Aalto University
School of Business | Mikkeli Campus

BIG TECH AND ONLINE PRIVACY

How does big tech address privacy regulation and online privacy concern?

Ville Turku

International Business
Bachelor's Thesis
Supervisor: Susan Grinsted
Date of approval: 8 April 2020

Aalto University
School of Business
Bachelor´s Program in International Business
Mikkeli Campus

Declaration

By completing this cover sheet and declaration, I confirm that this assignment is my own work, is not copied from the work (published or unpublished) of any other person, and has not previously been submitted for assessment either at Aalto University or another educational establishment. Any direct or indirect uses of material (e.g.: text, visuals, ideas...) from other sources have been fullyacknowledged and cited according to the conventions of the Harvard Referencing System.

Aalto University
School of Business | Mikkeli Campus

BIG TECH AND ONLINE PRIVACY

How does big tech address privacy regulation and online privacy concern?

Ville Turku

International Business
Bachelor's Thesis
Supervisor: Susan Grinsted
Date of approval: 8 April 2020

Aalto University
School of Business
Bachelor´s Program in International Business
Mikkeli Campus

Declaration

By completing this cover sheet and declaration, I confirm that this assignment is my own work, is not copied from the work (published or unpublished) of any other person, and has not previously been submitted for assessment either at Aalto University or another educational establishment. Any direct or indirect uses of material (e.g.: text, visuals, ideas...) from other sources have been fullyacknowledged and cited according to the conventions of the Harvard Referencing System.

AALTO UNIVERSITY
SCHOOL OF BUSINESS
Mikkeli Campus

ABSTRACT OF
BACHELOR'S THESIS

Author: Ville Turku
Title of thesis: Big Tech and Online Privacy**:** How does big tech address privacy regulation and online privacy concern?

Date: 8 April 2020
Degree: Bachelor of Science in Economics and Business Administration
Supervisor: Susan Grinsted

Objectives
The main objectives of this study were to explore the methods used by big tech – Amazon, Apple, Facebook, Google and Microsoft to manage challenges posed by privacy regulation and consumer online privacy concern. The study also aimed to increase the general understanding of how companies manage online privacy concern.

Summary
This study approached the problem by analyzing public documents pertaining to the management of online privacy concern by the big tech companies. Various kinds of documents were assessed, with qualitative document analysis as methodology, to gain an understanding of the topic. The documents used included, for example, annual reports by the companies, to understand how the companies approach the issue of regulation and the companies' websites, to explicate how the companies communicate to their users about issues pertaining to online privacy and concern thereof.

Conclusions
The results of this study indicate that big tech companies view privacy regulation both as a risk to be managed and an opportunity to be taken advantage of. While the companies expect negative effect from prevalent and upcoming regulation, the companies are proactively taking steps to affect future regulation. Most of the companies also utilize easily understandable communication towards their customers on issues pertaining to online privacy, which would be expected to reduce online privacy concern, however, more research on the subject is required in the future.

Key words: Privacy; Internet; Regulation; Digital Technology; Information Society; Business Ethics

Language: English

Grade:

AALTO UNIVERSITY SCHOOL OF BUSINESS
Bachelor´s Program in International Business
Mikkeli Campus

OUTLINE

Bachelor's Thesis

ABSTRACT

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

This bachelor's thesis aims to tackle the managerial perspective of online privacy concern. The measures used by big tech to manage the increasingly important concern will be examined. In this research project, big tech refers to the five largest companies operating in the tech industry – Amazon, Apple, Facebook, Google and Microsoft.

Lately, big tech has faced increasing scrutiny on their handling of online privacy matters. The increasing scrutiny has manifested, for example, in American politics with democratic presidential candidate Elizabeth Warren calling for a break-up of big tech (Kelly, 2019). Regulatory bodies have also voiced their concerns over issues pertaining to big tech's management of privacy issues (Romm, 2019).

Furthermore, previous literature on the measures which big tech uses to mitigate the privacy concerns of both the general public and the users of their services is quite scarce. Previous literature has rather focused on online privacy concern as a general phenomenon, and how it affects the actions and perceptions of consumers – rather than addressing the management perspective.

1.2 Research Problem

This research will address the knowledge gap in academic literature, relating to the measures used by big tech to manage online privacy concern. The current understanding of online privacy concern mainly relates to the consumer perspective, with a lack of understanding towards the managerial perspective. This research also relates to the public interest, as it should be properly understood how big tech companies manage online privacy concern, before proper critiques can be presented towards them. Therefore, it can be said that there is no adequate academic understanding of how large internet companies manage online privacy concern.

1.3 Research Question

Online privacy concern is manifested both from the side of consumers and regulatory bodies which represent the interest of consumers in the internet economy. Based on this distinction, the two main research questions of this thesis are:

- How do large online tech companies respond to consumers' concerns about online privacy?
- How do large online tech companies respond to regulatory actions concerning online privacy?

These two questions pertain to both the individual and societal factors of online privacy concern. Online privacy concern is considered a detrimental factor to the operations of big tech companies.

1.4 Research Objectives

This research aims to increase the understanding of the measures used by big tech to manage online privacy concern, and for that purpose there are four research objectives to guide the research. The four objectives are:

- To explore the different methods used by big tech to mitigate and leverage consumers' online privacy concern
- To explore the different methods used by big tech to mitigate and leverage the impact of privacy-related regulation

2. LITERATURE REVIEW

2.1 Introduction

This literature review will provide a succinct overview of the current academic discourse on online privacy, mainly from the perspective concerning businesses operating in the internet. The literature review will mostly involve discourse on the impact of online privacy as a subject to businesses, as opposed to the viewpoint of this study itself – the measures employed by big tech to manage online privacy concern.

Big tech herein refers to the largest five technological companies in the United States – Google, Apple, Facebook, Amazon and Microsoft, which will be better defined later.

The reason for the viewpoint of the literature review is the novelty of this study, as the literature on managing online privacy concern is mostly based on theoretical recommendations, rather than how it is managed in practice.

Firstly, dynamic between online privacy and big tech will be discussed. The definition of big tech will be first established based on previous literature, while the follow up will assess the impact of privacy concern on online business.

Secondly, the theory of online privacy, split into “social” and “individual” approaches will be assessed. The section will look into different theories on online privacy, which can be split into the two categories. This section will borrow heavily from fields outside of business, including philosophy, information sciences and social science.

Thirdly, the concerns regarding online privacy will be investigated, both from the consumer and regulatory perspectives. The section will establish the causes and effects of privacy concern. The section will also delve into the dynamic between consumers and the regulatory bodies.

Finally, findings of the literature review will be summarized. The previous topic areas will be presented concisely and gaps in the current literature will be identified. A conceptual framework for the dynamic between online privacy and big tech business will be presented from the perspective of pre-existing literature.

2.2 Big Tech

Big tech has received increasing attention towards their online privacy practices, especially with the recent Cambridge Analytica scandal (Isaak & Hanna, 2008) and other public discussion revolving around data collection. For the purpose of this research, this section of the literature review will establish what is meant by “big tech”, as well as assess the impact of online privacy concern on their business. Despite the

public discourse around these companies, the current state of literature relating to these companies in this context is quite lacking.

Big tech in the context of this paper is defined as the five largest public companies by market capitalization, excluding Saudi Aramco, the "GAFAM" – Google (Alphabet), Apple, Amazon, Facebook, Microsoft. Such a definition has for example been proposed by Smyrnaios (2016), who criticized these companies as being exploitative oligopolies, formed by neoliberal policies. Without agreeing nor disagreeing with Smyrnaios' views on these companies themselves, it is regardless evident that these five companies are powerful actors in the technological space and also very relevant, if for no other reason but the sheer amount of public discourse around the five.

2.3 Online Privacy

As online privacy is a central topic of this study, it must first be examined what constitutes online privacy. Study of online privacy is an interdisciplinary field, with the articles in this section of the literature review belonging to the fields of philosophy, information sciences and social sciences. The focus of this section is on assessing different reasonings for what privacy is, and how it might be violated or protected. Most of the theories use normative reasoning, some of which varies by theory – thus as can be seen in the following subsections, privacy is not a clear-cut topic.

This section will revolve around two prevalent discourses on privacy, which have emerged during the late 20th and early 21st century. The two approaches to be examined are the individual and social approaches to privacy, as per the grouping used by Marcel (2019). Finally, a brief comparison of the two approaches will be conducted.

2.3.1 Individual Approaches

Marcel (2019) describes individual approaches to online privacy as primarily relating to an individual's ability to retain autonomy over themselves. According to them, the individual approach to privacy is based on normative expectations of an individual's "right to be left alone", as originally described by Warren & Brandeis (1890). These

approaches are thus primarily concerned with the relationship between an individual and the preservation of the sanctity of their own information. The individual approaches to privacy also take an ethical universalist approach, as they argue for uncompromised normative rights.

Martin (2016) groups approaches to privacy into three groups: Access-view, Control/Fair information principle (FIP) and Context-dependent norms, the latter of which represents a social approach to privacy. For individual approaches of privacy, the access view and control/FIP approaches are thus relevant to this section of the literature review.

By the grouping of Martin (2016), the access-view represents the original “right to be left alone” definition of privacy. Thus, if a person wants to be left alone, that should be respected with privacy being retained. Martin argues that loss of privacy follows the act of sharing private information about oneself. The original papers cited by Martin to form the grouping of access-view privacy are somewhat connected by the same idea of privacy being fulfilled when one does not share their information, however, the grouping itself is not formulated in the original studies.

The other privacy approach established by Martin (2016) in their study is the control//FIP approach. Unlike the access-view approach, the control/FIP is perhaps better formulated as a distinct theory in privacy elsewhere in academic literature. The same approach appears to be originally formulated by Westin (1967) as cited in Pollach (2005): ‘‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’’. Privacy is thus about being able to control to what extent one’s personal information is shared to others. Similar views have been raised by Parker (1974) as referenced by Moore (2008), who argues that privacy is a normative subject and likewise no definition of privacy will be appropriate by the judgement of everyone.

