by many.	level playing field
	However, it is important that any legislation remains technology neutral and does not mandate any particular means to achieve such security, thereby allowing businesses to innovate and provide state of the art solutions to their users.	businesses innovate
	The Commission describes the rules of the Telecoms Framework as technology neutral and aims at deregulation in the long term (ec.europa.eu/digital-singlemarket/en/telecoms-rules). Mandating new and specific technical solutions and business models, as the question above indicates, is an absolute contradiction with these principles. Google has always operated on the belief that more access to information generally means more choice, economic opportunity and freedom for people.	business economic
	Companies chose at which end of the spectrum to offer their services, they can offer luxury cars or target the mass-market. At Google, we designed our services for everyone to be able to use.	companies

Table 18:

In-depth analysis of frame choice by Microsoft (Commission)

Type of frame	Arguments by Microsoft	Key words/word pairs
Public frame		
Consumer protection frame	We likewise believe that communication providers should remain free to innovate, including by developing security and encryption options demanded by their customers.	security customers
Crime and security	The GDPR contains new and more detailed rules on data breach notifications, which are also applicable to the electronic communication sector. These will be supplemented by regulatory guidance.	data breach
	The Council JHA conclusions adopted on 9 June 2016 on improving criminal justice in cyberspace and e-evidence underscore the need for further progress.	criminal
	Encryption options, or specific security features, should not be mandated in law, in order to preserve flexibility for diversity, competition, and innovation in service provision.	security
	We also recognize the importance of law enforcements role in providing security and preventing crime, subject to appropriate safeguards and procedures	security crime
	A business could, for example, use identifiers to prevent fraud on the service or its customers, and would not be able to do so if required to provide services to consumers without these identifiers.	fraud
	Note also that the GDPR will address these concerns to some extent. For example, it requires privacy by default, and squarely prohibits (and sanctions) misuses of personal data.	misuse
Human rights	A proximity principle, whereby LEAs should prioritize approaching (local) enterprises in their own jurisdiction with demands for data, before seeking it from their (non-local) providers, should be enacted. E.g., a law firm, not its service providers, should be asked to deliver (possibly privileged) communications from a rogue employee, unless that would jeopardize the investigation or introduce unacceptable delay. This principle would respect fundamental rights, increase trust, and reduce cross-border obstacles.	fundamental rights
	We strongly support protections for the confidentiality of electronic communications. Data protection is a human right.	Human right
	It should be clear that any right to secure communications for users is in respect of Member State and Union laws that would otherwise deprive them of that right - and not a right for them to force startups, etc., to implement encryption features, which may not be appropriate.	right to secure communications
Economic frame		
	And given the scale of change, telecoms laws should be re-designed from a blank slate; they are now needed most only where there are societal needs that are unmet as a result of enduring market failures.	market
	A proximity principle, whereby LEAs should prioritize approaching (local) enterprises in their own jurisdiction with demands for data, before seeking it from their (non-local) providers, should be enacted.	enterprise
	In particular, we believe that greater harmonization over when and how law enforcement authorities can access communications would promote a stronger Single Market for data, in line with its free flow of data initiative.	market
	As the Commission examines this issue, it should also consider that ALCSs may operate under conditions of greater competition than traditional ECSs -consumers switch between messaging apps routinely, and much more frequently than mobile phone or landline providers.	competition
	Given this greater level of competition, market forces influence product development significantly (as people easily switch away from services they dont trust, either in terms of data protection or reliability), and in this	competition market innovation

Type of frame	Arguments by Microsoft	Key words/word pairs
	context it is not clear that additional regulatory regimes - which may inhibit innovation and decrease competition by increasing barriers to entry - are needed.	
	Legal protections boost trust and adoption of online services, delivering economic growth.	economic growth
	A Regulation would help to harmonize rules across the EU, ensuring that businesses can operate with only one set of rules and helping consumers to understand their rights across the Union.	businesses
	The Commission should carefully assess the benefits of a Regulation but should also consider the risks, including a Union-wide loss of competitiveness if the Regulation becomes a vehicle for over-regulation of application layer communications. It would be better for some States to implement anti-competitive application layer communication regulations individually rather than to introduce such rules at the EU level.	competitiveness competitive
	Microsoft strongly supports empowering consumers and businesses to make choices regarding their communications, including encryption.	businesses
	We likewise believe that communication providers should remain free to innovate, including by developing security and encryption options demanded by their customers.	innovate
	Encryption options, or specific security features, should not be mandated in law, in order to preserve flexibility for diversity, competition, and innovation in service provision.	competition innovation
	Features, like encryption, that people want should be driven by market forces, not legal requirements.	market
	While Microsofts own business model does not rely primarily on advertising, we believe that innovation and competition flourish best when companies can freely choose how to structure their business. Additional rules that dictate business models could undermine this process. In addition, ISS providers - like other businesses - should have the right to prevent access to non-subscription based services if consumers refuse to be identified. A business could, for example, use identifiers to prevent fraud on the service or its customers, and would not be able to do so if required to provide services to consumers without these identifiers	business innovation competition companies
	Digital communications are, and will continue to be, characterized by rapid innovation and competition. In contrast, regulatory mechanisms -- such as delegated acts - can be cumbersome and slow to keep updated. They can also struggle to adapt as technology continues to evolve.	innovation competition
	As they do so, policymakers should also bear in mind that firms have an important incentive to ensure that the user experience remains high quality and enjoyable to consumers.	firms
	The current system, which sets out a complex patchwork of opt-in and opt-out requirements that vary according to Member State, circumstance and type of communication channel used, is confusing both to businesses and consumers.	business
	Businesses and particularly SMEs seeking to transact across borders face compliance challenges. The Commission should propose a scheme that simplifies these rules by introducing a new opt-out requirement that applies across all types of direct communication universally, and that applies in the same way in all Member States. This scheme would help SMEs operate more effectively across borders and would help consumers better understand their rights.	businesses SMEs
	Consumers and businesses will not use services they do not trust, and communications confidentiality including vis-vis law enforcement is key to that trust.	businesses
	The expansion of traditional telecoms laws to the ALCSs sector would risk endangering the sectors recent success, and would also slow innovation. Ultimately, such a development would also be likely to harm competition, as it would raise regulatory barriers to entry.	innovation competition

Table 19:

In-depth analysis of frame choice by Mozilla (Commission)

Type of frame	Arguments by Mozilla	Key words/word combinations
Public frame		
Consumer protection frame	Rules of the road that provide a baseline level of protection of user privacy and the increasing amount of data that can be collected, shared, and stored via the internet of things are demonstrably useful.	protection user
	Thus we believe that companies like Mozilla must be able to build the best security for their users that they can provide, to ensure the continuation of trusted communications systems which are key to fostering trust in the internet economy.	security users
	Furthermore, mandating a particular business model, approach, or technical standard is generally not the best way to protect the privacy of users.	protect users
	We encourage all stakeholders to not only comply with, but go beyond, what may be required by law to provide secure and privacy friendly products and services to users.	secure users
	The current EU legal instrument regarding electronic privacy, the e-Privacy Directive, is in need of reform. It fails to provide effective privacy protections for users, and yet also imposes inefficient burdens on industry.	protection user
	While blocking third party cookies may seem at first glance to be a low hanging fruit to better protect user privacy and security online — see this Firefox add-on called Lightbeam, which demonstrates the amount of first and third party sites that can "follow" you online — there are a number of different ways a user can be tracked online; via third party cookies is only an implementation of one form (albeit a common one).	protect user secure
	Focus on the harm - tracking - and not the implementation, which will provide more thorough protection for the user and will stand the test of time	protection user
	We view one of the primary objectives of the Regulation to be catalysing more offerings of privacy protective technologies and services for users. We strongly support this objective	protection user
Crime and security frame	The EPD has been an important instrument to advance national legislation fostering the privacy, security, and confidentiality of communications.	security
	As we have made clear on several occasions, including the Apple vs. FBI dispute and the UKs Investigatory Powers Bill, it is not possible to weaken the security of our products for law enforcement to use against only the bad guys (http://ti.me/29eKutu & http://bit.ly/29tdkIW).Creating gaps in security impacts everybody, increasing the risk of malicious hacking and identity theft. We thus strongly caution against the expansion or reinforcement of Art15(1), which could prevent companies from providing some forms of encryption services (such as true end-to-end encryption).	security malicious hacking
	It is our belief that the current status quo of online advertising is unsustainable. From that perspective, we welcome this process as an opportunity for a broad community of stakeholders to come together and re-evaluate certain practices and their effects – from ad-fraud, to pervasive tracking, to loss of trust and control of users- and to move together towards a more sustainable economic ecosystem where user control, transparency, and choice coexist with economic business models.	fraud
	We thus are generally supportive of this proposal, as it aligns with our data collection processes. However, one area of clarification needed is the threshold for what deletion "after receipt" would require. It is technically possible for IP logs, for example, to be deleted immediately after receipt, but retaining these logs for some reasonable amount of time can also be useful for things	fraud

Type of frame	Arguments by Mozilla	Key words/word combinations
	like fraud detection and analysis. We would therefore strongly encourage that deletion should follow after a reasonable amount of time and not be required as soon as technically possible.	
	Mozilla is supportive of the deletion and anonymising obligations, but we invite clarity on what "after receipt" means in practice. Deletion should follow after a reasonable amount of time and not be required as soon as technically possible, to allow useful applications such as fraud detection.	fraud
	Security or product updates: This includes scanning, filtering, and ultimately processing both communication content and metadata for the detection and prevention of malware, phishing, and spam, other forms of abuse of networks, services and users in addition to software updates, that are a crucial measure to enhance security. This is providing that updates are discreetly packaged, do not weaken the user's privacy settings, and finally, that the user should have the ability to turn off security updates if they so choose.	security malware
	The obligation to disclose data to law enforcement authorities in any member state may conflict with company structures which establish the data controlling entity in a particular member state or trigger conflicts of law that impair criminal investigations and put businesses in difficult situations where they may have to comply with incompatible requirements from different jurisdictions.	criminal
	We encourage the inclusion of procedural safeguards that would ensure at a minimum that any law enforcement request to access users' data is limited to people implicated in the crime	crime
	As a preemptive measure, given the concerning trend in the EU and around the world where state actors corrode, undermine, or outright ban critical security measures, strong protections for end-to-end encryption should be included in the ePR.	security
	Another layer of protection is needed in Article 11, to prohibit state actors from compelling or coercing services within the scope of the ePR to break, backdoor, or otherwise weaken secure (namely end of end encrypted) communications.	secure
Human rights frame	Article 7 of the Charter of Fundamental Rights establishes the right of individuals to secure their communications. This right is further specified in member state law and European case law.	Charter of Fundamental Rights
	For electronic communications, employing anonymisation techniques are likewise important both for the user and for the service; the former because their right to privacy is a fundamental right, and for the service because it greatly reduces the risk associated with collecting and processing communications content and metadata.	fundamental right
	Audience measurement: for a more technology neutral approach, we suggest removing the "web" qualifier, to ensure that it can apply in various contexts and purposes outside of the narrow scope of web. As an added safeguard, the measurements should not adversely affect the fundamental rights of the user.	fundamental right
Economic frame		
	For technology companies hoping to do business across the EU, this provides compliance difficulty and risk.	companies business
	On 2nd prompt, weve experienced and witnessed significant problems in understanding and applying Art5(3) of the EPD. This has achieved neither user trust and greater privacy nor legal certainty for online businesses.	businesses
	As we have explained in questions 1A and 2A, some provisions of the EPD (and Article 5(3) in particular) have generated confusion on behalf of users and businesses which regrettably undermine the spirit of the EPD.	businesses
	Businesses and enforcement authorities - whether DPAs or NRAs - in practice, have different interpretations of the law.	businesses
	Furthermore, the data protection directive (95/46/EC) and the EPD also differ, making it difficult to understand which framework to follow (e.g. for	business

