FUNDAÇÃO GETULIO VARGAS

ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

RAFAEL FERREIRA TRINDADE

DATA PRIVACY AS A STRATEGIC COMPETITIVE ADVANTAGE:

A case study of how Apple and Facebook use data privacy in their branding process

SÃO PAULO

2020

RAFAEL FERREIRA TRINDADE

DATA PRIVACY AS A STRATEGIC COMPETITIVE ADVANTAGE:

A case study of how Apple and Facebook use data privacy in their branding process

Thesis presented to Escola de Administração de Empresas de São Paulo of Fundação Getulio Vargas, as a requirement to obtain the title of Master in International Management (MPGI).

Knowledge Field: Marketing, Data Privacy

Adviser: Prof. Dr. Luís Henrique Pereira

SÃO PAULO

2020

Trindade, Rafael Ferreira.

Data privacy as a strategic competitive advantage : a case study of how Apple and Facebook use data privacy in their branding process / Rafael Ferreira Trindade. - 2020.

75f.

Orientador: Luís Henrique Pereira.

Dissertação (mestrado profissional MPGI) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Direito à privacidade. 2. Proteção de dados. 3. Internet - Aspectos sociais. 4. Vantagem competitiva. I. Pereira, Luís Henrique. II. Dissertação (mestrado profissional MPGI) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 681.324

Ficha Catalográfica elaborada por: Raphael Figueiredo Xavier CRB SP-009987/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

RAFAEL FERREIRA TRINDADE

DATA PRIVACY AS A STRATEGIC COMPETITIVE ADVANTAGE:

A case study of how Apple and Facebook use data privacy in their branding process

Thesis presented to Escola de Administração de Empresas de São Paulo of Fundação Getulio Vargas, as a requirement to obtain the title of Master in International Management (MPGI).

Knowledge Field: Marketing, Data Privacy

Approval Date

12/02/2020

Committee members:

_____

Prof. Dr. Luís Henrique Pereira

_____

Profa. Dra. Thelma Valéria Rocha

_____

Prof. Dr. Benjamin Rosenthal

Acknowledgment

I thank my family unconditionally, especially my mother, Marlene, my father, Ivanildo, my sister, Gabriela, and my half-sister, Bruna, who have always supported me and have always taught me the importance of effort and dedication. Today, I am only the man I am, thanks to the education and values they have taught me. I will be forever grateful for the belief and investment they had in my potential, even in the hardest times. They may not know, but they taught me to dream big. And because of that, maybe someday I will be as big as them.

A very special thanks to my advisor, Luís Henrique Pereira, for all the support and patience during the follow-up of this study, believing in me more than myself in some moments. I was very honored to count on you as my advisor, I have always admired you as a teacher, but now I also admire you as a friend.

I thank the professors Francisco Saraiva Júnior and Tânia Modesto Veludo de Oliveira for being responsible for me falling in love with the study and practice of Marketing. To the professor Francisco José Espito Aranha Filho I am grateful for having assisted me in the decision-making process to do the Masters. Also, I would like to thank LSE's professor Edgar A. Whitley for making me completely thrilled by the subject of data privacy. After his classes, I will never be able to see the world in the same way.

I am grateful for everyone who was part of my history. I believe there are no coincidences in the universe, each person who goes through our lives contributes to the achievement of our dreams. In particular, I thank Caio Pastor de Sandre for making me a better person every day. Being able to see the world through your eyes is the best life motivation anyone could ask for.

Last but not least, I am grateful to God for always illuminating my path.

Abstract

The growing number of data breaches in the world has brought the concern about Data Privacy to the mainstream media, raising the public awareness of the consequences of bad harvesting of personal data. Moreover, after the Europe Union's General Data Protection Regulation (GDPR), many companies started to change their positioning regarding data privacy.

The objective of this study is to identify evidences that data privacy has been and can be used as a competitive advantage. Being a very recent topic, it has yet not been studied deeply in a business and branding point of view. Therefore, this study aims to raise the awareness of the managerial implication of the topic.

Secondary data collected was used to build and analyze a case study of how Apple and Facebook have been handling data privacy and if this behavior consists a competitive advantage for them. Additionally, the Privacy Leverage Point Framework (Culnan and Armstrong, 1999) was used to identify if such companies were capable of leveraging data privacy as a competitive strategy. Also, each company was analyzed through the Brand Authenticity Framework (Fritz, Schoenmueller and Bruhn, 2017) in order to understand if their efforts with data privacy could be incorporated to their branding processes in a way that could be perceived as authentic to the consumers.

This study found evidences that data privacy can and is already being used as a strategic competitive advantage, as it was seen in the Apple case. However, it is important to pay attention to the authenticity of the move. The brand map of the company must be able to incorporate this positioning attempt, otherwise, it can shift from a strategic competitive advantage to a strategic competitive disadvantage, as the Facebook's case.

Finally, since this study is limited to analyze company's actions and communication pieces, a further study on the scenario thought the consumer's point-of-view is suggested. It is needed to be understood if the privacy calculus and the brand authenticity framework are consistent across developed/developing markets and industry sectors.

Key Words: Data Privacy, Branding, Marketing, Brand Authenticity, Surveillance Capitalism.

Resumo

O crescente número de violações de dados pessoais no mundo trouxe a preocupação com a privacidade de dados para a grande mídia, aumentando a conscientização do público sobre as consequências da má coleta dessas informações. Principalmente após o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, muitas empresas começaram a mudar seu posicionamento em relação ao assunto.