Thus, the control approach to privacy represents a similar individualistic view to privacy as the access-view approach: both are concerned with the individual’s decisions about their own privacy, as a rational decisionmaker. Even the differences between the two approaches are quite minor. Whereas the access-view approach is more concerned

with participation in information sharing actions compromising privacy, the control approach to privacy concerns “oversharing” one’s personal information. Therefore, the control approach to privacy appears more complete, as it is more detailed.

2.3.2 Social Contract Approach

Social contract approach to privacy is a recent development in privacy scholarship, having emerged in the early 21st century. The approach is a response to perceived inadequacies of individual approaches to privacy. Martin (2016), for example, argues that the individual approaches of privacy lead to misguidance of users on the behalf of online firms, as firms merely try to communicate their best intentions, without fulfilling them. Individual theories of privacy have also been criticized for being overly general and lacking sensitivity for contextual factors (Nissenbaum, 2004).

The social contract approach to privacy has originally emerged from the concept of privacy as a contextual integrity, as originally developed by H. Nissenbaum. in a journal article by the same title. In the model of contextual integrity, privacy should be evaluated in the context of the stakeholders’ norms. The concerns of privacy should primarily be among the stakeholders’ themselves. However, should a participant abuse their powerful position or act in an indecent way, then law and policy should be used to uphold privacy in line with the normative expectations of a community (Nissenbaum, 2004).

The further developed social contract approach to privacy combines the relativist tendencies of the contextual integrity model with some universal principles. The social contract theory of Martin (2016) maintains that privacy should be context-dependent, with a focus on social contracts negotiated in a community. The social contract model of Martin is based on three main principles:

(1) Contracting community focus – Privacy norms are developed by the community
(2) Microcontract norms – Individuals share information about the usage of personal information
(3) Role of contractors – Businesses are expected to promote strong expectations for privacy

The social contract theory of privacy makes a strong case for an ideal community, in regard of privacy, wherein both individuals and businesses have a strong sense of responsibility towards upholding privacy. The social contract theory, as Martin states, can be utilized as an analytical tool for consideration of stakeholders' interest. However, the viability of such model translating into the context of reality seems unlikely, as it would have to be predated by the community being responsible and knowledgeable about privacy. As Martin argues, consumers act irrational in matters pertaining to online privacy, as shown by various other studies. How would those same irrational consumers then be reasonably expected to be the normative gatekeepers of the hypothetical social contract?

2.3.3 Comparing Individual and Social Approaches

The individual and social approaches have both their merits. The individual approach makes a strong case for inalienable, universal right to privacy, while the social is more sensitive to the contextual dimension of privacy.

As scholars supporting the social contract approach have noted, the individual approaches to privacy could be inadequate, due to consumers making uninformed privacy-related decisions. Consistent with this critique, some studies, such as one conducted by Acquisti & Grossklags (2005) exhibits results which imply that consumers are not fully informed of privacy risks pertaining to their online behaviour.

Social contract approaches on the other hand, could be criticized for ethical relativism and compromising the individual perspective. While the supporters of social contract approach to privacy tend to argue for superseding the individual perspective, a recent study by Yeolib et al. (2018) shows that individual differences in online privacy concern vary due to personal factors. With variance in individual differences in concern, shared norms could lead to violation of the individual.

While the individual and social contract approaches appear quite contrary to one another, there have also been attempts in integrating the two perspectives. Such has been argued by Marcel (2019), who proposes that both individual and social

approaches to privacy are necessary for the problems of the digital age. Marcel proposes that individual autonomy must be retained, while the control over flows of information must be assessed according to the previously outlined social approaches, with certain improvements which are beyond the scope of this discussion.

2.4 Online Privacy Concern

Having established the theoretical background of online privacy, what must be understood next is the concern related to online privacy. This section will be split into two separate topics: consumer concern and privacy regulation. While there is a dynamic between these two topics, it makes sense to address them separately for clarity.

2.4.1 Consumer Concern

Online consumer privacy concern has been extensively studied, especially in relation to e-commerce and online advertising business. Ashworth & Free (2006) view internet services usage as a transaction wherein users trade privacy for use of services. They apply the concept of justice to evaluate the transaction. According to their theory, consumer concerns would arise from unjust transactions. The two types of justice expected, according to them are:

- Distributive justice – The transaction is just if the goods received by the firm amount to the personal information given up by the consumer
- Procedural justice – The transaction is just if the prevalent ethical norms are followed

The extended online privacy concern model of Anic et al. (2019) is consistent with the concept of distributive justice. According to the results of their study, the benefits of internet-use exceeds consumers' online privacy concern – which explains why people take part in online transactions and trade their privacy for services.

The study of Anic et al. (2019) also found that individuals' online privacy concern is affected by their computer anxiety and belief in privacy rights, with both factors leading to increased online privacy concern. Their model also notes that privacy concern is affected by the prevalent privacy regulation. However, the study was conducted on Croatian population, and thus there might be differences among populations. The authors also studied whether traditional values and social trust had a connection with privacy concern, but they did not find a link.

Similarly, Yao et al. (2007) found in their study of American undergraduate students that personal belief in privacy rights is a significant cause of online privacy concern. They also found empirical evidence that online privacy and need for privacy in traditional settings are closely connected, with belief in privacy rights being a mediating variable between need for privacy and online privacy concern.

A study was also conducted on another set of undergraduate students in Hong Kong by Yao & Zhang (2008), replicating similar results in terms of the relationship between privacy rights belief and online privacy concern. The study found additionally that more frequent internet use was associated with larger online privacy concern, while internet use diversity was associated with less concern. The results seem unintuitive and contradictory to the earlier 2007 study by Yao et al., wherein internet use diversity was associated with stronger belief in privacy rights, mediated by internet use frequency.

Online privacy concerns are also found to develop over time. Goldfarb & Tucker (2012) studied market research from 2001 to 2008 and discovered that refusals to respond to some questions had grown over time and that older people were more likely to refuse answering. As they state, however, the results cannot be necessarily generalized due to the survey limitations and possible shifts in demographics. Despite that, they posit that their survey could stand as evidence of increasing privacy concern over time. Noteworthy is also that they do not specifically address online privacy concern, but as shown before by the results of Yao et al. (2007), online privacy concern is closely related to privacy concern in general.

Actions from firms and regulators can also influence online privacy concern of individuals. Wirtz et al. (2007) found that online privacy concern can be mitigated both

with organizational and public policies, through the consumers' perception of regulation. Notable is that it was not the direct effects of regulation that Wirtz et al. studied, but consumers' attitudes towards regulation. According to their results, consumers might withhold, fabricate and take additional protective measures towards their information if they think that their privacy is being violated. The study was conducted only on US citizens, however a study of Lancelot Miltgen & Smith (2015) also found that perceived regulatory privacy protection led to smaller online privacy concern among UK citizens.

High quality communication and low sensitivity of information asked can also mitigate online privacy concern, according to Lwin et al. (2016). They found that requests of high sensitivity information lead to previously described protective measures for information disclosure, mediated by online privacy concern. The same hypothesis was tested with communication quality, but no support was found at a significant level. Nevertheless, the study confirmed again that online privacy concern leads to protective measures overall.

2.4.2 Privacy Regulation

Acting upon the privacy concerns of consumers, privacy regulation has gained increasing weight in public discussion. This section will succinctly explore the concept of privacy regulation, without going into too much detail with privacy regulation, as regulation varies by geographical areas. Based on the findings from the previous section, privacy regulation might influence online privacy concern through consumers' perception of regulation.

Current literature focusses on the effects of privacy regulation, especially in terms of the effectiveness of regulation to online privacy concern. A recent conference paper by Degeling et al. (2019) provides empirical evidence of the effectiveness of privacy regulation. The study found positive changes in large companies' online privacy policies consistent with the deadlines set by the European general data protection act (GDPR).

Whitman (2004) makes a point that privacy norms vary greatly across societies, thus it would be unrealistic to assume that Americans and Europeans, as an example, would accept the same kind of regulation as one another. The implication from this viewpoint is that not only will regulation vary across geographical borders, people in different societies will also have different expectations towards privacy, despite the global outreach of internet services.

Regulation also varies in form, as per the regulatory framework provided. The main two forms of privacy regulation are government and self-regulation. Both of these forms can be observed in Western countries, with regulation in the United States largely relying on industry self-regulation by third party certifiers while the European model relies on strong government regulation (Walsh et al., 2017).

While regulation should, if crafted to match the privacy expectations of the individuals in a community, lead to decreased privacy concerns, there might still be downsides to regulation. Fuller (2018) argues such a point, by positing that privacy regulation would be akin to a price control. Their logic is that if the ability of companies to collect private information were to be restricted, the companies would thus lose a portion of revenue accrued therefrom, thus setting a price control on their services. According to their argument, the overall welfare of consumers could be reduced as a result of privacy regulation, because price controls are generally seen as welfare-reducing by economists.

Similar concerns are raised by Campbell et al. (2015). Their model predicts that introduction of privacy regulation could lead to concentration of market in the hands of larger companies and reduce competition. Additionally, regulation could have the further effect of reducing product quality according to them.

2.5 Conclusions

Big tech was defined as the five largest public companies by market capitalization, excluding Saudi Aramco, which are Google, Apple, Facebook, Amazon and Microsoft. These companies have faced scrutiny for their large market power and business

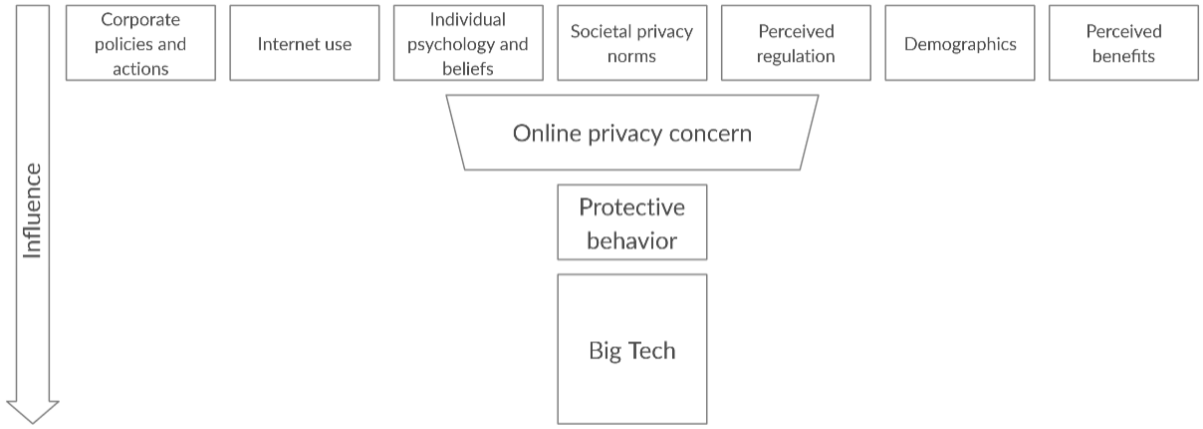
practises. Nevertheless, the literature relating to this aspect of these companies was found to be sparse.