Type of frame	Arguments by Mozilla	Key words/word combinations
	data breach notification obligations), and whether a particular product or service would mean a business is an Information Society Service (ISS) or a data controller.	
	From the perspective of businesses, varied implementations in MS also resulted in various, at times conflicting interpretations of EPD that ultimately stood in the way of consistent enforcement and application of the rules.	businesses
	Furthermore, mandating a particular business model, approach, or technical standard is generally not the best way to protect the privacy of users.	business
	Ultimately, there is sufficient technical development and rapid change in the ecosystem such that additional regulation might limit, rather than foster, increased innovation around privacy and security positive tools.	innovation
	Additionally, top-down regulation often forces particular business models rather than experimentation & innovation.	business innovation
	The current EU legal instrument regarding electronic privacy, the e-Privacy Directive, is in need of reform. It fails to provide effective privacy protections for users, and yet also imposes inefficient burdens on industry.	industry
	It is our belief that the current status quo of online advertising is unsustainable. From that perspective, we welcome this process as an opportunity for a broad community of stakeholders to come together and re-evaluate certain practices and their effects – from ad-fraud, to pervasive tracking, to loss of trust and control of users- and to move together towards a more sustainable economic ecosystem where user control, transparency, and choice coexist with economic business models.	economic business
	We are concerned however that many companies may make use of the legitimate interest as a loophole to collect and process sensitive data without users' knowledge or control. We therefore would advise against its inclusion.	companies
	A frequent justification for Legitimate Interest is to allow for innovation and testing of new products and services. However, we do not believe that the potential risks associated with this broad legal grounds is worth the risk to the privacy of users.	innovation
	Compliance with DNT will be challenging, even if legally required, when companies do not know what is required to comply and do not have an agreed upon standard to use.	companies
	Users can browse in regular mode, which permits Web sites to place cookies, or in private browsing mode, which has our Tracking Protection technology built in. We invest in making sure that both options are desirable user experiences, and the user is free to choose which they go with – and can switch between them at will. We'd like to see more of this in the industry, and welcome the spirit of Article 10 of the draft Regulation which we believe is intended to encourage this.	industry
	Mozilla strongly supports regulatory incentives that would require companies to have processes in place to address lawful access requests by state actors. We note that establishing a process by which requests can be fielded can actually benefit companies as without strong, transparent procedures, the risks for greater access to user data may be increased, particularly as increasingly, online service providers are approached by law enforcement and intelligence services to provide access to user data.	companies
	The obligation to disclose data to law enforcement authorities in any member state may conflict with company structures which establish the data controlling entity in a particular member state or trigger conflicts of law that impair criminal investigations and put businesses in difficult situations where they may have to comply with incompatible requirements from different jurisdictions.	company businesses
	any law enforcement request to access users' data is limited to people implicated in the crime; that the data is proportionate and necessary for the	companies

Type of frame	Arguments by Mozilla	Key words/word combinations
	investigation in question; and finally, requests are based on a "reasoned" request backed by a court or independent authority. Authorities should also be obliged to notify users about such requests and companies should be also allowed to do so.	

Table 20:

In-depth analysis of frame choice by Nokia (Commission)

Type of frame	Arguments by Nokia	Key words/word combinations
Public frame		
Consumer protection frame	The regulatory focus of the network regulators is primarily that of securing adequate market access and ensuring consumer protection against unfair business practices outside of data protection.	consumer protection
Crime and security frame	Security provisions in European legislation should be consistent, complimentary and not duplicate or overlap with each other. Different and even conflicting security requirements per Member State also do not seem appropriate and do not facilitate free movement of electronic communications equipment and services.	security
	Furthermore, business and science are able to provide suitable and userfriendly solutions and in practice do so already [e.g. encryption apps], and should be protected against blanket suspicions as well as discriminations and allegations that these kinds of protective measures are improper and only further crime an unlawful act.	crime unlawful
Human rights frame	The right to respect private and family life, home and communications is ensured by the EUs Charter of Fundamental Rights and the ICCPR Article 17. The protection granted by the Charter and the ICCPR is universal and should be also ensured in the law enforcement context. The existence and scope of this fundamental right should be clarified and defended against improper intrusion by the EU Member states.	right to respect private and family life, home and communications Charter of Fundamental Rights fundamental right
	In conclusion, the fundamental right should be strengthened, but no further technological regulation is warranted.	fundamental right
Economic frame		
	The objective of the ePD is not to govern the market admissibility of electronic communications equipment and services.	market
	In the era of convergence and technological neutrality, it is not appropriate to impose different data protection obligations on providers of functionally equivalent services depending on whether they are OTT and other information society providers or traditional telecommunications companies. It would not however be appropriate nor desirable to limit the processing of traffic and location data to consent only. This may impede innovation and hinder future legitimate uses of these data.	innovation
	There continues to be a lack of harmonization across the EU that creates additional cost to comply with the ePD across the EU that do not seem to be proportionate to the objective being pursued.	cost
	We support a continuation of an instrument covering privacy and data protection issues in the electronic communications sector provided it does not impose different data protection obligations on providers of functionally equivalent services depending on whether they are OTT and other information society providers or traditional telecommunications companies. It would not be desirable nor appropriate to limit the processing of traffic and location data to	companies innovation

Type of frame	Arguments by Nokia	Key words/word combinations
	consent only. This may impede innovation and hinder future legitimate uses of these data.	
	Furthermore, business and science are able to provide suitable and userfriendly solutions and in practice do so already [e.g. encryption apps], and should be protected against blanket suspicions as well as discriminations and allegations that these kinds of protective measures are improper and only further crime an unlawful act.	business
	Companies should remain free to select, adjust and enhance the security measures they believe appropriate to the risks presented by processing activities.	companies
	We believe that industry specific code of conduct and certifications as provided for under the GDPR help to foster a consistent level of information among the user and consistently applied transparent communication of privacy requirements.	industry
	The regulatory focus of the network regulators is primarily that of securing adequate market access and ensuring consumer protection against unfair business practices outside of data protection.	market business
	We believe that both the GDPR as well as the ePD in its current version prevent the establishment of new business models and data monetization.	business monetization
	In order to support a market environment favorable for new business models focusing on big data and IoT it would be important to allow companies to apply broader processing grounds like permitted under the GDPR (eg legitimate interest).	market business companies

Table 21:

In-depth analysis of frame choice by Orange (Commission)

Type of frame	Arguments by Orange	Key words/word combinations
Public frame		
Consumer protection frame	Today, communication services have evolved and include a broad set of services that consumers consider substitutable, even if they are technologically and regulatory different and do not grant consumers the same level of protection.	consumers protection
	Today European citizens cannot rely on European rules to consistently protect their privacy.	citizens protect
	Consumers should receive the same level of protection regardless of technology or type of service.	consumers protection
	Waiting for the opportunity to include the confidentiality of communications principle into the GDPR, a technology neutral wording independent of the main business of the undertaking providing the service should be adopted and included into a horizontal consumer protection tool.	consumer protection
	The application of privacy rules in the GDPR and the possibility to engage in ex-post antitrust actions provide a comprehensive framework to monitor the commercial exploitation of users' data by all kind of providers of digital services. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users.	safeguard individual users
	We recommend adopting a technological neutral language to express this principle encompassing all industries and, waiting for the next revision of the GDPR, to include it into a horizontal consumer protection text.	consumer protection

Type of frame	Arguments by Orange	Key words/word combinations
	Orange considers that the GDPR is the appropriate tool to protect individuals' personal data carried by M2M communications services	protect individuals
	ECD is personal data: the GDPR applies by default, and the ePR will be lex specialis, meaning it will prevail when the two regulations establish rules for the same situation. However, Recital 5 of the ePR explains that the ePR should not lower the level of protection enjoyed by natural persons under the GDPR.	protection persons
	The ePR should be driven by the objective to provide identical privacy protection to consumers, whichever service provider they choose, and identical opportunities to all providers of digital services to develop data based innovations.	protection consumers
	Furthermore, the distinction made by the text between "first-party" cookies and third-party cookies does not bring more security to end users' privacy: it is the purpose of the cookie that matters and is likely to impact privacy.	security user
	Finally, the draft ePR proposes to protect end-users from unsolicited direct marketing communications, the definition of which is unclear and may include behavioural on-line advertising.	protect users
	However, concerning machines transmitting personal data, the GDPR already rightly ensures individuals' protection, in a horizontal and technologically neutral way.	Individuals protection
Crime and security frame	The collection of a large amount of users' data by OTT is a new source of market power that is currently being taken into account by antitrust practitioners and authorities alike. Unlike telcos, OTT are global players that are allowed to commercially exploit the traffic data and the location data they collect.	exploit
	The application of privacy rules in the GDPR and the possibility to engage in ex-post antitrust actions provide a comprehensive framework to monitor the commercial exploitation of users' data by all kind of providers of digital services. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users. As a result, there is no need to apply different tools than GDPR and antitrust law.	exploitation abuse
	The spreading of encrypted data flows has consequence on several obligations that apply to network operators. When traffic is encrypted and routed through browser proxies by internet players, operators cannot perform: malware detection and anti-virus protections, cooperation with national law enforcement authorities and national intelligence services to ensure identification, localization and tapping of communications, fight against child pornography and content filtering (parental control).	malware
	As already recommended by the Art. 29 WP, first party analytics cookies should not require prior consent of website visitors as they are not likely to create a privacy risk (see ART 29 WP Opinion 4/2012). Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users device should not require prior consent.	fraud
Human rights frame	The confidentiality of communications is a well-established right that should be included into a horizontal instrument as the GDPR. Such a sound approach would have a balanced impact on the compliancy costs for both telecom operators and internet pure players.	confidentiality of communications right
	Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users fatigue without providing any enhanced level of protection to the right of confidentiality of the individual.	right of confidentiality
	Confidentiality of communications has always been a fundamental principle applied by the telecommunications industry. Orange supports the extension of this fundamental right to any form of interpersonal	fundamental right

Type of frame	Arguments by Orange	Key words/word combinations
	communications as proposed in the ePR draft. However, concerning machines transmitting personal data, the GDPR already rightly ensures individuals' protection, in a horizontal and technologically neutral way. Machine to Machine communications that do not carry personal data, as in the field of automated supply chains for example, do not justify extensions of individuals' fundamental rights or legitimate interests of legal persons; such communications are rightly covered by the contractual agreements between entities.	
	Unlike in the proposed ePR, "legitimate interest" and "performance of a contract" are legal grounds for processing personal data in the GDPR. Under this legal basis, the data controller is in charge of assessing the balance between its legitimate interest and the fundamental rights and freedoms of the data subject.	fundamental rights
Economic frame		
	Waiting for the opportunity to include the confidentiality of communications principle into the GDPR, a technology neutral wording independent of the main business of the undertaking providing the service should be adopted and included into a horizontal consumer protection tool.	business
	This situation is particularly imbalanced for traffic and location data because ePD rules do not permit the economical exploitation of big data analytics on the same regulatory ground than for OTT. The collection of a large amount of users' data by OTT is a new source of market power that is currently being taken into account by antitrust practitioners and authorities alike.	market
	The ePD compliancy costs are significant but what is more burdensome is the specific rule for traffic data and location data that does not permit the economical exploitation of big data analytics on the same regulatory ground as internet pure players.	costs economical
	The confidentiality of communications is a well-established right that should be included into a horizontal instrument as the GDPR. Such a sound approach would have a balanced impact on the compliancy costs for both telecom operators and internet pure players.	costs
	A future proof regulation needs a common approach to all industries competing in the same market.	industries competing market
	We recommend adopting a technological neutral language to express this principle encompassing all industries and, waiting for the next revision of the GDPR, to include it into a horizontal consumer protection text.	industries
	It is for commercial companies and market place to develop their business models.	commercial companies market business
	Less intrusive types of cookies (for instance cookies used for website statistics) should be exempted and regulation should be reserved for websites using cookies that pose genuine risks of privacy intrusion. The benefits will be fewer burdens to businesses, more alertness to privacy issues among users, and the possibility of more effective and targeted enforcement.	businesses
	There is no need for a specific ePD instrument. Key factors to facilitate users' ability to consent without disrupting the internet experience include inter alia manufacturers of terminal equipment such as operating systems and browsers to place on the market products with privacy by default settings as well as to mandate European Standards Organisations to produce standards and the support of self and co-regulation.	market
	Following the "lex specialis" rule, the ePR will prime over the GDPR on those issues and impact the whole digital economy as it goes beyond protecting confidentiality of communications and considerably limits the processing of data.	economy