The theory behind online privacy was examined. The theoretical approach to online privacy was split into two main discourses: individual and social contract approaches. It was determined that both approaches have their merits and drawbacks. The individual approaches support a notion of strong personal autonomy and universal ethical rights, without accounting for the social context of privacy. The social contract approaches are sensitive to the social context of privacy but lack the strong moral protections for privacy.

Online privacy concern was found to arise from a multitude of causes and be closely related to the concept of justice, as perceived by consumers. Online privacy concern was found to be a cause of both personal features, but also social factors relating to industry and government regulation of privacy. Privacy regulation was found to have merits in terms of improved privacy; however, drawbacks were also found, especially in terms of economic welfare and competitiveness of the internet. It was also found that privacy regulation tends to vary across societies, due to different expectations towards privacy and regulation thereof.

2.5.1 Conceptual Framework

The conceptual framework in this section will support the main research of this study. The framework is built upon the three sections of the literature review, focusing on the drivers of online privacy concern. The framework presents the direct relationship between online privacy concern and big tech – online privacy concern leads to protective measures on behalf of the users, which are expected to exert a negative influence on big tech. The second part of the study will focus on the measures undertaken by big tech to manage the variables at the top of the model.



3. METHODOLOGY

3.1. Qualitative Document Analysis

A qualitative research method was chosen to supplement the exploratory nature of this study. Despite most business research utilizing quantitative methods, qualitative research methods have many uses, namely the development of new theory (Suranga & Kalsi, 2015). As this study deals with a novel topic area, a qualitative method was considered the best option. Therefore, the focus is on understanding the measures used by big tech to manage online privacy concern, rather than trying to quantitatively assess the usage of the measures.

Furthermore, a document analysis method was chosen for the study, mainly due to the potential difficulty of obtaining any useful data by, for example, interviewing representatives of the companies. For big tech, privacy is evidently also a matter of public relations, thus it could be assumed that no meaningful data beyond the publicly available could be collected from there. Document analysis was determined to be useful as a method, for clarifying, from publicly available sources the methods which big tech use to manage online privacy concern.

Qualitative document analysis is an emerging research method, which tackles a research problem in a way like thematic analysis, allowing the researcher to identify themes from the source material, which can then be further developed through the use

and analysis of different documents (Bowen, 2009). Inferences were made from source texts through the interpretation of the author of this study, both through deductive and inductive reasoning. According to Azungah (2018), deduction can be used to relate findings to previous literature while induction can be used to discover new themes from research material. In this study, deduction serves as a tool for explaining online privacy concern management with previous research as a basis, while induction serves the purpose of identifying new theoretical relationships.

Document analysis is highly dependent on the selection of documents to be assessed, as the selected documents act as the foundation for the research. The selection criteria and reasoning for the documents which were considered are further detailed in the following section.

3.2. Data and Collection Methods

Documents were selected for the research based on both inductive and deductive reasoning, as previously described. This combination allows for discovery of new information, however, with the potential fallback of researcher bias – as researcher judgement is at the centre of the document selection. The two separate selection criteria for the documents were, based on the research objectives:

- The document should explain how big tech addresses privacy concern
- The document should explain how big tech addresses privacy regulation

Documents were selected from online sources, through search engine. The documents were interpreted as they were. The types of documents chosen included:

- Webpages
- Annual reports
- Trade research
- Databases
- News articles
- Opinion pieces and other similar writings

4. FINDINGS

4.1 Introduction

This section will assess the inferences made from the data. The findings will be split into different subsections, based on the themes identified from the source documents. The source documents include various website sources, previous trade research and financial disclosures. The full bibliographic detail of the sources is available in the reference list at the end of this paper. Previous trade research and similar documents are explicitly cited in text, while the rest of the findings are paraphrased from the source documents. Additional detail and the sections of the findings which each document relates to will be laid out in the appendix 1.

4.2 Lobbying and Advocacy

According to a previous report compiled by vpmentor.com (n.d.), privacy is among the most significant lobbying issues among big tech in the United States. The data compiled by vpnmentor.com from lobbying reports submitted to U.S House of Representatives since 2005 was summarized in table 1.

Company	**Proportion of lobbying reports mentioning privacy**	**Rank of topic "privacy" as a mention among ten select topics in lobbying reports. 1 = most frequent topic, 10 = least frequent topic.**
Amazon	25%	2
Apple	45%	3
Facebook	61%	1
Google	64%	1
Microsoft	43%	2

Table 1: Lobbying reports submitted to U.S. House of Representatives by Big Tech since 2005 pertaining to privacy. Sourced from vpnmentor.com (n.d.).

The data indicates, that privacy is the foremost lobbying issue among big tech, in terms of frequency among Facebook and Google in the United States. Among the other three companies, privacy is also a key issue, ranking higher than most other key issues as outlined in the report. The report does not make statements about the attitude of these companies towards privacy issues, but rather just shows that privacy is considered an important issue.

In the United States, most of big tech is represented by Internet Association (IA), lobbying organization “representing the interests of the internet economy”. Members from big tech include Amazon, Facebook, Google and Microsoft, out of which all but Microsoft are founding members. The group directly advocates their views to policymakers in the United States.

IA tries to partake in the legislative process for privacy regulation. The organization seeks a federal, unified framework for privacy legislation. According to the group, the legislation should be made as simple as possible and be applied consistently. Emphasis is placed on meeting the “reasonable expectations” of consumers towards privacy and protecting them from harm.

Despite the calls for regulation, the statements of IA also place a lot of emphasis on the role of internet companies’ role in ensuring adequate protections of privacy. They note, that their member companies have already acted transparently and provided privacy controls to their users. As they also argue for a standardized regulation across the board, they posit that the regulation should be contextually applied – it should be based on performance standards, not prescription and the case-by-case protections of privacy should be grounded in risk assessment. Thus, while IA calls for privacy regulation, a lot of judgement would be placed in the hands of the companies themselves.

According to data sourced from the EU lobbying database lobbyfacts.eu, it was found that most of the big tech engage in privacy lobbying in Europe. The data available at LobbyFacts is sourced directly from EU official governmental bodies. The data pertaining to big tech and privacy obtained from LobbyFacts.eu is compiled in table 2.

Company	How many times the words "privacy" or "e-privacy" were included among the topics of lobbying meetings with European Commission	Total amount spent on lobbying overall, in Euros (€)
Amazon Europe Core SARL	0	1 750 000 - 1 999 999
Apple Inc.	8	2 000 000 - 2 249 999
Facebook Ireland Limited	20	3 500 000 - 3 749 000
Google	17	8 000 000 - 8 249 999
Microsoft Corporation	13	5 000 000 - 5 249 999

Table 2: Privacy-related lobbying and total amount spent on lobbying by big tech towards European Commission. Sourced from LobbyFacts.eu (n.d.).

Based on the data presented above, every one of the big tech companies except Amazon has directly lobbied the European Commission on issues pertaining to privacy. All the companies have spent significant monetary amounts on lobbying, with Google clearly distinguishing themselves among the group. Noteworthy is, that these lobbying figures do not include the possible lobbying by consultancies, trade unions and other actors alike which could represent these companies. The monetary amounts specifically spent on privacy-related lobbying are also not disclosed.

4.3 Regulatory Compliance

Regulatory compliance was found to be a focal point for the management of online privacy concern for big tech. Specifically, the annual reports of each of the big tech companies mentioned risks associated with privacy regulation and precautions which the companies are taking to mitigate the adverse effects from privacy regulation towards them. Annual reports were reviewed for this section, as companies are often unwilling to disclose their risk management positions to the public in other ways. The

annual reports were sought using U.S Securities Exchange Commission's EDGAR database.

Central concern of the companies are the adverse effects which they face from privacy regulation. The risks mentioned by the companies were summarized in table 3.

Company / Risk	Alphabet (Google)	Amazon	Apple	Facebook	Microsoft
Fines and penalties	X	X	X	X	X
Product and service changes	X	X		X	X
Decreased service usefulness or attractiveness	X		X		
Decreased service demand or availability		X	X		
Having to change business operations and practices	X	X	X	X	X
Impediment of product development	X			X	X
Increased costs	X	X	X	X	X
Civil and criminal litigations	X	X	X	X	
Diversion of management resources	X			X	
Negative publicity	X	X	X	X	X

Adverse operational or financial impact	X	X	X	X	X
Increased regulatory oversight	X			X	
Inability to target advertising	X			X	

Table 3: Risks recognized by big tech companies relating to privacy regulation. Compiled from the 2019 Annual report form 10-Ks of Alphabet, Amazon, Apple, Facebook and Google.

There are numerous risks which all the companies have noted in their reports, however differences in recognition exist. The most common negative impacts relate to increased costs, changes of business practices, litigations, adverse operational or financial impacts and penalties. Interestingly, Microsoft did not mention litigations explicitly in relation to privacy as did the other companies. Negative publicity was also mentioned by all the companies. Overall, the risks were stated in very nonspecific terms and these companies did not link the risks associated with privacy regulation to explicit, concrete examples.

Most of the companies apart from Apple mentioned having to change their products and services as a risk. Apple mentioned, however, in addition to Alphabet, that regulatory actions might lead to decreased service usefulness or attractiveness. Like Apple, Amazon also recognizes the risk of decreased service demand or availability arising from regulatory actions.

Impediment of new product development, denoting either inability or increased difficulty of deploying new products was mentioned by Alphabet, Facebook and Microsoft. Diversion of management resources, increased regulatory oversight and inability to target advertising were something which only Alphabet and Facebook mentioned.

The companies anticipate unintended causes, which could compromise the privacy of their users. These include, for example, data breaches which would be a cause of privacy concern despite it not being the companies' intention to compromise the users' data. Third parties are also considered a risk, when dealing with users' private data. Facebook for example mentions of a prior case (Cambridge Analytica) in which, according to them, some data was unintentionally accessed by the other company they were offering data access to. Such events also present a regulatory risk for the companies, as the companies could be held liable for compromising the liability of their clients, despite even their best intentions to not have that happen.

In addition to present regulation, the companies expect uncertainty in the regulatory landscape pertaining to online privacy. Regulation could develop in a way, which would introduce additional requirements for the companies. The companies also posit, that the interpretation of present laws could change or be applied in a novel way, which could not be expected. International and state differences are also seen as a cause of ambiguity in complying with privacy regulation, as different jurisdictions have divergent rules on privacy regulation. For example, EU has recently put into effect the General Data Protection Regulation, which has been a major undertaking for big tech to deal with. Other similar regulatory reforms are taking place which have been noted by the companies, such as California Consumer Privacy Act and Brazilian General Data Protection Law.

It is also postulated by the companies, that due to their size they could be targeted by extensive scrutiny from regulators. Thus, the companies would have to act above the expectations set by present regulation. Likewise, the companies argue that their size makes it challenging act in accordance with regulation, due to the unprecedented scope of their operations. The companies are expecting, for example, targeted privacy audits from regulators towards privacy practices. To manage the effects of privacy regulation, most of the companies claim to be investing to make their services more private.

4.4 Market Positioning

Big tech provides the most popular products and services in their respective market segments. The *Best Global Brands 2019* -report (Interbrand, 2019) lists big tech among the following ranks in their global brand ranking, based on the brands' role in the market, the strength of the brand and their financials:

- Apple – 1st
- Google – 2nd
- Amazon – 3rd
- Microsoft – 4th
- Facebook – 14th

These rankings represent the relative strength of these companies in the global economy, which implies that these companies have significant market power.
The products and services of the companies also hold significant shares of their respective market, thus incurring potential drawbacks, such as switching costs to users interested in using competing companies' products and services.

Furthermore, secondary sources were assessed to find the market shares of big tech companies in their respective fields of business. Due to the wide-ranging operations of the companies, only their central products and services were considered (see table 4).

Market	Product / Service	Market Share	Company
Search Engines	Google	91.98%	Google
	bing	2.55%	Microsoft
Consumer Operating Systems	Android	38.61%	Google
	Windows	34.96%	Microsoft
	iOS	15.63%	Apple
	OS X	8.3%	Apple
Mobile Phones	iPhone	27.03%	Apple
US e-commerce	Amazon	37.30%	Amazon
Social Media	Facebook	64.99%	Facebook
	Instagram	8.54%	Facebook
	YouTube	3.1%	Google

Table 4: Market shared of big tech's products and services in select markets. Sourced from statcounter.com (n.d.) and emarketer.com (n.d.).

These statistics demonstrate the large economic power which big tech hold in their respective consumer markets, leaving consumers with quite few viable alternatives to choose apart from big tech's products.

4.5 User Privacy Information and Controls

Different big tech companies were found to have both similar and dissimilar approaches to informing their users about information pertaining to their online privacy and allowing their users to control their private information. For this section of the findings, various consumer privacy-related webpages of the big tech companies were reviewed. Overall, most of big tech was found to inform their users about their privacy practices in a clear and understandable way.

Google has a "Safety Centre" webpage to inform their users about the handling of private information. The webpage posits that the collection of data leads to improved services and is collected because of that. A point is made, however, that Google always informs what data is being collected and how and why it is being used.

Furthermore, it is said that users can control themselves how their private information is used. The webpage and all subpages of it address the user personally and employ colourful infographics and cartoony human figures in addition to the text body (see figure 1).

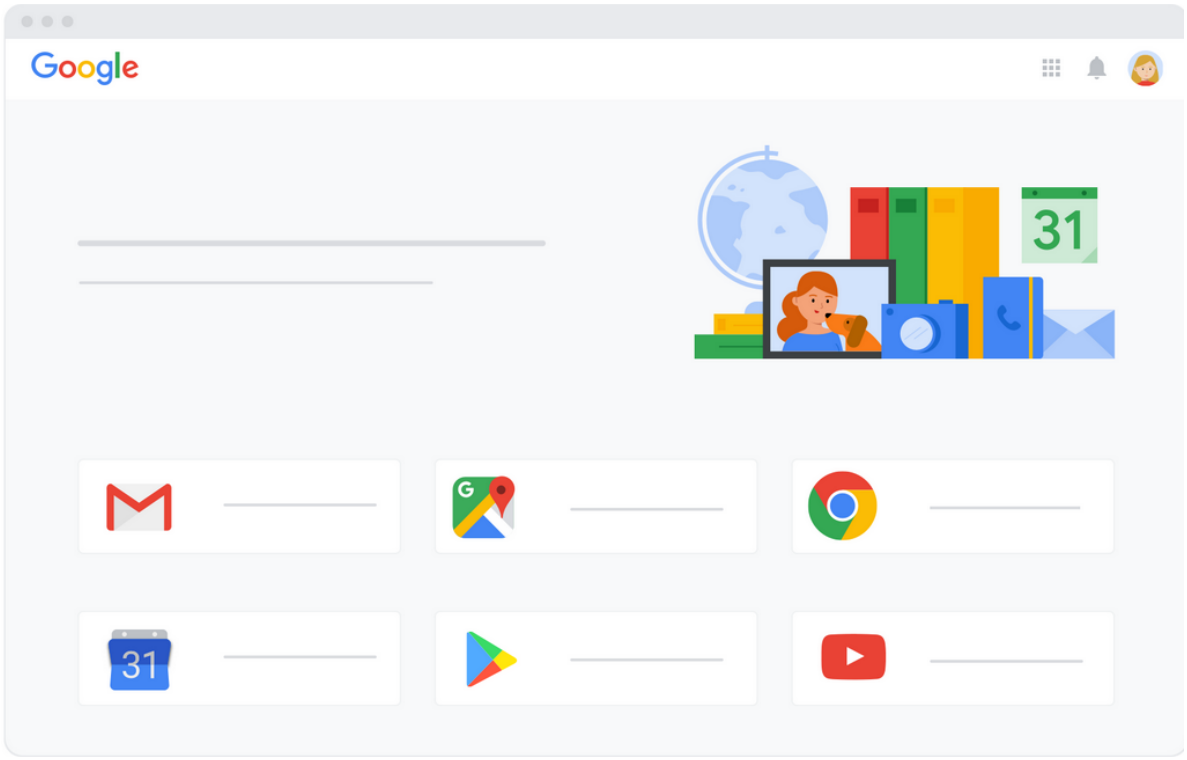


Figure 1: An example of infographics used on Google's Safety Centre (safety.google.com/privacy)

Noteworthy is, that upon trying to access one of the subpages of the English *privacy.google.com*, the author of this study was redirected to *safety.google.com*, in Finnish which was slightly different from the original page accessed in terms of the different subpages. Even after tweaking their language settings, the author of this study could not access *privacy.google.com* in its entirety and had to thus review *safety.google.com*, in Finnish. This possibly implies that Google communicates differently to users about privacy in different countries, although this remains unverified.

On the subpage "Transparency", Google gives examples of data collected by their services and purposes for which the said data is used. Examples include automatic filling of Google Searches, fast pathfinding in Google Maps and discovery of interesting

content in YouTube. Throughout the webpage, a positive tone is displayed, with most of the content being placed under the header “We make Google’s services more useful with data”. A small paragraph is kept under the header “Data protection is at the forefront of our products”, which states that data protection is in a central position in product development processes at Google, all the way from design to product management.

Another subpage about “Data Protection Control” informs the users about the possibility to personalize their privacy settings with “efficient and easy data protection tools”, to control what data is collected and used by Google’s services. The control options allow users to quite precisely select which services can use which data and for what purposes – for example, a user can select that their recent actions on their Google account should not influence the personalized advertisements that they receive. It is also possible for users to review, export and delete their private information. To make things easier, there is a possibility for a “Safety Check-up” to review one’s safety settings quickly, in a few minutes.

On the final subpage “Advertisements and Data”, the first header posits that Google doesn’t sell private information to third parties. On the page, Google details how the personalized advertisements work. The company posits that the use of data collected by using Google’s services makes the advertisements more useful, while privacy of their users remains protected due to anonymization of information. The company also states that users can opt out of advertisements they don’t want to see and that they can also review on what basis different advertisements were selected to be displayed to them.

In addition to the Safety Centre, Google also has a “Privacy & Terms” subpage which details in more specific terms how users’ private information is handled. The subpage further links into “Privacy Policy”, the aforementioned “Safety Centre”, “Google Product Privacy Guide” and “Our Privacy and Security Principles”. The privacy policy lays out the legally required privacy policy, in very legal and specific terms. The section has however been made been accessible to users and supplemented with infographics as with the Safety Centre. The privacy policy also has direct hyperlinks into the previously posited privacy control options. The product privacy guide provides specific details

about the privacy controls that are available to users in Google's different products. Finally, the privacy and security principles presented by Google are the following:

1. Respect our users. Respect their privacy. – Paying consideration to data collection, the use of said data and the protection of it.
2. Be clear about what data we collect and why. – Being transparent in making the information "available, understandable and actionable".
3. Never sell out users' personal information to anyone. – Data is collected for Google's services and advertising purposes, not to sell it to third parties.
4. Make it easy for people to control their privacy. – Users should have the personal choice for appropriate privacy settings.
5. Empower people to review, move, or delete their data. – Users should retain full control over their data whenever and without specific reasons.
6. Build the strongest technologies into our products. – Safeguarding users' privacy with latest technology.
7. Lead by example to advance online security for all. – Google considers itself the pioneer in online security and shares their knowledge with other organizations.

Additionally, Google informs their users about Government requests for information at *transparencyreport.google.com*, a webpage which specifies the amount of government requests for private information which Google can disclose. Users can view per country yearly data on the amount of which type of requests were received and the percentage of requests were supplied with some data.