Type of frame	Arguments by Orange	Key words/word combinations
	The ePR should be driven by the objective to provide identical privacy protection to consumers, whichever service provider they choose, and identical opportunities to all providers of digital services to develop data based innovations.	innovations
	The new ePR does not avoid over-notification from websites, as those whose business models are based on audience will need consent banners to inform individuals that they can change their settings to access their service.	business
	Moreover, by giving a pivotal role to software companies such as providers of Internet browsers, several of which also carry Internet services and advertising activities, the new ePR could severely harm competition.	companies competition
	Generally speaking, the current wording gives a significant strategic advantage to vertical, integrated, identification-based ecosystems and does not seem to take into account business models based on advertising and targeting, that are increasingly essential to the very functioning of the Internet (e.g. recommendation tools).	business
	The collection of a large amount of users' data by OTT is a new source of market power that is currently being taken into account by antitrust practitioners and authorities alike. Unlike telcos, OTT are global players that are allowed to commercially exploit the traffic data and the location data they collect. However, there is no technicall or legal reason to consider that traffic and location data collected from telcos and OTT should be treated differently by regulators and competition authorities	market commercially

Table 22:

In-depth analysis of frame choice by Telefónica (Commission)

Type of frame	Arguments used by Telefónica	Key words/word combinations
Public frame		
Consumer protection frame	Currently, European citizens cannot rely on European regulation to consistently protect their personal data and privacy, as different sets of rules are applied to functionally equivalent services, from the user point of view, depending only on the classification of the service provider (according to an old fashioned ECS definition).	citizens protect
	Europe needs to address the current patchwork of regulation, which compromises the effective and consistent protection of consumers across the digital value chain.	protection consumers
	Additionnally, in both cases, transposition of general data protection rules and transposition of ePrivacy Directive has been very different in Member States leading to a lack of harmonisation that has also been very negative for providers and for consumers.	protection consumers
	Maintaining two different set of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection.	consumer protection
	A specific sector regulation will only increase confusion for users as they do not know by which rule they are protected.	users protected
	Here it is important to recall the Digital Single Market Strategy, which explicitly mentions that GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that offers their services on the European market.	protect individuals
	Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users fatigue without providing	protection individual

Type of frame	Arguments used by Telefónica	Key words/word combinations
	any enhanced level of protection to the right of confidentiality of the individual.	
	Telefnica believes that there is no need for a new ePrivcay instrument. Selfregulation and European standards on Do Not Track solutions should be developed as they will help to increase the level of privacy protection without disrupting consumers Internet experience.	protection consumers
	An overall standard at EU level is necessary to ensure that consumers in Europe are not protected in a different way depending on their location.	consumers protected
Crime and security	In 2009, ePrivacy Directive introduced for the first time some obligations on security. The GDPR has extended the scope of the new rules on security to all sectors with the primary aim to have a comprehensive, technologically neutral set of rules on security of processing and data breach notifications.	security data breach
	Therefore, it does not make sense to maintain dissimilar security requirements under the ePrivacy Directive, the GDPR and the Framework Direcitve, as this creates an undesired and overly complex situation for telecom providers, stakeholders, authorities and consumers. Maintaining specific rules embedded in a sectoralspecific ePrivacy legal instrument together with the new GDPR provisions on security of processing is not sustainable.	security
	When traffic is encrypted and routed through browser proxies by internet players, operators cannot develop security measures like malware detection and anti-virus protections, or cooperate with national law enforcement authorities to ensure interception of communications, fight against child pornography and content filtering (parental control). Thus, legislation should focus on providing a coherent solution to tackle all these challenges.	security malware
	Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymized so that it is impossible to identify the users device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users fatigue without providing any enhanced level of protection to the right of confidentiality of the individual.	fraud
Human rights	The objectives of ensuring confidentiality of communications might be very relevant, but the point is that the costs of compliance have only be put on a certain number of actors (e-communications service providers) while other actors not covered by EPD should also ensure the confidentiality of communications and the fundamental right to privacy.	fundamental right to privacy
	There is no need to define further security measures and obligations in order to ensure the right of individuals to secure their communications.	right to secure their communications.
	Consequently there is no need for complementing the right of confidentiality of communications with additional legal provisions on encryption regarding the communication between individuals, especially as they cannot keep pace of technology developments.	right of confidentiality of communications
	This is the data as a currency model where the user accept to participate with different extension and terms in the advertising ecosystem in exchange of a free service. This model must be based upon the assumption of informed consent where the transaction is under the reasonable expectations of the consumer. If that is the case, the regulation must not prevent enterprises to freely decide its business model, always based on the respect to fundamental rights and freedoms of individuals.	fundamental rights
	Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users fatigue without providing	right of confidentiality

Type of frame	Arguments used by Telefónica	Key words/word combinations
	any enhanced level of protection to the right of confidentiality of the individual.	
Economic frames		
	European citizens cannot rely on European regulation to consistently protect their personal data and privacy, as different sets of rules are applied to functionally equivalent services, from the user point of view, depending only on the classification of the service provider (according to an old fashioned ECS definition). This weakens confidence in the European digital ecosystem and prevents consumers from fully benefitting from the potential of the single market.	market
	Telecommunication service providers are highly regulated as regards the privacy and security, while Over the Top (OTT) players are not regulated the same way for the provision of functionally equivalent services. The problem is not only for consumers but also for the competitivity of the European industry. The uneven application of privacy and data protection rules for equivalent services destroys the ability for these players to compete on equal footing in a single market.	competitivity industry compete market
	It is important that consumers are able to enjoy consistent privacy standards and experiences, irrespective of the technologies, infrastructure, business models, who provides a service or where a company may be located.	business company
	As long as the ePrivacy Directive coexists with the new GDPR, there will be no level playing field, consumers will not experience comparable digital privacy online and operators will continue to face this dual compliance regime and their competitive position will be compromised.	level playing field competitive
	Maintaining two different sets of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection.	market
	Here it is important to recall the Digital Single Market Strategy, which explicitly mentions that GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that offers their services on the European market.	companies market
	As an example, the new GDPR will imply a more consistent and horizontal approach leading to a level playing field and thus contributing to users trust and awareness.	level playing field
	The implementation of the ePrivacy Directive has implied additional direct costs for the regulated businesses, but the most important costs are no doubt the opportunity costs, as traditional telecommunications operators have been prevented from offering new services that have been launched by other actors not subject to the ePrivacy	costs businesses
	These services are very demanded and widely adopted by consumers, but telecom operators have not been able to respond to this demand due to regulatory burdens. This imposes a significant loss of competitiveness on the concerned organizations and a relevant impact on the innovation and on the time to market for new services. Besides, investments that would have been made in the absence of regulation are delayed of finally discarded.	competitiveness innovation market investments
	The objectives of ensuring confidentiality of communications might be very relevant, but the point is that the costs of compliance have only be put on a certain number of actors (e-communications service providers) while other actors not covered by EPD should also ensure the confidentiality of communications and the fundamental right to privacy. This has put European telecommunications service providers at a competitive disadvantage vis à vis other players offering the same services.	costs competitive
	The recent CERRE study on Consumer Privacy in Network Industries states that a future proof regulation requires a common approach to all industries and that sector-specific privacy regulations are inadequate in a dynamic environment and should be withdrawn.	industries

Type of frame	Arguments used by Telefónica	Key words/word combinations
	The long term priority of the ePrivacy review should enable European businesses to compete at the global level in Big Data, Cloud, IoT.	businesses compete
	Therefore, once GDPR adopted, the review should focus in removing overlapping provisions with GDPR, transferring consumer protection rules (not strictly related to privacy) into more appropriate tools and clarifying the scope of the remaining provisions, if any, in order to achieve a true level playing field between traditional telcos and Internet based service providers in the interest of businesses and end users (as stated in the DSM Strategy).	level playing field businesses
	It is in the interest of industry to offer consumer-friendly solutions as a central differentiating factor between companies (race to the top). If this is the case, the regulation must not prevent enterprises to freely decide its business model, always based on the respect to fundamental rights and freedoms of individuals.	industry companies enterprises business
	Already the GDPR recognises the importance of self-regulation and encourages the drafting of Codes of Conduct by industry. Therefore, another sector specific ePrivacy incorporating these points would be redundant. Europe should fully take stock of the GDPR, which creates a level playing field for all companies offering services in the EU.	industry level playing field companies
	Therefore, the most important thing is to avoid this duplicity and allow the GDPR to create the necessary level playing field between all players irrespective of sector or geographic location.	level playing field

Table 23:

In-depth analysis of frame choice by Vodafone (Commission)

Type of frame	Arguments by Vodafone	Key words/word combinations
Public frame		
Consumer protection frame	The e-Privacy Directive (EPD) has had limited success protecting the confidentiality of communications across the EU for the key reason that, by being too sector & technology specific, it has not kept up with new forms of communications over the internet such as voice over IP or instant messaging. As a result consumers are subject to different standards of protection for what are in effect the same communication services.	consumers protection
	Currently, consumers have different levels of protection for functionally equivalent services and service providers will face regulatory arbitrage. Mandating specific security tools as legal rights risks prematurely dating any new legislation, thereby failing adequately to secure the lasting protection for the citizen's right to privacy at the heart of the proposed measures.	consumers protection secure protection citizen
	We believe that encryption plays a critical role in helping our customers keep their data safe and secure as well as protecting Vodafone's own networks and systems from unauthorised and malign access. There would only be a requirement for a legal right of individuals to secure their communications through use of encryption if the citizen's existing legal right to confidentiality of communications under Article 5 of the EPD could be at risk of being undermined in some way over time - which, in our view, would be an very worrying development were it to transpire.	customers safe secure individuals secure
	Should the Review decide to keep these provisions, we would suggest moving them to the new legislation coming out of the Telecoms	consumer protection

Type of frame	Arguments by Vodafone	Key words/word combinations
	Framework on the basis that they relate to issues of consumer protection, not confidentiality of communications.	
	A consumer protection authority has a different skill set and view of the world to that of a data protection authority or telecoms regulator; the risks and sanctions are different too. Therefore provisions which are more about consumer protection than confidentiality should be addressed in the relevant legislation.	consumer protection
Crime and security	As addressed in our answers to Q2A, there is regulatory overlap between EPD and GDPR rules on data breach notification (and security standards more widely); these should be removed for a simpler legal framework.	data breach
	The security obligations of the e-Privacy Directive are at least partially consistent with the other security obligations listed, but they are not coherent. Providers of electronic communications services are subject to numerous security duties to keep electronic communications secure and introducing more security laws is not the answer. Telecoms companies are already subject to overlapping security obligations by virtue of the EPD, Framework Directive (Art.13a) and GDPR. Meanwhile the NIS Directive may apply to over the top communication service providers in some instances. These sets of overlapping (and not always coherent) legal obligations are confusing, complicated and do not result in better security. Good security is achieved by investing in security engineers, not lawyers.	security
	Any legal obligations should only be kept where it can be demonstrated that it is necessary. The obligation should not mandate any specific security technology. It should recognize the evolving nature of security risks and related mitigations (state of the art), and it should be risk based. It should also be remembered that good security is at the heart of a communications service providers business; we would do it regardless of whether there are security laws.	security
	First, with regard to security measures, we would incur these costs even in absence of the EPD because we have to. Any credible organisation that seeks to retain and grow its customer base is already spending money on putting in place appropriate security measures, regardless of what the law says.	security
	We believe that encryption plays a critical role in helping our customers keep their data safe and secure as well as protecting Vodafone's own networks and systems from unauthorised and malign access.	unauthorized malign
	It is also necessary to maintain the security of our network & protect against malware (processing for this purpose needs to be legally recognised) & improve our services both technically (e.g. identifying areas with bad connectivity) & commercially (e.g. monitoring trends in service use to develop better pricing models).	malware
	It is crucial that business and consumers should only have to report to one regulatory authority in the event of a breach.	breach
Human rights	Respecting our customers right to privacy is one of our highest priorities. We believe that encryption plays a critical role in helping our customers keep their data safe and secure as well as protecting Vodafone's own networks and systems from unauthorised and malign access.	right to privacy
	There would only be a requirement for a legal right of individuals to secure their communications through use of encryption if the citizen's existing legal right to confidentiality of communications under Article 5 of the EPD could be at risk of being undermined in some way over time - which, in our view, would be an very worrying development were it to transpire.	right to secure communications
	Mandating specific security tools as legal rights risks prematurely dating any new legislation, thereby failing adequately to secure the lasting protection for the citizen's right to privacy at the heart of the proposed measures.	right to privacy
Economic frame		