Like Google, Apple has a page dedicated to privacy, *apple.com/privacy,* with robust explanation about their privacy practices. The page is clean in appearance and starts by explaining that privacy is a fundamental human right and a core value at Apple. The page starts by giving examples of Apple's applications and how privacy is a consideration in them. The examples include, for example, the anonymity of location history in Maps-application, the privacy of personal messages in iMessages and the delivery of news based on interests, not identifier in Apple News. The text body is supported by graphical animations with convergent messages (see figure 2).

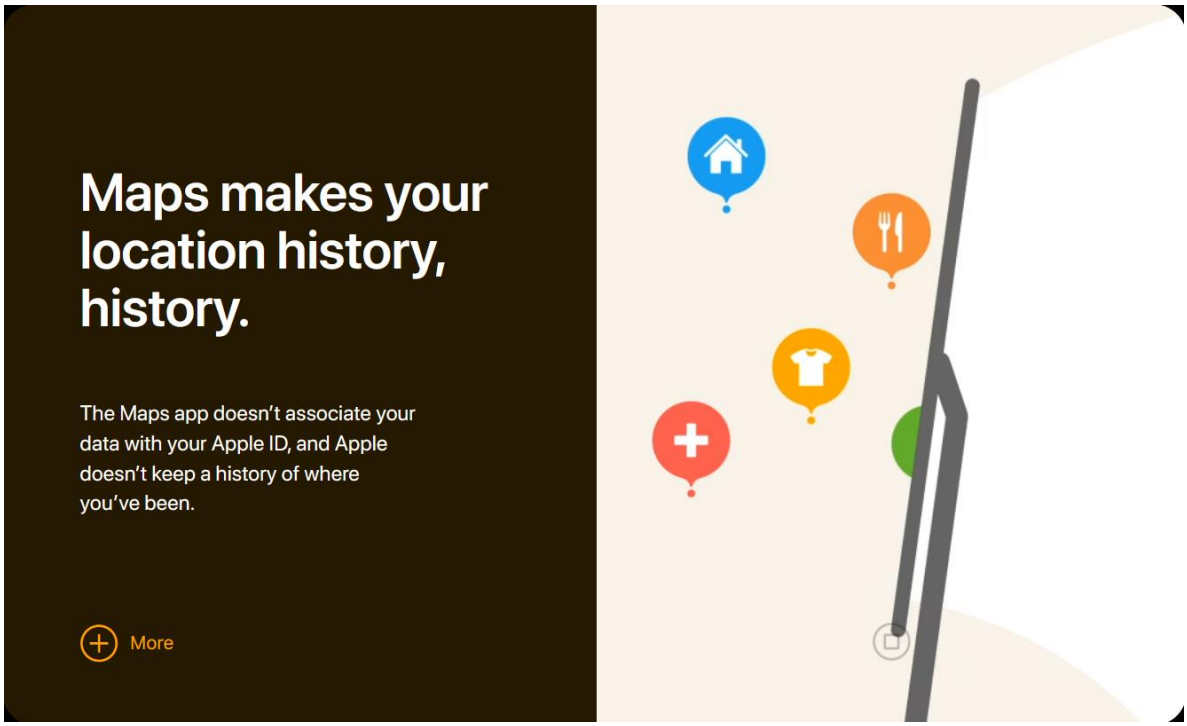


Figure 2: Still image example of the supporting graphical animations utilized on Apple's privacy-webpage (apple.com/privacy)

The "Features" subpage of Apple's privacy webpage starts with a statement consistent with the ones on the main page – "We're committed to protecting your data". A point is made about Apple's products using innovative technologies and minimizing the accessibility of data to others, to maximize privacy. The page then goes on to list features of Apple's apps which uphold the privacy of their users. The page essentially expands upon the points posited on the main page, with further information. Each of the applications listed has their own list of privacy features, which appear to be built and considered for the purpose of the specific application. For example, the iMessages application is stated to utilize end-to-end encryption. It is also stated that the iMessages application cannot access users' conversations and contacts. Furthermore, it is stated that while the messages are backed up on Apple's servers on iCloud, it is possible to turn off the feature.

Further down the "Features" subpage, Apple lists five ways in which they protect their users' privacy:

- Data minimization – Collecting as little data as possible, not maintaining profiles of their users

- On-device intelligence – Processing as much information as possible on the users' devices, so information doesn't have to be sent to Apple's servers
- Transparency and control – Informing the users about the usage of their private data and letting the users control the collection of said data
- Protecting your identity – Anonymizing the identity of data which must be sent to Apple's servers for processing
- Data security – Combining hardware, software and services designed for privacy to uphold data security

On Apple's "Control" subpage of the privacy webpage, Apple further explains about the possibility of controlling one's sharing of private information with Apple. A point first made about securing one's device from unintended users, by measures such as two-factor authentication and face identification. The webpage then explains the settings which can be used to control one's private information, which appear quite similar to the previously explained Google's "Privacy tools". The settings include the ability to select the data that is shared, with the possibility to download and delete the said data. Personal advertising can also be tweaked as with Google. As a final note, the webpage makes a point about the possibility of malicious attempts by third parties to phish users' private information, through e-mails and text messages, for example.

Apple also provides a "Transparency Report" on another subpage, which details the different types of information requests made by governments across the world about private information on Apple's users. The webpage allows users to view which type of information requests which governments made, how many identifiers (users) the request concerns and for how many of those requests Apple supplied with the otherwise private information of their users. For example, a report on the page shows the requests received between January – June 2019 from the Finnish government (see table 5).

Requests for Customer Data

Request Type ⊕	Requests Received ⊕	Identifiers Specified in Requests ⊕	Requests where Data Provided ⊕	Percentage of Requests where Data Provided ⊕
Device	5	1,100	5	100%
Financial Identifier	2	2	1	50%
Account	10	17	9	90%
Emergency	0	-	0	-

Table 5: Apple's Customer Data Requests from the Finnish government between January – June 2019 (https://www.apple.com/legal/transparency/fi.html)

In addition to the other subpages, the privacy section of Apple's website also links into privacy policy as a subpage, which contains the legally required privacy policy in more specific and legal terms than what is presented in the more readable format in the formerly presented webpages. The privacy policy links into some specific pages where Apple's users can change settings related to their personal information.

Microsoft was found to have a similar "Safety Centre" as Google, carrying the same name. As was the case with Google, there is also a possibility of Microsoft changing some information on their webpage, depending on the geographical location of the user. The author of this study, for example, tried to change the localization of the webpage to American English, which caused a hyperlink to "EU Compliance DoCs" disappearing from the webpage. The webpage itself was reviewed as the Finnish version, for the purpose of consistency with the other webpages reviewed.

Microsoft's Safety Centre has the picture of Satya Nadella, the CEO of Microsoft at the top. Next to the image is the statement "Your own information improving your user experience – in your own control", implying similar things as the statements presented by Google – user data improves their services and the users should have control over their private information. The first section of the webpage is titled "Satya's' Bulletin", implying that the statement is directly attributable to the CEO of Microsoft. The beginning of the statements concerns the same overarching themes as Google and Apple have posited – intelligent services and personalized technology, with consideration towards users' privacy and users' own control over their private information.

Next up on the page, Microsoft presents their six key principles for privacy, which are:

- Control – Users can easily control the use of their private information
- Transparency – Users can make decisions based on transparent collection of personal information
- Data security – The personal data of users is protected with appropriate technology
- Strong legal protections – Microsoft respects local privacy laws and privacy as a human right
- Other than content-based personalization – Microsoft does not use personal information to personalize advertisements
- User's benefit – Data is collected to benefit users

After the notice, Microsoft gives examples of the most commonly collected information, explained with small paragraphs complemented by images (see figure 3), showing mostly cartoon human figures doing daily routines. The page addresses the user personally in a light, personal tone. Under the paragraphs, there are hyperlinks available for further and more detailed reading on the subject. The examples include, among others, the locations visited by Microsoft's users, login and payment information and diagnostics information about Windows 10 usage. For each of the categories, examples are given about the users of the information. For example, Windows 10 usage information enables Microsoft to "care about your data security and continuously improve your user experience". Further down the page are specific links to change privacy settings in different Microsoft products, such as Office and Skype.

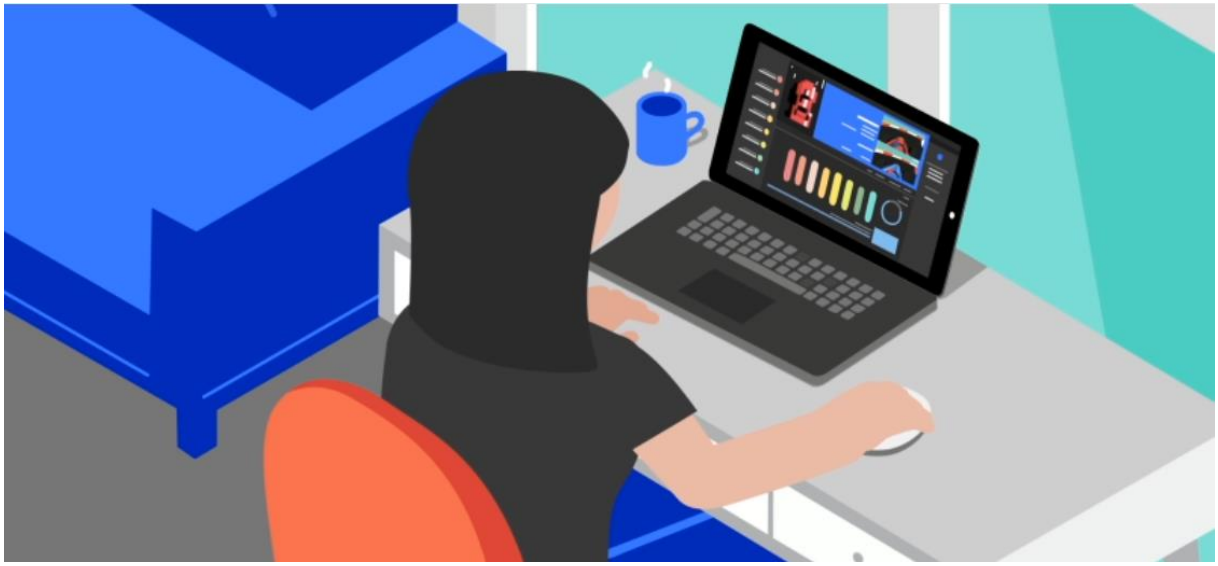


Figure 3: Example of complementary images on Microsoft's Safety Centre (privacy.microsoft.com)

In addition to the commitment to privacy presented on the main page, there are various links for further reading on privacy and control of private information in Microsoft's services.