Type of frame	Arguments by Vodafone	Key words/word combinations
	As a service provider based in countries across the EU, sources of confusion relate to working out which competent authority to answer to because (a) the type of regulator differs by Member State and (b) in some Member States, more than one regulator has jurisdiction over the same matter. This is confusing for consumers (who do not know who to complain to) as well as for business.	business
	Rules on unsolicited marketing communications remain relevant but would better belong in a horizontal legislative instrument given that they apply to all market players.	market
	It should also be remembered that good security is at the heart of a communications service providers business; we would do it regardless of whether there are security laws.	business
	In order for businesses to scale-up in the Digital Single Market, it is crucial that rules are harmonised across the EU.	businesses market
	EPD has not stood the test of time: While the underlying policy drivers have not changed, technology has advanced and new forms of communications have developed. Currently, consumers have different levels of protection for functionally equivalent services and service providers will face regulatory arbitrage. This has already been recognised in the DSM strategy, where it was stated that rules must be simpler, future proof and must also ensure a level playing field between traditional telecoms companies and new internet players where they compete in the same market and that this must be addressed across the Telecoms Framework, EPD, audio visual media and services regulation and platforms.	level playing field companies compete market
	First, with regard to security measures, we would incur these costs even in absence of the EPD because we have to. Any credible organisation that seeks to retain and grow its customer base is already spending money on putting in place appropriate security measures, regardless of what the law says.	costs grow money
	Second, in some areas of the EPD, for example obtaining consent to use cookies or send unsolicited communications, operational costs incurred in complying with the EPD in practice are very much intertwined with those incurred complying with data protection law. That said a significant legal cost is incurred by our business Europe wide interpreting the different implementations of the EPD country by country and answering to the different regulators. Further legal cost is anticipated working through the regulatory overlaps brought about by the GDPR which is why a simpler regime would be welcome.	costs business
	Finally, the narrow legal grounds for processing traffic data in EPD provide additional burdens in terms of customer relationship management and analytics compared to other industries.	industries
	We support the protection of confidentiality of communications; it is fundamental to the building of user trust in digital networks and it is fundamental to our business. It underpins any Digital Single Market.	business market
	The EPD is expensive because it is complex to comply with.	expensive
	This results in an oversight of confidentiality protection for a large swathe of communication services (in addition to distorting competition in the market).	competition market
	In order for businesses to scale-up in the Digital Single Market, it is crucial that rules are harmonised across the EU.	businesses market
	Under the EPD it was up to each Member State to ensure that an appropriate national authority was competent to investigate and enforce the national laws. In some countries, the data protection authority is the competent authority, in others it is the telecom regulatory authority or some other authority; in some countries it can be more than one. This leads to confusion all round; for business, consumers and the regulatory authorities themselves.	business
	It is crucial that business and consumers should only have to report to one regulatory authority in the event of a breach.	business

Type of frame	Arguments by Vodafone	Key words/word combinations
	In our view security obligations, confidentiality of communications and obligations on traffic and location data should apply equally to all forms of service provider whether a traditional telecoms operator or an over the top service provider. We do not think it would be appropriate to extend the rules into a companys VPN, or other private or closed network, or to WIFI.	companys

Appendix B: In-depth analysis of interest group frame choice (Parliament)

The tables contain direct quotes from the interest groups presentation notes for the hearing in the European Parliament. These were subject to the in-depth analysis of frame choice vis-à-vis the Parliament.

Cause groups

Table 24

In-depth analysis of frame choice by Access Now (Parliament)

Type of frame	Arguments by Access Now	Key words/word combinations
Public frame		
Consumer protection frame	The primary public interest is the legal and technical protection of people and not cementing semi- or fully unlawful business practices.	protection people
	Reaching consistency with the GDPR, if it meets the above detailed requirements, will lead to a level playing field. The expression "level playing field" is so overused, however, that it is very difficult to attribute any meaning to it. In ePrivacy jargon, the traditional meaning is to level the field between telecoms and Over-The-Top service providers. To change that discourse, I'd like to offer a new approach to what we should mean by "levelling the playing field" in this context. The playing field must be levelled to protect users because the field is uneven: telcos and online service providers are both in a dominant position compared to the users due to the lack of information and transparency. A level playing field for users would address this information asymmetry.	protect users
	As the agenda of this hearing says, the proposal expands its scope to cover the new forms of electronic communications and ensure the same level of protection of individuals regardless of the communication service used. The effort to fulfill that proposal is not yet fully delivered.	protection individual
Crime and security frame	-	
Human rights frame	My main point about this topic is that in order to meet the requirements of the EU Charter of Fundamental Rights and achieve legal consistency with the General Data Protection Regulation we must indeed level the playing field. Level the playing field for users in the form of racing to the top, not to the bottom.	Charter of Fundamental Rights
	The rules of the ePrivacy Regulation should not only uphold the level of protection afforded by the GDPR but should exceed it to protect the	fundamental right to privacy

Type of frame	Arguments by Access Now	Key words/word combinations
	fundamental right to privacy, as also stressed by the Article 29 Working Party.	
	To respect the fundamental rights of privacy and data protection is not a favor, it is a legal obligation.	fundamental rights of privacy and data protection
Economic frame		
	Processing and monetising personal data should come at a price.	monetizing
	The primary public interest is the legal and technical protection of people and not cementing semi- or fully unlawful business practices.	business
	The proposed ePrivacy Regulation must therefore increase the level of protection for the confidentiality of communications and defend against tracking in order to reach a higher level of protection than the GDPR. That would create a level playing field for all actors.	level playing field
	The European Union has taken the first steps to create the Digital Single Market which can only be successful if the trust of European citizens is regained.	market

Firms

Table 25:

In-depth analysis of frame choice by Facebook (Parliament)

Type of frame	Arguments by Facebook	Key words/word combinations
Public frame		
Consumer protection frame	Messaging is now an area of intense innovation and development, and I wanted to talk to you today about the services we and others are working on to help people express themselves and stay connected with their loved ones in a safe and secure way.	people safe secure
	Finally, I want to tell you about our work — and the work of others in the industry — to make people's online experience safer.	people safer
Crime and security frame	Along with other email and messaging services, we process communications data to help find malware and other things that could harm people.	malware
	For example, child exploitation content is shared with saddening frequency online, but we and others have developed tools to identify these types of images.	exploitation
	Bad actors won't consent. Think about the spam, malware, and child exploitation cases I mentioned above. If you were a bad actor, why would you agree to such processing? I fear requiring such tools to be opt-in effectively gives the bad actor an *opt-out*.	malware exploitation
Human rights frame	-	
Economic frame		
	Messaging is now an area of intense innovation and development, and I wanted to talk to you today about the services we and others are working on to help people express themselves and stay connected with their loved ones in a safe and secure way.	innovation
	Finally, I want to tell you about our work — and the work of others in the industry — to make people's online experience safer.	industry
	But the proposed Regulation, as currently drafted, threatens to hold back the artificial intelligence and big data innovation I just described.	innovation

Type of frame	Arguments by Facebook	Key words/word combinations
	We believe the Parliament has an opportunity to reform the proposal so that it does more to encourage growth in these services while also protecting privacy.	growth

Table 26:

In-depth analysis of frame choice by Schibsted Sverige (Parliament)

Type of frame	Arguments by Schibsted Sverige	Key words/word combinations
Public frame		
Consumer protection frame	-	
Crime and security frame	-	
Human rights frame	-	
Economic frame		
	Users prefer advertising over payment for content. This is reflected in our revenues.	payment revenue
	We compete with the global players to ensure independent, pluralistic, and accessible European press	compete
	Need for flexible rules to promote user empowerment and transparency; to secure a level playing field; and to allow for innovation	level playing field innovation

Table 27:

In-depth analysis of frame choice by Symantec (Parliament)

Type of frame	Arguments by Symantec	Key words/word combinations
Public frame		
Consumer protection frame	-	
Crime and security frame	If ePrivacy is focused on protecting interactions= confidentiality it has a role to play in the security architecture	security
	Less protection because fewer organisations can collect security relevant info (security providers and CERTs are not included)	security
	New ePrivacy Regulation (...) weakens security	security
	Focus needs to be on capabilities to be achieved to deliver security as opposed to a generic obligation to deliver a "confidential" environment	security
Human rights frame	-	
Economic frame		
	The more restrictive the framework is for metadata the less likely is for EU businesses to grow in new/big data sectors	businesses grow
	Less growth = less jobs, less innovation, less competitiveness	growth

Appendix C: Analysis of frame usage for each individual interest group in their group alphabetical order (Commission)

Cause groups

Access Now

Access Now defends user's rights (Access Now, 2020). It correspondingly also used multiple human rights and consumer protection arguments. The organization welcomes and supports the Commission proposal for revising the ePrivacy Directive. It argues that "[t]he GDPR does not specifically cover the right to private life enshrined in Article 7 of the EU Charter of Fundamental Rights, and specific protections will have to be articulated in the future revised e-Privacy" (Access Now, 2016a). By including key words such as 'Charter of Fundamental Rights' and 'right to privacy' the use of human rights frame is signalled. To strengthen its argumentation, Access Now draws attention to a 2015 EuroBarometer study which supports the organization's argument that there is "the need for robust and clear safeguards for the protection of users' data and confidentiality, which will lead to increased trust in services" (Access Now, 2016a). The organization thus emphasizes aspects related to consumer protection which indicates the employment of a consumer protection frame by using the signaling word combinations of 'protecting' and 'user'. With respect to enhancing the overall security, it points out that "[t]he referenced legal instruments establish security obligations and requirements that broadly correspond to the objectives of the e-Privacy Directive. To avoid duplication, administrative burden and uncertainty, the security obligations set under the e-Privacy Directive should re-assessed against those instruments" (Access Now, 2016a). On the economic side, Access Now (2016a) argues that "the costs arising from the revised ePrivacy rules are justified by the improved safety for users (…). Any compliance costs associated with the privacy and security obligations of the e-Privacy Directive are at least mitigated by the benefits produced by the same privacy and security obligations in regard to increased user trust and networks' protection."

Overall, Access Now makes use of 11 consumer protection, three crime and security, nine human rights and seven economic arguments. As the number of public arguments exceeds the number of economic arguments, it overall relies on a public frame.

Bits of Freedom

"Bits of Freedom is the leading digital rights organization in the Netherlands, focusing on privacy and freedom of communication online." (Bits of Freedom, 2020).

It supports the Commission proposal to update the ePrivacy Directive and argues

> [a]t the time of the ePD's adoption, many elements of current technologies were not yet fully developed (…). These developments are not fully accounted for in the ePD. This has created arbitrary differences in the protection of users between different but functionally equivalent services (Bits of Freedom, 2016).

By referring to the 'protection of users' the employment of a consumer protection frame is signaled. Consumer protection is the center of the organization's argumentation. In most of its arguments, it emphasizes that privacy protection is a 'fundamental right' consumers have. Highlighting these key words signals the use of human rights frame. More precisely, Bits of Freedom draws attention to the inadequacy of the current ePrivacy Directive. It states that it "has failed to achieve full protection of the individual's right to privacy, confidentiality of communications and freedom to seek information without being continuously profiled and monitored online" (Bits of Freedom, 2016). Therefore, a revision is needed.

> [T]he new legal instrument must ensure full communications confidentiality and integrity on fundamental rights grounds. It is key that end users are protected against fundamental rights interferences, irrespective of the type of communications provider or services involved (Bits of Freedom, 2016).

In addition, the organization also addresses a few economic aspects. It argues that in any case, data protection should not be a matter of money. "The protection of fundamental rights should not depend on an economic cost/benefit analysis (…). Privacy protection should not be commodified, leading to different levels of protection depending on how much an individual could afford" (Bits of Freedom, 2016). The key words indicating the use of an economic frame include 'economic' and 'cost'.

Bits of Freedom provides four consumer protection, three crime and security, 15 human rights and five economic arguments. Therefore, a public goods frame was overall employed.

Bureau Européen des Unions de Consommateurs (BEUC)

BEUC represents interests of all Europe's consumers (Bureau Européen des Unions de Consommateurs, 2020). As its responses to the Commission's questionnaire were not publicly available and a written request was also unsuccessful, a summary of its responses, which has been published on its website, serves as the basis for analyzing BEUC's frame selection

approaching the Commission. BEUC emphasizes the need for a strong and coherent legal framework that allows to protect consumers' fundamental rights to privacy and data protection adequately. It argues that "[a] robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services" (Bureau Européen des Unions de Consommateurs, 2016). BEUC (2016) stresses that, "[t]he ePD is a fundamental piece of legislation for the protection of consumers' privacy." Whereas the organization extensively reflects on aspects related to consumer protection, human rights and crime and security, it does not address the frequently addressed aspect of creating a level playing field for companies. In contrast, it does not approve of the firms' position to repeal the regulation and specifically states: "We strongly welcome the Commission's determination to revise and update the e-Privacy Directive (ePD), despite continuous calls for repeal coming from different industry sectors" (Bureau Européen des Unions de Consommateurs, 2016). Due to the fact that over-the-top communication platforms are currently not covered by ePrivacy rules, legislation urgently needs to be adapted to the new communications landscape.

BEUC used 17 public goods arguments, nine relating to consumer protection, one relating to crime and security and seven relating to human rights. Additionally, it made two economic arguments. Thus, with respect to the analysis procedure, a public frame was overall employed by BEUC.

Center for Democracy and Technology (CDT)

CDT fights for online civil liberties and human rights, driving policy outcomes that keep the internet open, innovative, and free (Center for Democracy and Technology, 2020c). CDT welcomes the Commission's proposal for a revised ePrivacy Directive. With respect to the adoption of the GDPR and developments in communications technology and business models, it emphasizes the need to update the ePD. It argues that "[r]apid advancement in tracking technology has highlighted the need for consumer protection in this area" (Center for Democracy and Technology, 2016). By referring to 'consumer protection' CDT the use of a consumer protection frame is indicated. CDT does not believe that ePrivacy rules are redundant considering the existence of the GDPR. In contrast, it argues that "[a] compelling argument for proposing a new instrument to replace the E-Privacy Directive is the fact that the GDPR is not based on Article 7 of the Charter of Fundamental Rights of the EU on the right to privacy and confidentiality of communications" (Center for Democracy and Technology, 2016). In its eyes, GDPR does not sufficiently protect the right to confidentiality of communication.

> [A] new instrument should primarily target the areas not covered by the General Data Protection Regulation (GDPR). In particular, it should affirm the right to confidentiality of communications and strengthen consumer protection. This Article is not covered by GDPR, which implements Article 8 of the Charter of Fundamental Rights (Center for Democracy and Technology, 2017).

By highlighting individuals' 'right to privacy and confidentiality of communications' and pointing to the 'Charter of Fundamental Rights' CDT thes use of a human rights frame is indicated multiple times. Simultaneously, CDT is aware that the revision of existing ePrivacy rules will impact some businesses significantly. Therefore, it also reflects on the economic side to the proposal.

> In terms of substance, a new instrument should be conducive to the provision of a wide range of communications services, built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes (Center for Democracy and Technology, 2016).

It becomes clear that CDT sees a necessity in adapting existing rules in the way that it enhances consumers' protection while also allowing for innovation. The use of the key words 'business' and 'innovation' thereby indicates the use of an economic frame.

CDT overall uses one consumer protection, five crime and security, five human rights and 24 economic arguments. The number of economic arguments is much higher than the number of public goods arguments. Therefore, it employed an economic frame.

European Digital Rights (EDRi)

European Digital Rights (EDRi) is a civil and human rights organization which defends the rights and freedoms in the digital environment (European Digital Rights, 2020). EDRi supports the Commission's proposal and stresses the importance of updating the current legal framework covering electronic communication in light of the fundamental changes to communication provision. "The evergrowing connectedness of devices will increase the need for clear rules on protection of the confidentiality of communications, both for individuals and for businesses" (European Digital Rights, 2016a).

> [I]t is of utmost importance that internet users can rely on the confidentiality of their communications and the integrity of their devices. Their communications deserve protection in order to give effect to the fundamental rights to privacy, personal data protection and freedom of expression (European Digital Rights, 2016a).

EDRi does not only stress the need for adequate 'consumer protection' which alludes to the use a consumer protection frame, but in particular, it draws attention to the fact that it is a right that individuals possess. "The European institutions need to make an extra effort to ensure that privacy and confidentiality of communications of European citizens are not considered as a tradeable asset, but as a right to be strongly protected" (European Digital Rights, 2016a). In order to sufficiently safeguard that right, "the current text will need thorough work to ensure that the privacy, data protection and other fundamental rights of citizens are fully respected in the digital environment, especially also by providers of e-communication networks and -services and OTT providers" (European Digital Rights, 2016a). 'Right to privacy' and 'fundamental rights' are thereby signaling words for the use of a human rights frame. EDRi also makes multiples arguments which indicate the employment of a crime and security frame due to the occurence of the key word 'security'. "All of these legal instruments include security obligations which are, in one way or another, in the spirit of the text of the ePD. However, given the divergencies in the different instruments, we believe that the framework stated in the GDPR concerning security requirements should be set as the standard and be applied to the future legal instrument substituting the ePD" (European Digital Rights, 2016b). EDRi focuses its argumentation not only on aspects of consumer protection, security and human rights, but it equally outlines its position with respect to the proposal's impact for businesses. Here, EDRi comments in part on specific articles of the proposal and explains the impact on businesses. The most expressive economic argument it makes, summarizes that "EDRi considers the proposed Regulation will be a boost for innovation and economic growth in Europe" (European Digital Rights, 2016a). 'Innovation', 'economic' and 'growth' suggest the use of an economic frame.

EDRi overall uses two consumer protection, eight crime and security, six human rights and 14 economic arguments. As the number of public goods arguments exceeds the number of economic arguments, it employed a public frame.

Open rights group

The Open Rights Group is a UK based digital campaigning organization working to protect the rights to privacy and free speech online (Open Rights Group, 2020). The organization responded to the Commission's questionnaire but did not publish a supplementary position paper. It acknowledges the need to revise the current legislation on ePrivacy as it does not cover contemporary communication channels comprehensively. Current legislation would not allow individuals to understand and protect their data and privacy. Even though the

organization does not seem to have expert knowledge in the field of ePrivacy, it stresses businesses' obligation to adhere to the fundamental human rights. "We do not have information on these aspects, but generally respect for fundamental rights should be a core aspects of any modern business, incorporated in their financial calculations" (Open Rights Group, 2016) As it simulataneously refers to 'fundamental rights' and 'business' the use of both a human rights and economic frame is indicated. "Individuals have a right to secure their communications, but companies also have an obligation and should not simply pass this responsibility on to the customer" (Open Rights Group, 2016) Thus, it links economic and human rights aspects. It even specifically states that privacy protection is a human right: "An additional aspect is that a monetary approach could lead to the people suffering economic deprivation enjoying lower levels of privacy – which ultimately is a human right" (Open Rights Group, 2016). Additionally, with regards to security implications underlying the current insufficient regulation, the organization outlines "What data is retained for billing and for how long needs tightening. This is currently open to abuse" (Open Rights Group, 2016). 'Abuse' thereby signals the use of a crime and security frame.

Overall, the Open Rights Group uses two consumer protection, four crime and security, five human rights and six economic arguments. As the number of public goods arguments exceeds the number of economic arguments, it employed a public frame.

Sectional Groups

Application Developers Alliance

The Alliance "represents software developers and the companies invested in their success" (Application Developers Alliance, 2017). It welcomes any efforts to align existing privacy rules and match them with the digital environment. However, as the ePrivacy Regulation does not seem to deliver those objectives, the Alliance advocates for repealing it. In fact, it is "also dubious that the proposed regulation will help achieve better consumer satisfaction or protection" (Application Developers Alliance, 2017). The use of the word combination 'consumer' and 'protection' thereby indicates the use of a consumer protection frame. More generally, the Alliance "encourage[s] the Commission to consider deregulation of existing electronic communication services where this does not harm consumer interests or compromise national or public security, prevention, detection and prosecutionof [sic!] criminal offences" (Application Developers Alliance, 2016). Referring to 'security' and 'criminal' makes the organization alludes to the use a crime and security frame. With respect to potential

economic implications of the proposal, the Alliance outlines that laws and regulations should support and not hinder innovations.

> The current proposed rules would restrict and discourage the development of features based on content analysis, from the more traditional (such as spam-filtering or fraud detection software) to the most innovative (applied artificial intelligence). Some of the many examples of industry leaders collaborating to accelerate the growth of artificial intelligence (Application Developers Alliance, 2017).

"Possible new rules concerning this matter should be technology neutral and should avoid to require any specific business model to be adopted" (Application Developers Alliance, 2016). These arguments contain important key words that signal the use of an economic frame. They include: 'innovative', 'growth' and 'business'.

As the Alliance employed five consumer protection, five crime and security, no human rights, 20 economic arguments, it overall relied on an economic frame.

DIGITALEUROPE

"DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe" (DIGITALEUROPE, 2020). It advocates for simplifying the existing legal framework and repealing legislation in case it overlaps with other legislation and represents a burden for businesses. More precisely it states,

> [t]he review of the ePD offers a unique opportunity to simplify and streamline legislation in line with the European Commission's Better Regulation Agenda; and to achieve a simple, consistent and meaningful set of rules designed to protect citizens' privacy and personal data (DIGITALEUROPE, 2016a).

Referring to the key words 'consumer' in combination with 'protection' indicates the employment of a consumer protection frame. With respect to consumer protection, it further argues that "[a]ll provisions must be carefully considered as to whether they are relevant or bring any value to the protection of citizens" (DIGITALEUROPE, 2016a). Digital Europe also emphasizes that it is a human right that should be safeguarded. "No law should restrict individuals ability to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, a right enshrined in the Charter of Fundamental Rights" (DIGITALEUROPE, 2016b). Including the key words 'human right' and 'Charter of Fundamental Rights' clearly signals the use of a human rights frame. Although the organization acknowledges the right, it does not see a necessity in keeping the ePrivacy regulation as a separate legal instrument.

> It seems that the only real reason for maintaining the current ePrivacy framework is to ensure that the fundamental right to private communications (as established in Article 7 of the European Charter of Fundamental Rights) is respected. Arguably a standalone legal instrument, such as the ePD, is not necessary to ensure that communications remain confidential. The right is fundamental in EU law and there is a wealth of EU national and case law where this right has been enforced and concretely implemented, even outside privacy legislation (DIGITALEUROPE, 2016a).

In addition to highlighting aspects of consumer protection and human rights, it also elaborates on the topic of 'security' alluding to the use of a crime and security frame.

> [S]ecurity plays an integral part in protecting users from malicious activity and generating trust in the reliability of devices and services. The Article 29 Working Party has consistently argued that processing for maintaining and managing technical security should fall under one explicit exception for the processing of terminal equipment data in the ePR. The European Parliament's report and the Council's Doc. 15333/17 have proposed an exception that only applies for security updates (i.e. downloads) to the device but does not reflect the fact that detecting security vulnerabilities, with a view to creating patches, also requires an upload of data from devices. We therefore urge the co-legislators to adopt a more general security exception that is consistent for all type of data covered by the ePR (DIGITALEUROPE, 2018b).