Firstly, there is a link available to a privacy dashboard which allows users to change their privacy settings pertaining to their Microsoft account. Additional guidance is provided on the same page for changing the privacy settings of various Microsoft's products and services.

Secondly, privacy policy can be accessed from the same page. The privacy policy consists of specific and legal terms, which further detail the statements as presented on the main page of the Safety Centre.

Thirdly, there is a page for government data requests as with Apple and Google. The data is presented in a similar format, with data being available either by country or region and by specific time periods. The number of requests, users/accounts specified in the requests and the type of disclosures is specified.

Fourthly, there is a link to Microsoft's "Trust Centre" which has further reading on the topic of privacy. The subpage covers the following topics:

- How users' data is protected in the cloud
- How Microsoft complies with GDPR
- What are Microsoft's privacy principles
- How Microsoft manages data
- Additional documentation on privacy-related matters

Finally, Microsoft provides a privacy report which again further elaborates on the topics covered on other areas of the webpage, with more specific figures, such as the number of unique users who have visited their privacy dashboard.

Facebook, unlike the companies mentioned before, does not have a specific privacy section on their webpage. Rather, Facebook informs their users about the handling of their private information in their "Help and support centre". Unlike the other companies, Facebook does not make a point on the webpage about the privacy of information towards Facebook and the potential third parties with which Facebook shares the information. Rather, privacy is posited by Facebook as the ability to control the visibility of one's private information towards other Facebook users. This is exemplified by the link to "Safety Check-up", which concerns the sharing of one's information with the "people you want". The only thing mentioning the sharing of information with third parties is the "checking and removal of recently used other companies' applications and sites to which you have logged in with your Facebook credentials". The help page further links into other help pages concerning the specifics of controlling the visibility of one's private information in Facebook.

As with other companies, Facebook provides a privacy policy for detailed information about their privacy practices, accessible separately at *facebook.com/privacy*. Unlike other companies, Facebook only details their privacy practices in their privacy policy. The privacy policy is laid out as a text-only document, with links to some relevant help articles.

Amazon was found to have divergent information about privacy across geographical regions. As with Facebook, Amazon only supplies privacy information in the form of help articles and a privacy notice. For the purpose of this study, the Amazon.co.uk and

Amazon.com webpages were reviewed, representing the US and UK versions of Amazon, as no Finnish version was available for full consistency. Both versions have an article in the help database with the title “Security & Privacy”, however the content differs quite significantly. For example, in the US version under the “Privacy” header are the following links:

- Amazon & My Data
- How Do I Request My Data?
- Amazon.com Privacy Notice

Whereas in the UK version the following links are displayed:

- How Does Amazon Use My Data?
- What Data Does Amazon Collect And Use?
- How Does Amazon Keep My Data Secure?
- Amazon Digital And Device Privacy Settings
- How Do I View And Manage My Data On Amazon?
- How Do I Request My Data?
- Amazon & My Data

The help articles, as is the case with most other of the companies, apart from Facebook, detail the collection of personal data and the uses of it in clear terms for users. Examples are given, such as, that the data allows Amazon to “handle your orders and payments, deliver your items and provide you with the right services”. The language addresses the user as “you” personally, however it is quite formal and legal-like. Overall, the articles presented in the help database of Amazon read more like a privacy policy, rather than information which would inform the common user in clear and concise way about the handling of their private information and their ability to control it. The “Privacy Notice” of Amazon is a standard privacy policy presented in a plaintext format in a very legal-like text with hyperlinks to the help articles mentioned before.

4.6 Executive Communication on Privacy

CEOs and other top executives are a significant part of the public image of the big tech companies, and thus their statements might be considered to represent the views and interests of their respective companies, even if the executives do not explicitly state so. That being the case, this section of findings describes some recent public statements made by tech company executives regarding online privacy.

In an interview with ABC News (Yang & Scott, 2019), Tim Cook, the CEO of Apple, proclaimed that online privacy has become a major societal issue. In the interview, Tim Cook had established that Apple's users are "not their product" and that the company is an ally of consumers in the protection of their privacy. Furthermore, in opinion piece previously published in Time Magazine earlier the same year (Cook, 2019), he called for "the U.S. congress to pass comprehensive federal privacy legislation". In the same piece, he outlined four rights which should be covered by the legislation:

- Right to have personal data minimized
- Right to knowledge
- Right to access
- Right to data security

Facebook's CEO, Mark Zuckerberg also shared his vision for the privacy-related matters for Facebook in 2019. In his note (Zuckerberg, 2019), published on Facebook's website, he acknowledges the bad reputation that Facebook holds on user privacy and posits that the company will improve their privacy practices. The vision for the company's private future is built on six key principles, which are:

- Private interactions
- Encryption
- Reducing permanence
- Safety
- Interoperability
- Secure data storage

Similar communications have been made on behalf of Google. Also, in 2019, the CEO of Google, Sundar Pichai wrote an opinion piece for New York Times (Pichai, 2019),

reiterating the main points of communication made on behalf of the company – data is collected to improve services and it is protected. In his piece, he reiterates Google's views towards online privacy as presented on their own webpage. Additionally, he argues that privacy should "be equally available to everyone in the world". Pichai posits that while legislation will be helpful in ensuring privacy, companies should be leading the charge.

Microsoft's President Brad Smith has also posited in an event in 2019, that privacy is an emerging issue that needs to be addressed. Smith presented that data should belong to individuals and that data should become more open and accessible, to avoid few large companies amassing extensive wealth and economic power. Smith also noted, that customers' privacy concerns have recently shifted from governments' abuse of private information towards abuse by companies (news.microsoft.com, 2019). Microsoft's CEO, Satya Nadella has also argued in favor of privacy, calling for "data dignity" and transparent data privacy laws at World Economic Forum 2020 (Chowdhury, 2020)

Amazon was found to differ from the other big tech companies in the sense, that no meaningful comments were found to have been made regarding privacy by their high-level executives.

5. ANALYSIS

5.1 Regulation

Regulation was found to be a major concern for big tech, with possible adverse effects for the companies including financial liabilities, added costs, regulatory scrutiny, decreased innovation and brand damage. For some of the companies, such as Facebook, some of these effects have become manifested already.

Regulation is viewed as both a local and international issue by the companies, ranging from the present to the future. The companies assume that there will be developments

in privacy regulation across the globe, which is a cause for uncertainty towards the future among the companies.

Compliance with regulation is not viewed only as a matter of the companies' own actions, but also as a matter of unintended events, such as data breaches. Such cases have previously manifested, for example, in the case of Facebook.

The companies utilize various measures to avoid adverse effects from privacy regulation. Most importantly, the companies try to comply with the pre-existing privacy regulation to avoid the detrimental effects from noncompliance. The companies take steps to reduce uncertainty by observing the changing regulatory landscape and by adapting to it. Internal controls and processes are used to reduce the risk of unintended noncompliance.

In addition to direct management efforts towards complying with privacy regulation, the companies engage in lobbying and political advocacy, both on their own behalf and through intermediaries, such as Internet Association. Privacy was found to be a key issue in the lobbying efforts of these companies. In addition to lobbying, key figures, such as all of the five companies with the exception of Amazon, have clearly taken a pro-privacy stance in the public.

Through advocacy, these companies could possibly have concrete effects on future privacy regulation. These companies have, for example, sought for a unified privacy framework in the United States, which would reduce their burden of compliance. The privacy regulation proposed on behalf of these companies could significantly reduce the uncertainty these companies experience with present discourse on privacy regulation. Furthermore, in promoting their own views of privacy regulation, these companies could be hypothesized to influence societal privacy norms, being the largest companies in their respective fields.

Both compliance with privacy regulation and proposals to regulate online privacy should be beneficial for big tech in managing online privacy concern, since as previous literature has shown, perceived regulation decreases online privacy concern among consumers. Based on the findings, a relationship between the compliance towards

privacy regulation and online privacy concern can be hypothesized. For example, Facebook, a company out of the five which has had previous breaches of compliance could be expected to have suffered from an increase in online privacy concern.

5.2 Online Privacy Concern

Most big tech companies have taken a stance of promoting online privacy and clearly informing their customers of their data collection practices, while also informing the customers of their rights and possibilities concerning the use of their personal data. Even so, differences among the companies exist.

Apple, Google and Microsoft all communicate clearly and understandably to their users on issues pertaining to online privacy. The companies clearly explain why personal data is collected and how it is used. By doing this, it could be assumed that the consumers of these companies would have less online privacy concern, due to increased perception of privacy protections. The communication used by these companies is both personal and compassionate, which could be received by consumers as showing care towards consumers' privacy concern. Previous research supports this, as it has been previously found that high quality community might reduce online privacy concern among consumers.

Likewise, the same companies allow consumers to meaningfully change their choices regarding their personal data. By giving their users control over their own private information, the consumers will not have to resort to protective behaviour, such as giving false information.

Furthermore, perhaps partially due to GDPR requirements, all the companies offer an ability for their users to remove their personal data with varying degrees of ease. Providing easy and understandable options for their users could be assumed to reduce the online privacy concern of the consumers.

In their approach to online privacy concern, some characteristics of previously posited ethical theories can be recognized. Firstly, most of the companies seem to act

consistently with the control approach to privacy. According to the approach, privacy is achieved when individuals can control what personal information is shared of them, which is exactly what the different “privacy tools” offered by big tech do. Likewise, there are some emerging characteristics of social contract approach to privacy, especially in terms of communication. This approach can be noticed, for example, in the calls to privacy as posited by Tim Cook who calls for regulation to protect consumers’ privacy.