With respect to the economic implications of the proposal, Digital Europe elaborates that businesses would face additional financial burden which could not be justified. "We do not believe the compliance costs associated with the ePD are proportionate to the objectives pursued. Industry has been faced with conflicting provisions and an un-harmonised implementation across Member States. This has led to confusion and a negative impact for both industry and citizens" (DIGITALEUROPE, 2016b). "This inconsistency created additional costs for business and led to fragmentation in the internal market" (DIGITALEUROPE, 2016b). "An open market will allow companies to compete and users to rely on the services, which they believe constitute the best offerings" (DIGITALEUROPE, 2016b). It becomes clear that the proposed new ePrivacy regulation is economically not viable. The employment of an economic frame is therby indicated by the use of the key words 'costs', 'industry', 'market', 'company' and 'compete'.

Digital Europe uses 14 consumer protection, 30 crime and security, 9 human rights and 41 economic arguments. It thus overall employed a public frame.

Ecommerce Europe

Ecommerce Europe is the voice of the Digital Commerce sector in Europe representing more than 100,000 companies selling goods and services online to consumers in Europe. (Ecommerce Europe, 2020). Overall, Ecommerce Europe supports the plan to modernize the current ePrivacy Directive in order to adapt the ePrivacy legal framework to the digital environment which is imperative for its members' businesses. Nevertheless, the organization does not welcome all provisions included in the draft.

> Instead of focusing on the processing of personal data and privacy aspects which are sufficiently covered by the GDPR also for electronic communications, the Regulation should focus on the right on confidentiality of electronic communications. This makes perfect sense given the fact that the main issues of the ePrivacy framework (confidentiality of electronic communication content and metadata, respect for the private sphere of the terminal equipment of the end-user and respect for a natural persons' electronic mailbox) are based on the fundamental right of respect for everyone's private and family life, home and communications, as laid down in Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) and not on the fundamental right to the protection of personal data, as laid down in Article 8 of the Charter and Article 16 of the Treaty on the functioning of the European Union (Ecommerce Europe, 2017).

Here, Ecommerce Europe clearly discusses human rights aspects. Thereby key words such as 'human rights' or 'Charter of Fundamental Rights' indicate its use of a human rights frame. From an economic point of view "Ecommerce Europe also supports co-regulation and soft-law in the digital sphere because technological developments and business models are evolving too fast in relation with the legislation which tends to lag behind" (Ecommerce Europe, 2016). Considering the great competition in the market, Ecommerce Europe calls for equal treatment of all firms. "The major players that develop browsing software (Google Chrome, Microsoft Internet Explorer, Apple Safari) - all established outside of the European Union - would be able to regulate standard access to the terminal equipment by browser setting consent systems, not only for themselves but also for their competitors. This would in fact allow these players to have a very favorable position, permitting them to use cookies necessary for the operation of the browser itself for all the services they provide on the web (search, advertising, audience analysis, etc.) and preventing competitors to benefit in the same way from the browser settings.

> In that perspective, Ecommerce Europe asks European legislators to come up with provisions that prevent the major publishers of navigation software to abuse browser

> setting consent systems to have a competition advantage or not complying with the European standards required by the GDPR (Ecommerce Europe, 2017).

Ecommerce elaborates extensively on economic aspects, which indicate the use of an economic frame. Key words include ‘business, ‘competition’ and ‘market’. Concerning aspects of security underlying the proposal, the organization gives precise recommendations:

> Ecommerce Europe strongly recommends a new exception (subsection (e)) on behalf of repairing security, technical faults and/or errors in the functioning of information society services: (e) it is necessary to maintain or restore the security of information society services, or detect technical faults and/or errors in the functioning of information society services, for the duration necessary for that purpose (Ecommerce Europe, 2017).

Thus, by referring to ‘security’ the employment of a crime and security frame is indicated.

Ecommerce Europe emphasized three issues referring to consumer protection, two crime and security, one human rights argument and 19 referring to economic issues. It therefore overall employed an economic frame.

European Telecommunications Network Operators' Association (ETNO)

ETNO represents Europe’s telecommunication network operators. During the preparations of the GDPR, ETNO has already pleaded for repealing the ePrivacy framework. It believes that the GDPR already covers the digital environment adequately. As the objective is to “move towards a consistent privacy framework for the benefit of businesses and consumers” (ETNO, 2017) there is no need for a separate legal instrument. ETNO makes clear that “[t]he coexistence of two different set of rules creates legal uncertainty and confusion, undermining the coherence and trust on the online Consumer Policy, as European citizens cannot rely on consistent protection of their personal data and privacy” (ETNO, 2016). Thus, from a consumer protection point of view, updating the ePrivacy rules would have the opposite effect and would rather weaken consumer protection. “Maintaining two different set of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection” (ETNO, 2016). These arguments indicate the use of a consumer protection frame as they contain the key words ‘consumer’ or ‘citizen’ in combination with ‘protection’. Alongside the negative implication for consumers, business would also be negatively impacted. “Trying to be even more protective for consumers, the future ePrivacy Regulation could actually have a negative effect on European consumers, reducing the ability for telecom operators in Europe to create the best in class products for them”. (ETNO, 2017). “The unequal application of rules for functionally equivalent services prevents telecommunications services providers from competing on equal footing in a single market” (ETNO, 2016). Referring to prospective

obstacles for fair competition by using the key words ‘competing’ and ‘market’ indicates the existence of an economic frame. From a security point of view

> [t]he new GDPR, together with the possibility to engage in ex-post antitrust actions (and the possibility of legal actions from national DPA), provide a comprehensive framework to monitor the commercial exploitation of users data by all kind of providers of digital services, regardless of the type of services provider at stake. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users. As a result, there is no need to apply different tools than GDPR and Antitrust Law in order to monitor the commercial exploitation of traffic and location data by any provider of digital services (ETNO, 2016).

Thereby the key words ‘exploitation’ and ‘abuse’ signal the use of a crime and security frame. Overall, while ETNO elaborates also quite extensively on the implications for consumers, its argumentation focuses to a greater extent on economic aspects. It concludes

> [a]s long as the ePD coexists with the new GDPR, there will be no level playing field, consumers will not experience comparable digital privacy online and operators will continue to face this dual compliance regime and their competitive position will be compromised (ETNO, 2016).
>
> Maintaining a double set of rules based on an old structure of sharing of competences will stand in the way of an equal level playing field, will continue to cause confusion for businesses and consumers and will finally hamper the possibility of European telecommunication providers to develop innovative services (ETNO, 2017).

The used key words for an economic frame include ‘level playing field’, ‘competitive’, ‘businesses’ and ‘innovative’.

ETNO used 19 public goods arguments, thereof 11 consumer protection arguments, four crime and security arguments and five human rights arguments. Additionally, it used 32 economic arguments. As the number of economic arguments exceeded all other types of arguments the overall employment of an economic frame could be identified.

European Internet Services Providers Association (EuroISPA)

”EuroISPA is a pan European association of European Internet Services Providers Associations (ISPAs). It is the world's largest association of Internet Services Providers (ISPs), representing over 2300 ISPs across the EU and EFTA countries” (EuroISPA, 2020). EuroISAP does not see a necessity in keeping a separate ePrivacy regulation. In fact

> the EU Treaty, EU Charter of Fundamental Rights, GDPR Directive and Member States' constitutions all already protect the secrecy of communication, thus allowing the use of encryption and other means of self protecting personal communication. New European legislation is not needed to ensure this already existing right (EuroISPA, 2016).
>
> Furthermore, there is a chance that legislating for such a right would actually result in a diminished right. This principle is enshrined as a fundamental right under Article 7 (Respect for private and family life) of the EU Charter of Fundamental Rights and has been further specified and applied through national and European case law (EuroISPA, 2016).

By using the key words 'Charter of Fundamental Rights' and 'fundamental right' the employment of a human rights frame is indicated. From a consumer protection perspective, "individuals should always be able to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, but more importantly no law should restrict that ability" (EuroISPA, 2016). Despite the fact, that EuroISPA reflects on public goods issues, its argumentation on economic arguments is more elaborate. Most importantly, "[r]egulation should not unduly interfere with companies freedom to choose and develop innovative business models where there is clear consumer demand. This would be contrary to the fundamental principle that regulation should only be enacted where it is necessary to address a clear issue in the market, and that any regulation should be proportionate and technologically neutral, so as not to favour certain business models or technology over others" (EuroISPA, 2016). "There is no necessity to treat traffic data any different than other kinds of data. This approach will result in redundant double regulation, that further restricts companies' opportunities to use such data and stifle innovation in Europe" (EuroISPA, 2016). Using words such as 'innovation' and 'business' clearly characterizes an economic frame.

As EuroISPA discusses four public goods issues, thereof one crime and security and three human rights aspects, and makes ten economic arguments, it overall employs an economic frame.

European Magazine Media Association (EMMA)/ European Newspaper Publishers' Association (ENPA)

ENPA, representing publishers of newspapers in Europe and EMMA, the European Magazine Media Association, provide a joint position on the ePrivacy regulation. Their members are newspaper and magazine publishers who face significant challenges with respect to digitization. For their business models, cookies are essential as they provide them with information on their readership.

> They [cookies] allow publishers to develop innovative ways of reaching out to their readers online, for instance by matching their potential interests with tailored advertising offers. Misinterpretations of the scope and requirements of Article 5(3) have had detrimental consequences in some countries (including financial costs) and represent further obstacles to the development of data-driven business models online (EMMA/ENPA, 2016b).

ENPA/EMMA (2016b) is concerned that

> [a] general consent requirement for the setting of cookies only favours large international companies such as free e-mail providers or social networks, which base their business models on log-in systems. For those companies it is relatively simple to obtain the required consent of their customers, due to the direct contact inherent in the system with their customers."

Thus, they see their members disadvantages as opposed to the big players. Nevertheless, they argue that "[t]he European Commission should not propose legislation imposing a particular type of business model on private undertakings. This would infringe the fundamental freedom to conduct a business while not efficiently and proportionately addressing the issue at stake" (EMMA/ENPA, 2016a). All these arguments include important key words that characterize an economic frame. These include 'innovative', 'business' and 'companies'. ENPA/EMMA overall predominantly focuses on economic aspects related to the Commission's proposal, which are highlighted by the signal words 'innovative', 'companies' and 'business'.

Overall, only two consumer protection and 13 economic arguments are provided which results in the employment of an economic frame.

European Publishers Council (EPC)

The European Publishers Council (EPC) is composed if Chairmen and CEOs of the leading media corporations in Europe. It represents companies that operate in the fields of "news media, television, ration, digital market places, journals, eLearning, databases and books" (European Publishers Council, 2020). The EPC only responded to the Commission's questionnaire but did not publish a supplementary position paper.

EPC does not welcome the Commission's ePrivacy draft as they do not see any benefit for their members. "Regarding the areas of interest to EPC membership, we believe that the additional protections of ePD afforded to subscribers and users are effectively non-existent" (European Publishers Council, 2016). Referring to 'protection' in combination with 'user' thereby indicates the use of a consumr protection frame. Another reason for its aversion towards

the proposal is its narrow focus on Europe. “Given the global nature of the internet any attempt to produce only European standards would be a failure and disregard the reasonable expectations of a global industry” (European Publishers Council, 2016). ‘Industry’ os the key word of this example that indicates the use of an economic frame. While it also draws attention to the fact that “[m]any forget that in the Charter of Fundamental Rights Art 16 and 17 protect the freedom to conduct business and the right to property, therefore they should be taken equally into account when formulating policy proposals” (European Publishers Council, 2016), it still predominantly focuses on discussing the economic implication of the draft. In advocates for minimum intervention in the market. “Contractual freedom is paramount in the free economy and should have as little interference as possible” (European Publishers Council, 2016).

> Industry has shown responsibility by setting up a self-regulatory program providing simple information to users, but also providing them with the tools to exercise effective choices and control by opting out of data collection via cookies for the purposes of online behavioral advertising techniques, which have been very well received by consumers (European Publishers Council, 2016).

While the business perspective prevails, EPC still acknowledges that “[l]egislation should keep the right balance protecting the privacy of consumers on the one hand and business interests on the other (European Publishers Council, 2016).

As it provides three consumer protection, two crime and security, two human rights, and 14 economic arguments, it overall employed an economic frame

GSMA

> The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors (GSMA, 2020).

GSMA does not welcome the Commission’s proposal on updating the ePrivacy legal framework as it does not see any added value. The organization gives a balanced account of the drafts’ prospective implications for consumers and businesses. GSMA’s key argument is that

> [t]he ePDs current scope does not reflect the converging area of electronic telecommunications where functionally equivalent services are not subject to the same regulatory constraints. Accordingly, the ePD is neither technology-agnostic nor provideragnostic. This has led to the problem that users cannot rely on consistent protection standards across the digital market even when using comparable services (GSMA, 2016b).

Thus, by simultaneously referring to a consumer protection and an economic argument, GSMA makes clear that the new regulation would neither benefit consumers nor businesses. In this case, the key words ‘user’ in combination with ‘protection’ and ‘market’ indicate the use of a consumer protection and economic frame respectively.

> As it is applied only to telco providers and not to other players supplying similar services, the consumer is not protected in an equal measure and telco operators have been put at a competitive disadvantage compared to other players offering similar services (GSMA, 2016b).

Here again, the use of a consumer protection and economic frame is simultaneously signaled using the key words ‘consumer’ in combination with ‘protected’ and ‘competitive’. Therefore, GSMA advocates that “[a]n overall consumer protection standard has to be established to ensure that consumers are protected regardless of their location” (GSMA, 2016a). Also, with respect to aspects of security

> [a]ll types of network listed whether public, private, closed or non-commercial WIFI should apply a level of security that is appropriate to the circumstances. As opposed to setting up a separate legal instrument, GDPR can offer “a more consistent and horizontal approach will be taken, which leads to a level playing field and thus contributes to raise users trust” (GSMA, 2016b).

“Generally, in cases where a competitive market can solve the required objectives through self-regulation, any unnecessary legislation leads to legislative burden and disproportionate costs“(GSMA, 2016a). ‘Competitive’, ‘market’ and ‘costs’ thereby indicate the use of an economic frame.

Overall, GSMA provides seven consumer protection, six crime and security and 13 economic arguments. Since both types of frames are used to an equal extent, GSMA employed a public and economic frame simultaneously.

Firms

Cisco

Cisco Systems Inc. is a leader in Internet networking. “Its networking solutions connect people, computing devices and computer networks, allowing people to access or transfer information without regard to differences in time, place or type of computer system” (Cisco Systems Inc., 2020). Cisco Systems elaborates extensively on its position concerning the ePrivacy regulation. It did not only respond to the Commission questionnaire but also provided a supplementary position paper. The arguments provided by Cisco Systems overall indicate that

it would recommend withdrawing from the current proposal. While it clearly outlines the need for adequate consumer protection, it does not see a necessity in keeping a separate legal instrument to achieve it. It outlines that "[i]ndividuals should have the right to secure their communications but we are not convinced that the ePD, or its potential successor, is needed to achieve this end" (Cisco Systems, 2016a). According to the determined key words for frame classification, this argument indicates the use of a human rights frame which is signaled by the words 'right to secure communications'. Arguments related to crime and security are also highlighted by the firm "Nevertheless, the ePD creates an unnecessary overlay that could lead to different security requirements (especially as the GDPR requirements are somewhat broader) and certainly gives rise to different enforcement bodies having the right to issue instructions to service providers, quite possibly in different countries (given the one stop shop found under the GDPR)" (Cisco Systems, 2016a). "As a result of the arguments above, there is no need to maintain or extend security measures or maintain data breach requirements under the ePD" (Cisco Systems, 2016b). 'Security' thereby indicates the use of a crime and security frame. In addition, Cisco Systems provides multiple arguments that underline that protection of personal data is a human right. It elaborates that "[t]he right to private communications is established in Article 7 of the European Charter of Fundamental Rights. As a result, it is important that this fundamental right is adequately reflected in Community law" (Cisco Systems, 2016b). In contrast to other interest groups, Cisco Systems does not only reflect richly on issues related to public goods but equally reflects on the economic impact of the proposal. It argues that a separate legal instrument for ePrivacy would entail high costs for companies. "According to our understanding, the ePD adds little in terms of protection related to the risks presented but brings significant additional costs" (Cisco Systems, 2016a). "The mandate of expensive new services is not commensurate with the return in terms of public good, particularly in a competitive market" (Cisco Systems, 2016a). The use of an economic frame is indicated by the key words 'costs', competitive' and 'market'.

Overall, Cisco Systems provided 28 public goods arguments and 17 economic arguments. As the number of public goods arguments exceeds the number of economic arguments, it overall employed a public frame.

Facebook

Facebook is an American company that offers online social networking services. It helps people around the world to stay connected and share information and ideas (Facebook, 2020). New users can create profiles, upload photos, join or start new groups. Facebook has submitted

the filled in questionnaire as well as a complementary document that elaborates on a few answers (1A, 6A, 20A, 25A) in greater detail. Facebook clearly outlines its aversion towards the Commission's proposal. In its view, a standalone ePrivacy regulation is not required as other legal instruments cover the issue of personal data privacy and protection. A revised ePrivacy regulation would only duplicate existing legislation and would consequently lead to a fragmented legislative landscape that harms businesses and consumers. More specifically, it argues that "where privacy regulations applied to traditional telecommunications operators are no longer needed to protect consumers, because they are adequately covered in the GDPR or other legislation, they should be eliminated" (Facebook, 2016a). Facebook provides multiple arguments that characterize a consumer protection frame, which can be identified using the signal words "protect and consumer", as the example has demonstrated. In addition to referring to the aspect of consumer protection, the firm also addresses two security and crime aspects that potentially arise with the introduction of the revised ePrivacy regulation. "From our perspective, we consider that including measures on security in the ePD is unnecessary. Measures aimed at ensuring sufficient security (whether in terms of security of networks, security of equipment) already exist in a number of other legislative instruments" (Facebook, 2016b). There is therefore no regulatory gap that needs to be filled by including security measures in the ePD. It further elaborates on a crime and security aspect. "Building in a "secret" opening for law enforcement to unlock encryption also creates an opening for other actors to exploit it. Criminals and oppressive regimes could use a "backdoor" to achieve their own ends" (Facebook, 2016a). 'Security', 'exploit' and 'criminal' thereby indicate the use of a crime and security frame. Facebook is also aware that confidentiality of communication is a fundamental right which needs to be preserved.

> The Charter of Fundamental Rights states everyone has the right to respect for his or her private and family life, home and communications. Confidentiality of communication is guaranteed as a fundamental right under Art. 7 (Respect for private and family life) of the Charter and is further specified and applied through a number of national and European case law. This allows users to access and use the best possible technology/methods to secure and protect the confidentiality of their communications (Facebook, 2016a).

In addition to highlighting aspects related to public goods, Facebook also addresses potential negative economic consequences for businesses in case the proposal will be adopted. "From our perspective we consider that the ePD has led to increase in compliance costs for businesses which cannot readily be justified" (Facebook, 2016a). "Duplication of rules will be burdensome

for business, and will lead to an increase in costs of compliance - that is unnecessary and disproportionate - and ultimately risks leading to higher costs for users" (Facebook, 2016a). "In a data-driven economy that takes full advantage of the growth opportunities of data, private companies should be free to decide their business models, as long as the privacy rights of the users are cared for and safeguarded" (Facebook, 2016a). Considering that the new regulation leads to higher compliance costs for businesses, hinders innovation, and generally discriminates online services, Facebook overall does not approve of the proposed regulation. Following its argumentation, the key words 'costs', 'businesses', 'economy' and 'growth' thereby characterize an economic frame.

Following the hand-coding procedure as explained in chapters 5.4.2 and 5.6, 14 public goods arguments and 16 economic arguments could be identified. More specifically, Facebook used ten arguments that refer to consumer protection emphasizing the importance of ensuring security, privacy and confidentially of the communication to its users, two arguments that refers to security and crime and two arguments concerning human rights.

Google Inc.

Google Inc. offers a wide range of internet services and products. Its mission is "to organize the world's information and make it universally accessible and useful" (Google, 2020). Google pleads for the adoption of rules that protect the confidentiality of communications but do not hinder its business. It argues that "[r]egarding the confidentiality of communications, it is important to find a workable and practically implementable solution to achieve the fundamental objective of this right, namely to protect the privacy of the communications from other individuals" (Google, 2016). According to the procedure of frame classification, Google highlights a human rights aspect. This is signaled by using the words 'fundamental right'. Google further outlines that "[t]he right to privacy and confidentiality are important fundamental rights" (Google, 2016). With regards to potential economic implications of the proposed ePrivacy Regulation, the firm outlines the obstacles business might face. "The implementation of the e-Privacy Directive has proven challenging and resource intensive to many in industry" (Google, 2016). One of the reasons is incoherence across member states. Based on a study which Google cites, it outlines that the regulation's "implementation varies significantly among Member States, creating challenges for businesses trying to participate in the Digital Single Market" (Google, 2016). On the one hand, Google directs attention to the aspect of inconsistency, on the other hand it also addresses that rules should not restrict future innovations. "However, it is important that any legislation remains technology neutral and does

not mandate any particular means to achieve such security, thereby allowing businesses to innovate and provide state of the art solutions to their users" (Google, 2016). The words 'industry', 'market', 'businesses' and 'innovate' clearly indicate Google's reliance on an economic frame. Aligning ePrivacy rules with already existing legislation, in particular the newly revised GDPR should be a priority. This would create legal clarity and pave the way to a harmonized and coherent legal framework that effectively protects personal data.

Overall, Google Inc. used ten public goods arguments, thereof five consumer protection arguments, one crime and security argument and four human rights arguments. Additionally, it emphasized eight economic aspects. As the number of public goods arguments exceeds the number of economic arguments, Google overall employed a public frame (Appendix A).

Microsoft

Microsoft is a software company that aims to "empower every person and every organization on the planet to achieve more" (Microsoft, 2020). It draws in particular attention to potential impacts for businesses. It questions the need for separate electronic communication rules to the already existing laws, including the GDPR. "Given this greater level of competition, market forces influence product development significantly (…), it is not clear that additional regulatory regimes - which may inhibit innovation and decrease competition by increasing barriers to entry - are needed" (Microsoft, 2016). The signal words 'competition', 'market' and 'innovation' for the identification of an economic frame are used. The issue of competition is taken up multiple times by Microsoft. It further elaborates that

> [t]he Commission should carefully assess the benefits of a Regulation but should also consider the risks, including a Union-wide loss of competitiveness if the Regulation becomes a vehicle for over-regulation of application layer communications. It would be better for some States to implement anti-competitive application layer communication regulations individually rather than to introduce such rules at the EU level (Microsoft, 2016).

"Digital communications are, and will continue to be, characterized by rapid innovation and competition. In contrast, regulatory mechanisms -such as delegated acts - can be cumbersome and slow to keep updated" (Microsoft, 2016). Whereas the economic side to the proposal is discussed quite extensively, Microsoft only addresses issues of consumer protection briefly. "We likewise believe that communication providers should remain free to innovate, including by developing security and encryption options demanded by their customers" (Microsoft, 2016). Referring to 'innovate and 'security' in combination with 'customers' simultaneously

indicates the use of an economic and a consumer protection frame respectively. However, it emphasizes that "[i]t should be clear that any right to secure communications for users is in respect of Member State and Union laws that would otherwise deprive them of that right - and not a right for them to force startups, etc., to implement encryption features, which may not be appropriate" (Microsoft, 2016). Microsoft (2016) "strongly support[s] protections for the confidentiality of electronic communications. Data protection is a human right". The examples of its argumentation clearly hint at the use of a human rights frame which derives from the key words 'human right'.

Microsoft overall employed an economic frame as it stressed a larger number of economic arguments as opposed to public goods arguments. In fact, it provided 19 economic arguments and ten public goods arguments (one consumer protection, six crime and security, three human rights).

Mozilla

> Mozilla is
>
> committed to an internet that includes all the peoples of the earth (…) that promotes civil discourse, human dignity, and individual expression (…) that elevates critical thinking, reasoned argument, shared knowledge, and verifiable facts [and] (…) that catalyzes collaboration among diverse communities working together for the common good (Mozilla, 2020).