It could also be assumed, since these companies hold quite monopolistic positions in their markets, they would not have to address online privacy concern appropriately. For example, the switching costs for consumers in the consumer operating systems market might be so high, that consumers will rather discount their own privacy than switch to alternative products. Further dominance and capture of market share could thus also been as a tool to mitigate online privacy concern.

6. DISCUSSION

6.1 General Discussion

This study approached the problem of growing online privacy concern, by exploring the methods used by big tech companies themselves to address online privacy concern and regulation. As most previous studies relate to the standpoint of consumers, this study provided a novel outlook in describing how companies at the forefront of the internet economy approach the problem.

While the study did not exhaustively cover every single aspect of the problem, it sets a solid foundation for future research. The highest value of the findings of this study is in explicating in academic research what can already be observed from the actions of these companies. This study, for example, explicates that big tech sees online privacy concern both as a risk and an opportunity. The companies approach privacy regulation as a risk in their annual reports, yet the same companies and their leadership figures call for more regulation at the same time. The companies have also taken novel approaches to providing their users with relevant information about their own private

information and the control over said information. Noteworthy is also the fact, that clearly not all the companies approach online privacy concern as seriously.

6.2 Limitations

The limitations of this study are mainly related to the methodology, qualitative document analysis and the target companies selected for the research.

Firstly, qualitative document analysis is highly dependent on the judgement of the researcher conducting the analysis. Thus, while under an ideal situation the analysis would be completely objective, the interpretation of language by the researcher always leaves room for personal bias, even if the possibility for bias is recognized in the research process. Likewise, the selection of documents can lead to a biased outlook on the subject, if documents with additional or contrary information are left out of the process.

Secondly, with qualitative document analysis, the source documents must be trusted to provide accurate information. The methodology provides a look from the outside to the workings of the companies being researched, and thus if a company's outward communication is inconsistent with the goals of their management and other internal goals, the research could too provide an explanation that is inconsistent with reality.

And finally, as this study relates only to big tech, it cannot be generalized to other companies dealing with online privacy concern and privacy regulation, as these companies hold quite a unique position in today's economy, due to their enormous shares of their respective market segments. Furthermore, these companies have a controversial public presence which could affect the objectivity of this study, not only by influencing the author's judgement but by also affecting the reliability of the source material about the companies.

7. CONCLUSIONS

7.1 Main Findings

This study explored and explicated the ways in which big tech companies – Apple, Amazon, Facebook, Google and Microsoft address online privacy concern and privacy regulation.

It was found, that regulation is approached by big tech both as a risk as an opportunity. The companies dedicate resources and effort to comply with the prevalent regulation and plan for possible changes in regulation. Regulation is seen by the companies as a risk and a possible cause for adverse effects on their business, such as increased costs and inability to conduct business in their current form.

While regulation was found to be viewed as a risk by big tech, many of the companies also take a proactive stance towards regulation, in one form or another. Some of the companies themselves, and some of their key executives have demanded for increased regulation of privacy, going as far as calling privacy a basic human right that needs to be protected by law. Additionally, the companies have spent resources on lobbying lawmakers in the EU and USA on issues pertaining to privacy regulation, however, the stance taken in the lobbying was not explicated. Furthermore, however, for example, a lobbying organization which was found to represent all of the five companies has taken a stance for federal privacy framework in the USA.

To address consumer privacy, these companies were found to also communicate to their users on issues pertinent to online privacy. Especially Apple, Google and Microsoft were found to communicate clearly to their customers about the usage of their private information. The same companies were also found to provide clear guidelines and tools which their users can utilize to control how their private information is used by these companies.

Amazon and Facebook were also found to try to address their users' online privacy concern in same way as the other three companies, however in a much more rudimentary way. The findings show that big tech can not necessarily be grouped

together as one entity on online privacy issues, as the way in which these companies address online privacy concern and regulation was found to have similarities, but also differences across the companies.

7.2 Implications for International Business

The study contributes to understanding the management of online privacy concern and privacy regulation. Previous studies have taken mostly the viewpoint of consumers towards privacy issues, with this study providing additional insight into how online privacy concern is managed in concrete terms.

Despite the critique which the big tech companies have received on issues pertaining to online privacy, the companies have evidently had enormous success too. The ways in which big tech address online privacy concern and privacy regulation can be mimicked by other companies to achieve similar outcomes in managing online privacy concern.

In addition to having concrete value for management purposes, this study explicates big tech's actions in managing online privacy concern and thus provides valuable information which could advance more informed discourse on the topic.

7.3 Suggestions for Further Research

Further research could attempt to quantify the results derived from this study and investigate the same topic with different target companies. Further viewpoints and sources which might have been left unconsidered in this study could also be evaluated.

To quantify the results of this study, it would make sense, for example, to compare the online privacy concern outcomes of different big tech companies and measure how that relates to the differences mentioned among the companies in this study. It would also be sensible to overall evaluate whether the methods employed by big tech are enough for managing online privacy concern, as this study only discovered those methods, instead of trying to evaluate the effectiveness of them.

Furthermore, studies like this one could be undertaken in different industries and market segments. For example, as this study relates to the largest internet companies in the international market, another point of focus could be local companies in a specific country.

REFERENCES

Acquisti, A. & Grossklags J. (2005) 'Privacy and rationality in individual decision making.' *IEEE Security & Privacy* [Online]. 3 (1): 26-33.

Alphabet (2020) *Form 10-K 2019.* Mountain View, California: Alphabet Inc.

Amazon (2020) *Form 10-K 2019.* Seattle, Washington: Amazon.com, Inc.

Amazon Europe Core SARL (n.d.) Available from: https://lobbyfacts.eu/representative/5615fc9a365b4e0f9e9c0d7929a73f17/amazon-europe-core-sarl [Accessed on 23 March 2020].

Amazon Remains the Undisputed No. 1 (2020) Available from: https://www.emarketer.com/content/amazon-remains-the-undisputed-no-1 [Accessed on 23 March 2020].

Amazon.com Help: Security & Privacy (n.d.) Available from: https://www.amazon.com/gp/help/customer/display.html/ref=help_search_1-2?ie=UTF8&nodeId=201908990&qid=1586095454&sr=1-2 [Accessed on 5 April 2020].

Amazon.co.uk Help: Security & Privacy (n.d.) Available from: https://www.amazon.co.uk/gp/help/customer/display.html/ref=hp_bc_nav?ie=UTF8&nodeId=201908990 [Accessed on 5 April 2020].

Apple (2019) *Form 10-K 2019.* Cupertino, California: Apple Inc.

Apple Inc. (n.d.) Available from: https://lobbyfacts.eu/representative/1e43aba7ad7041e08fb16b2bdacd5414/apple-inc [Accessed on 23 March 2020].

Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V. & Skrinjaric, B. (2019) 'Extended model of online privacy concern: what drives consumers' decisions?' *Online Information Review* [Online]. 43 (5): 799-817.

Ashworth, L. & Free, C. (2006) 'Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns.' *Journal of Business Ethics* [Online]. 67 (2): 107-123.

Azungah, T. (2018) 'Qualitative research: deductive and inductive approaches to data analysis.' *Qualitative Research Journal* [Online]. 18 (4): 383-400.

Bowen, G. (2009) 'Document Analysis as a Qualitative Research Method.' *Qualitative Research Journal* [Online]. 9: 27-40.

Campbell, J., Goldfarb, A. & Tucker, C. (2015) 'Privacy Regulation and Market Structure.' *Journal of Economics & Management Strategy* [Online]. 24 (1): 47-73.

Chowdhury, H. (2020) *Data privacy is a 'human right' says Microsoft's Satya Nadella.* Available from: https://www.telegraph.co.uk/technology/2020/01/23/data-privacy-must-seen-human-right-says-microsofts-satya-nadella/ [Accessed on 5 April 2020].

Cook, T. (2019) *You Deserve Privacy Online. Here's How You Could Actually Get It.* Available from: https://time.com/collection-post/5502591/tim-cook-data-privacy/ [Accessed on 5 April 2020].

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. & Holz, T. (2019) 'We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy.' In: Network and Distributed System Security Symposium 2019; San Diego, California, U.S.: 24-27 February. Reston, Virginia, U.S.: ISOC. pp. 1-15.

Facebook (2020) *Form 10-K 2019.* Menlo Park, California: Facebook, Inc.

Facebook Ireland Limited (n.d.) Available from: https://lobbyfacts.eu/representative/64755e0fc2a14e46aa9d8646df6f8f19/facebook-ireland-limited [Accessed on 23 March 2020].

Fuller, C.S. (2018) 'Privacy law as price control.' *European Journal of Law and Economics* [Online]. 45 (2): 225-250.

Goldfarb, A. & Tucker, C. (2012) 'Shifts in Privacy Concerns.' *American Economic Review* [Online]. 3 (102): 349-353.

Google (n.d.) Available from: https://lobbyfacts.eu/representative/1d40cdaf822941888d1e6121858bb617/google [Accessed on 23 March 2020].

Tietosuoja | Googlen Turvallisuuskeskus (Data Protection | Google's Safety Centre) (n.d.) Available from: https://safety.google/privacy/ [Accessed on 5 April 2020].

Interbrand (2019) *Best Global Brands 2019.* Available from: https://www.rankingthebrands.com/PDF/Interbrand%20Best%20Global%20Brands%202019.pdf [Accessed on 23 March 2020].

Isaak, J. & Hanna, M.J. (2018) 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection.' *Computer* [Online]. 51 (8): 56-59.

Kelly, J. (2019) *Senator Elizabeth Warren Says 'It's Time To Break Up Amazon, Google And Facebook'— And Facebook CEO Mark Zuckerberg Fights Back.* Available from: https://www.forbes.com/sites/jackkelly/2019/10/02/senator-elizabeth-warren-says-its-time-to-break-up-amazon-google-and-facebook-and-facebook-ceo-mark-zuckerberg-fights-back/ [Accessed on 2 March 2020].

Lancelot Miltgen, C. & Smith, J. (2015) 'Exploring information privacy regulation, risks, trust, and behaviors.' *Information & Management* [Online]. 52 (6): 741-759.

Lwin, M.O, Wirtz, J. & Stanaland A.J.S. (2016) 'The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern.' *Internet Research* [Online]. 26 (4): 919-941.