Mozilla did not only reply to the Commission's questionnaire, but it also published a supplementary position paper which reflects on the Commission's draft for a revised EU legal instrument regarding electronic privacy. Against the backdrop that technological changes have taken place and the current ePrivacy rules, the e-Privacy Directive, "fails to provide effective privacy protections for users, and yet also imposes inefficient burdens on industry" (Mozilla, 2017). This argument exemplifies the use of both a consumer protectioin and economic frame as the key words 'protection' in combination with 'consumer' as well as 'industry' are mentioned. Mozilla is generally supportive of the proposal and confirms the need to update ePrivacy rules. With respect to the protection of consumers it outlines that "[r]ules of the road that provide a baseline level of protection of user privacy and the increasing amount of data that can be collected, shared, and stored via the internet of things are demonstrably useful" (Mozilla, 2016). It believes "that companies like Mozilla must be able to build the best security for their users that they can provide, to ensure the continuation of trusted communications systems which are key to fostering trust in the internet economy" (Mozilla, 2016). Mozilla takes up the aspect of consumer protection eight times. In addition, reflecting on the crime and security side

to the proposal, Mozilla argues that security or product updates need to take place. “This includes scanning, filtering, and ultimately processing both communication content and metadata for the detection and prevention of malware, phishing, and spam, other forms of abuse of networks, services and users in addition to software updates, that are a crucial measure to enhance security” (Mozilla, 2017). ‘Malware’, ‘abuse’ and ‘security’ thereby indicate the use of a crime and security frame. Following the coding procedure, Mozilla makes use of ten crime and security arguments which were identified in the basis of the occurrence of key word, including ‘security’, ‘crime’ and ‘fraud’. Mozilla is also aware that “Article 7 of the Charter of Fundamental Rights establishes the right of individuals to secure their communications” (Mozilla, 2016).

> For electronic communications, employing anonymisation techniques are likewise important both for the user and for the service; the former because their right to privacy is a fundamental right, and for the service because it greatly reduces the risk associated with collecting and processing communications content and metadata (Mozilla, 2017).

In addition to elaborating on aspects related to public goods, Mozilla addresses economic aspects which indicate the use of an economic frame. Key words include ‘business’, ‘industry’ and ‘innovation’. “From the perspective of businesses, varied implementations in MS also resulted in various, at times conflicting interpretations of EPD that ultimately stood in the way of consistent enforcement and application of the rules” (Mozilla, 2016). “The current EU legal instrument regarding electronic privacy, the e-Privacy Directive, is in need of reform. It (…) imposes inefficient burdens on industry” (Mozilla, 2017). “Mozilla strongly supports regulatory incentives that would require companies to have processes in place to address lawful access requests by state actors” (Mozilla, 2017).

Mozilla makes 21 public goods arguments, thereof eight refer to consumer protection, ten to crime and security and three to human rights. In addition, it uses 18 economic arguments. Thus, it overall employs a public frame.

Nokia

Nokia is a communications service provider that offers “a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe” (Nokia, 2020). To express its position concerning the Commission’s proposal on a revised ePrivacy legislation, Nokia responded to the Commission’s public consultation and wrote a separate position paper which specifically addresses the consultation questions 17, 18 and 19. Overall, Nokia is concerned that the new ePrivacy regulation would not improve consumer’s protection

while benefiting the dominant player in the data economy. Therefore, it does not welcome the Commission's draft in its present form, but it calls on policymakers to review it. While the question of whether it is justified to include OTT in the new legislation has been discussed controversially among many firms, Nokia does not prioritize this issue. Rather, it generally supports strengthening existing privacy and data protection rules for electronic communication irrespective of the type of firm that is covered by the legislation.

> In the era of convergence and technological neutrality, it is not appropriate to impose different data protection obligations on providers of functionally equivalent services depending on whether they are OTT and other information society providers or traditional telecommunications companies. It would not however be appropriate nor desirable to limit the processing of traffic and location data to consent only. This may impede innovation and hinder future legitimate uses of these data (Nokia, 2016b).

This statement is one example that shows its use of an economic frame. Key words are 'companies' and 'innovation'. However, from an economic point of view, Nokia also sees a necessity in adapting the current ePrivacy and GDPR rules. "We believe that both the GDPR as well as the ePD in its current version prevent the establishment of new business models and data monetization" (Nokia, 2016b). Additionally, Nokia points out that

> [t]he right to respect private and family life, home and communications is ensured by the EUs Charter of Fundamental Rights and the ICCPR Article 17. The protection granted by the Charter and the ICCPR is universal and should be also ensured in the law enforcement context. The existence and scope of this fundamental right should be clarified and defended against improper intrusion by the EU Member states (Nokia, 2016b).

It thus uses an argument that indicates the use of a human rights frame. Nokia furthermore argues that "[s]ecurity provisions in European legislation should be consistent, complimentary and not duplicate or overlap with each other" (Nokia, 2016b). Highlighting the 'security' aspect of the proposal indicates the use of a crime and security frame.

As Nokia makes seven public goods arguments, thereof two consumer protection, two crime and security and three human rights arguments, and eleven economic arguments, it overall employs an economic frame.

Orange

"Orange is one of the largest operators of mobile and internet services in Europe and Africa and a global leader in corporate telecommunication services" (Orange, 2020). Orange

makes multiple arguments that refer to consumer protection. Today's communication landscape is versatile. The main issue that derives from it concerns the inconsistent level of protection for users. More precisely, Orange states

> "[t]oday, communication services have evolved and include a broad set of services that consumers consider substitutable, even if they are technologically and regulatory different and do not grant consumers the same level of protection. (…) European citizens cannot rely on European rules to consistently protect their privacy (Orange, 2016).

It further elaborates that "[t]he ePR should be driven by the objective to provide identical privacy protection to consumers, whichever service provider they choose" (Orange, 2017). Incorporating words such as 'cititzens' and 'consumers' in combination with 'protection'thereby indicates the use of a consumer protection frame. In accordance with other firms, Orange does not only address issues related to public goods that underlie the Commission's ePrivacy regulation draft, but it also states its position on the potential economic impact. In particular, it reflects on the imbalances between OTT and traditional telecommunication companies.

> Unlike telcos, OTT are global players that are allowed to commercially exploit the traffic data and the location data they collect. However, there is no technical (sic!) or legal reason to consider that traffic and location data collected from telcos and OTT should be treated differently by regulators and competition authorities (Orange, 2016).

'Exploit' indicates the use of a crime and security frame. While 'competition' usually signals the use of an economic frame, the word combination of 'competition authorities' was excluded from the list of key words that determine an economic frame. As a traditional telecommunications company, Orange thus feels disadvantages as compared to OTT. It advocates that OTT must also adhere to the same rules as traditional telecommunication companies. Otherwise, competition would not be fair. "Moreover, by giving a pivotal role to software companies such as providers of Internet browsers, several of which also carry Internet services and advertising activities, the new ePR could severely harm competition" (Orange, 2017). Based on the occurrence of key words such as 'companies', and 'competition' this argument clearly signals the use of an economic frame. In line with the request for equal standards for communication providers of any kind, Orange believes that "[t]he ePR should be driven by the objective to provide identical privacy protection to consumers, whichever service provider they choose, and identical opportunities to all providers of digital services to develop data based innovations" (Orange, 2017). Thus, it makes clear that creating a level playing field

for companies, would not only create economic balances but it would also be vital to ensure consistent consumer protection. Lastly, Orange addresses the security aspect underlying the proposal. “The application of privacy rules in the GDPR and the possibility to engage in ex-post antitrust actions provide a comprehensive framework to monitor the commercial exploitation of users' data by all kind of providers of digital services. This framework provides a safeguard against abuse of dominant position based on the over-exploitation of personal information related to individual users” (Orange, 2016). The use of the key words ‘exploitation’ and ‘abuse’ thereby signal the employment of a crime and security frame.

Looking into Orange’s argumentation in more detail, 22 public goods arguments (14 consumer protection, four crime and security, four human rights) and 16 economic arguments could be identified. Therefore, Orange overall relied on an economic frame.

Telefónica

Telefónica is one of the largest telephone operators and mobile network providers in the world (Telefónica, 2020c). The company’s aim is to “facilitate communication between people, providing them with the most secure and state of the art technology in order for them to live better, and for them to achieve whatever they resolve” (Telefónica, 2020b). In line with its corporate views as states on its website, Telefonica highly values personal data and believes that its control is key to generating users’ trust (Telefónica, 2020a). Telefónica argues that in case the GDPR and the ePrivacy regulation continue to coexist, personal data protection and privacy cannot be adequately ensured and a level playing field cannot be created for businesses.

> As long as the ePrivacy Directive coexists with the new GDPR, there will be no level playing field, consumers will not experience comparable digital privacy online and operators will continue to face this dual compliance regime and their competitive position will be compromised (Telefónica, 2016).

Referring to ‘level playing field’ and ‘competitive’ indicates the use of an economic frame. It welcomes the Commission’s proposal in the regard that it envisages to cover Over the Top (OTT) players alongside traditional telecommunication service providers. This has been overdue considering that OTTs have not been subject to the same strict regulation so far despite the fact that they offer equivalent services.

> Telecommunication service providers are highly regulated as regards the privacy and security, while Over the Top (OTT) players are not regulated the same way for the provision of functionally equivalent services. The problem is not only for consumers but also for the competitivity of the European industry. The uneven application of

> privacy and data protection rules for equivalent services destroys the ability for these players to compete on equal footing in a single market (Telefónica, 2016).

By using words such as 'level playing field', 'competitive' 'industry' and 'market', Telefónica makes economic arguments. It also reflects on the issue of consumer protection. The existing legislative landscape for the protection of personal data shows significant weaknesses. "Currently, European citizens cannot rely on European regulation to consistently protect their personal data and privacy, as different sets of rules are applied to functionally equivalent services, from the user point of view, depending only on the classification of the service provider (according to an old fashioned ECS definition)" (Telefónica, 2016).

Overall, Telefónica used 19 public goods arguments, thereof eleven consumer protection arguments, four crime and security arguments and five human rights arguments. In addition, 14 economic arguments 17 could be identified. Following the procedure that the highest number of arguments determines the overall frame that has been used, Telefónica employed a public frame.

Vodafone

Vodafone is a multinational telecommunications company that provides diverse communications services to consumers and businesses Currently, Vodafone is the largest 5G network in Europe (Vodafone, 2020). Vodafone provided valuable insights into the telecommunication sector's positions towards the prospective revision of the ePrivacy directive. As opposed to OTT such as Facebook who do not support the adoption of a regulation that covers them under the same regulations as telecommunication firms, Vodafone made clear that online service providers urgently need to be included in the new regulation in order to create a level playing field and ensure fair competition.

> EPD has not stood the test of time: While the underlying policy drivers have not changed, technology has advanced and new forms of communications have developed. Currently, consumers have different levels of protection for functionally equivalent services and service providers will face regulatory arbitrage. This has already been recognised in the DSM strategy, where it was stated that rules must be simpler, future proof and must also ensure a level playing field between traditional telecoms companies and new internet players where they compete in the same market and that this must be addressed across the Telecoms Framework, EPD, audio visual media and services regulation and platforms (Vodafone, 2016).

As this argument includes the key words ‘consumer’ in combination with ‘protection’ as well as ‘level playing field’, ‘companies’, ‘compete’ and ‘market’, the use of a consumer protection frame and an economic frame is simultaneously indicated. It further elaborates on the weaknesses of the current ePrivacy rules and its underlying impact for consumers. “The e-Privacy Directive (EPD) has had limited success protecting the confidentiality of communications across the EU for the key reason that, by being too sector & technology specific, it has not kept up with new forms of communications over the internet such as voice over IP or instant messaging. As a result, consumers are subject to different standards of protection for what are in effect the same communication services” (Vodafone, 2016). Through the answers provided, Vodafone also underlines that current security obligations are in fact “sets of overlapping (and not always coherent) legal obligations [which] are confusing, complicated and do not result in better security. Good security is achieved by investing in security engineers, not lawyers” (Vodafone, 2016). Based on the occurrence of the key word ‘security’, this argument exemplifies the use of a crime and security frame.

Vodafone used 19 arguments related to public goods, thereof nine consumer protection arguments, seven crime and security arguments and three human rights arguments. It also stressed 15 economic aspects. Overall, Vodafone employed a public frame as more of these arguments are used than of public goods arguments.