Marcel, B. (2019) ‘Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy.’ *Ethics and Information Technology* [Online]. 21 (4): 307-317.

Martin, K. (2016) ‘Understanding Privacy Online: Development of a Social Contract Approach to Privacy.’ *Journal of Business Ethics* [Online]. 137 (3): 551-569.

Microsoft (2019) *Form 10-K 2019.* Redmond, Washington: Microsoft Corporation.
Microsoft Corporation (n.d.) Available from: https://lobbyfacts.eu/representative/60239386204445e2b0fb38cada46b204/microsoft-corporation [Accessed on 23 March 2020].

Mobile Vendor Market Share Worldwide (2020) Available from: https://gs.statcounter.com/vendor-market-share/mobile [Accessed on 23 March 2020].

Moore, A. (2008) ‘Defining Privacy.’ *Journal of Social Philosophy* [Online]. 39 (3): 411-428.

Nissenbaum, H. (2004) ‘Privacy as contextual integrity.’ *Washington Law Review* [Online]. 79 (1): 101-139.

Operating Systems Market Worldwide (2020) Available from: https://gs.statcounter.com/os-market-share [Accessed on 23 March 2020].

Our Members (n.d.) Available from: https://internetassociation.org/our-members/ [Accessed on 23 March 2020].

Pichai, S. (2019) *Google’s Sundar Pichai: Privacy Should Not Be a Luxury Good* Available from: https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html [Accessed on 5 April 2020].

Pollach, I. (2005) ‘A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent.’ *Journal of Business Ethics* [Online]. 62 (3): 221-235.

Privacy (n.d) Available from: https://internetassociation.org/positions/privacy/ [Accessed on 23 March 2020].

Privacy - Apple (n.d.) Available from: https://www.apple.com/privacy/ [Accessed on 5 April 2020].

Privacy - Government Information Requests - Apple (FI) (n.d.) Available from: https://www.apple.com/legal/transparency/fi.html [Accessed on 5 April 2020].

Privacy & Terms – Google (n.d.) Available from: https://policies.google.com/?hl=en-US [Accessed on 5 April 2020].

Requests for user information – Google Transparency Report (n.d.) Available from: https://transparencyreport.google.com/user-data/overview?hl=en [Accessed on 5 April 2020].

Romm, T. (2019) *DOJ issues new warning to big tech: Data and privacy could be competition concerns.* Available from: https://www.washingtonpost.com/technology/2019/11/08/doj-issues-latest-warning-big-tech-data-privacy-could-be-competition-concerns/ [Accessed on 2 March 2020].

Search Engine Market Worldwide (2020) Available from: https://gs.statcounter.com/search-engine-market-share [Accessed on 23 March 2020].

Smyrnaios, N. (2016) 'L'effet GAFAM: stratégies et logiques de l'oligopole de l'internet' (The GAFAM effect: strategies and logics of the internet oligopoly). *Communication & Languages* [Online]. 188 (2): 61-83.

Social Media Stats Worldwide (2020) Available from: https://gs.statcounter.com/social-media-stats [Accessed on 5 April 2020].

Suranga, J.M. & Kalsi, G.S. (2015) 'The importance of qualitative methods in an exploratory business research: a case study from Punjab, India.' *International Journal of Advanced Research in Management and Social Sciences* [Online]. 4 (2): 85-96.

The Internet Association Announces Membership and Policy Platform. (2012) Available from: https://internetassociation.org/ialaunches/ [Accessed on 4 March 2020].

The Issues That Matter to the Big Tech Lobby (n.d.) Available from: https://www.vpnmentor.com/research/us-lobby-report/ [Accessed on 23 March 2020].

The world's reached a turning point on data and privacy, says Microsoft President Brad Smith (2019) Available from: https://news.microsoft.com/en-gb/2019/09/23/the-worlds-reached-a-turning-point-on-data-and-privacy-says-microsoft-president-brad-smith/ [Accessed on 5 April 2020].

Tietokäytäntö (Privacy Policy) (n.d.) Available from: https://www.facebook.com/policy.php [Accessed on 5 April 2020].

Tietosuoja – Microsoftin tietosuoja (Data protection – Microsoft's data protection) Available from: https://privacy.microsoft.com/fi-FI/ [Accessed on 5 April 2020].

Walsh, D., Parisi, J.M & Passerini, K. (2017) 'Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation.' *Electronic Commerce Research* [Online]. 17 (2): 185-203.
Warren, S.D. & Brandeis, L.D. (1890) 'The Right to Privacy.' *Harvard Law Review* [Online]. 4 (5): 193-220.

Whitman, J.Q. (2004) 'The two Western cultures of privacy: Dignity versus liberty.' *Yale Law Journal* [Online]. 113 (6): 1151-1221.

Wirtz, J., Lwin, M.O & Williams, J.D. (2007) 'Causes and consequences of online privacy concern.' *International Journal of Service Industry Management* [Online]. 18 (4): 326-348.

Yang, A. & Scott, T. (2019) *Apple CEO Tim Cook talks protecting customers' private data, limiting screen time: 'You are not our product'.* Available from:

https://abcnews.go.com/Technology/apple-ceo-tim-cook-talks-protecting-customers-private/story?id=62808679 [Accessed on 5 April 2020].

Yao, M.Z, Rice, R.E & Wallis, K. (2007) 'Predicting user concerns about online privacy.' *Journal of the American Society for Information Science and Technology* [Online]. 58 (5): 710-722.

Yao, M.Z & Zhang, J. (2008) 'Predicting User Concerns about Online Privacy in Hong Kong.' *CyberPsychology & Behavior* [Online]. 11 (6): 779-781.

Yeolib, K., Boreum, C. & Yoonhyuk, J. (2018) 'Individual Differences in Online Privacy Concern.' *Asia Pacific Journal of Information Systems* [Online]. 28 (4): 274-289.

Yksityisyytesi | *Facebookin ohje- ja tukikeskus* (Your Privacy | Facebook's help and support centre) (n.d.) Available from: https://fi-fi.facebook.com/help/238318146535333?helpref=hc_global_nav [Accessed on 5 April 2020].

Zuckerberg, M. (2019) *A Privacy-Focused Vision for Social Networking.* Available from: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ [Accessed on 5 April 2020].

APPENDICES

Appendix 1: Documents used for findings

Type	Reference List Title	Additional detail	Section(s)
Webpage	*Privacy*	internetassociation.org	4.2 Lobbying and Advocacy
Webpage	*The Internet Association Announces Membership and Policy Platform*	internetassociation.org	4.2 Lobbying and Advocacy
Webpage	*Our Members*	internetassociation.org	4.2 Lobbying and Advocacy
Annual report	*Form 10-K 2019*	Alphabet (Google)	4.3 Regulatory Compliance
Annual report	*Form 10-K 2019*	Amazon	4.3 Regulatory Compliance
Annual report	*Form 10-K 2019*	Apple	4.3 Regulatory Compliance
Annual report	*Form 10-K 2019*	Facebook	4.3 Regulatory Compliance
Annual report	*Form 10-K 2019*	Microsoft	4.3 Regulatory Compliance
Trade Research	*The Issues That Matter to The Big Tech Lobby*	vpnmentor.com	4.2 Lobbying and Advocacy
Database	*Amazon Europe Core SARL*	lobbyfacts.eu	4.2 Lobbying and Advocacy
Database	*Apple Inc.*	lobbyfacts.eu	4.2 Lobbying and Advocacy
Database	*Facebook Ireland Limited*	lobbyfacts.eu	4.2 Lobbying and Advocacy

Database	*Google*	lobbyfacts.eu	4.2 Lobbying and Advocacy
Database	*Microsoft Corporation*	lobbyfacts.eu	4.2 Lobbying and Advocacy
Trade research	*Best Global Brands 2019*	rankingthebrands.com	4.4 Market Positioning
Trade research	*Search Engine Market Share Worldwide*	gs.statcounter.com	4.4 Market Positioning
Trade research	*Operating Systems Market Share Worldwide*	gs.statcounter.com	4.4 Market Positioning
Trade research	*Mobile Vendor Market Share Worldwide*	gs.statcounter.com	4.4 Market Positioning
Trade research	*Amazon Remains the Undisputed No. 1*	emarketer.com	4.4. Market Positioning
Trade research	*Social Media Stats Worldwide*	gs.statcounter.com	4.4 Market Positioning
Webpage	*Tietosuoja | Googlen Turvallisuuskeskus (Data Protection | Google's Safety Centre)*	privacy.google.com Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Privacy & Terms – Google*	policies.google.com Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Requests for user information – Google*	transparencyreport.google.com	4.5 User Privacy

	Transparency Report		Information and Controls
Webpage	*Privacy - Apple*	apple.com/privacy Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Tietosuoja – Microsoftin tietosuoja* (Data protection – Microsoft's data protection)	privacy.microsoft.com Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Yksityisyytesi | Facebookin ohje- ja tukikeskus* (Your Privacy | Facebook's help and support centre)	facebook.com/help Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Tietokäytäntö* (Privacy Policy)	facebook.com/policy	4.5 User Privacy Information and Controls
Webpage	*Amazon.co.uk Help: Security & Privacy*	amazon.co.uk/help Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls
Webpage	*Amazon.com Help: Security & Privacy*	amazon.com/help Includes subpages accessed with hyperlinks	4.5 User Privacy Information and Controls

Online news article	*Apple CEO Tim Cook talks protecting customers' private data, limiting screen time: 'You are not our product'.*	abcnews.go.com	4.6 Executive Communication on Privacy
Online opinion piece	*You Deserve Privacy Online. Here's How You Could Actually Get It*	time.com	4.6 Executive Communication on Privacy
Online note	*A Privacy-Focused Vision for Social Networking.*	facebook.com	4.6 Executive Communication on Privacy
Online opinion piece	*Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*	nytimes.com	4.6 Executive Communication on Privacy
Online news article	*The world's reached a turning point on data and privacy, says Microsoft President Brad Smith*	news.microsoft.com	4.6 Executive Communication on Privacy
Online news article	*Data privacy is a 'human right' says Microsoft's Satya Nadella*	telegraph.co.uk	4.6 Executive Communication on Privacy