O objetivo deste estudo é identificar evidências de que a privacidade de dados pode ser usada como uma vantagem competitiva. Por ser um tópico recente, ainda não foi estudado profundamente do ponto de vista administrativo e de *branding*.

Dados secundários foram coletados para a construção e análise de um estudo de caso sobre como a Apple e o Facebook lidam com a privacidade de dados e se esse comportamento consiste em uma vantagem competitiva para as empresas. Além disso, o *Framework* dos Pontos de Alavancagem de Privacidade (Culnan e Armstrong, 1999) foi usado para identificar se essas empresas eram capazes de alavancar a privacidade de dados como uma estratégia competitiva. Cada empresa também foi analisada por meio do *Framework* de Autenticidade de Marca (Fritz, Schoenmueller e Bruhn, 2017), a fim de entender se seus esforços poderiam ser incorporados às marcas de uma maneira percebida como autêntica por seus clientes.

Este estudo encontrou evidências de que a privacidade de dados pode e já está sendo usada como uma vantagem competitiva estratégica, como no caso da Apple. No entanto, o mapa de significados da marca deve ser capaz de incorporar tais ações contempladas no posicionamento, caso contrário, pode deixar de ser uma vantagem competitiva e passar a ser uma desvantagem competitiva estratégica, como no caso do Facebook.

Por fim, uma vez que este estudo se limita a analisar as ações e comunicações das empresas, um estudo mais aprofundado considerando o ponto de vista dos consumidores é sugerido. Ainda é necessário entender se o cálculo de privacidade e o *framework* de autenticidade da marca são consistentes através de mercados desenvolvidos e em desenvolvimento e através de diferentes setores.

Palavras Chave: Privacidade de Dados, Branding, Marketing, Autenticidade de Marca, Capitalismo da Vigilância.

List of Tables

List of Figures

Table of Contents

Introduction

Overview

More than ever, data privacy has become an extremely important topic for discussion. The increasing data breaches worldwide have attracted the attention of the mainstream media, thus alerting the public to the consequences of the data breaches. One of the biggest and most recent events was the Cambridge Analytica case, where a political research firm obtained personal data from more than 70 million Facebook users through a phony personality quiz (Garrahan & Kuchler, 2018). Although it did not initially seem to be critical, the information obtained was allegedly used to influence the results of the 2016 United States (US) presidential election. This situation presented to the public the seriousness of data breaches.

Since then, most data breaches are isolated to a smaller number of users and have not been linked to so serious an impact as affecting the results of a general election. Even so, the topic is relevant because the public has come to appreciate how many aspects of their daily life are susceptible to data exploitation. Vacuum-cleaning bots map homes to sell the information to other companies (Quach, 2017), and private medical data sell for billions of dollars (Thielman, 2017). Although user information is anonymized, the risks are not mitigated; data miners and brokers can build up detailed dossiers on individuals by cross-referencing the data with other sources. Even ride-sharing might not be safe from privacy issues since Uber recently announced that it would start audio-recording rides as a safety measure (Chaudhry, 2019).

Data gathering is not limited to companies; governments collect personal data as well. The US Homeland Security has started a mandatory face-scanning procedure in all American airports (Whittaker, 2017). This situation raised the question of the right to give consent regarding the collection of biometric data; it received a simple “if you don’t like it, don’t travel” answer from the government. The topic is very controversial, especially since the technology is imperfect. Amazon’s facial recognition software, recognized as one of the world’s most advanced, wrongly identified 28 US lawmakers as criminals (Singer, 2018), thereby showing how the compulsory extraction of personal data raises much doubt.

A recent Accenture research (Tielman, 2019) shows that while customers feel brands do not know them well enough to personalize their experience to make them feel special, they feel that brands harvest too much personal data, thereby making them lose trust in companies.

Amid this paradox, 69% of customers interviewed said that they would abandon brands that do not handle private data properly, and 73% of consumers are willing to share more personal information if brands are transparent about how it is used.

Given the appreciation of the gravity of the data misuse and how much data is being extracted without consent, public awareness of the topic has grown, and many privacy discussions have graduated into the public debate.

With this scenario of higher awareness of the subject, especially after the General Data Protection Regulation (GDPR) of the European Union, many companies have changed their position regarding data privacy.

Facebook, undoubtedly one of the most vilified companies regarding user privacy, recently announced that its services would be redeveloped as a privacy-focused social network, based on principles, such as encryption, reducing permanence, safety, interoperability, and secure data storage (Zuckerberg, 2019).

Meanwhile, Apple has focused on iPhone communication regarding their claim of privacy: "(…) we believe privacy is a fundamental human right. And so much of your personal information — information you have a right to keep private — lives on your Apple devices." ("iPhone Privacy," n.d.). Moreover, regarding their first 2019 keynote, while presenting their new strategy of focusing heavily on new services (such as TV streaming, magazines, games, and credit card services), the company positioned privacy as the main differentiation factor, thus making clear their argument for why people should choose Apple services over the competition: Apple want their costumers to trust that they cannot know their personal information, such as which movies they are watching, which music they listen, which magazines they read, and where and how they use their credit card. In general, everything is encrypted locally (in the device) and handled with care (Waters, 2019).

Research Question

This study aims to answer the following research question: Can data privacy be used by companies as competitive advantage strategy?

Also, as an additional research objective, this study aims to understand if whether company's promises in their data privacy communication might be perceived as authentic or not, and how it may affect brand image.

This study identifies examples of when data privacy has been used as a competitive advantage, thereby contributing to the data privacy literature in the marketing field. Given that this topic is very recent, personal data privacy has not yet been studied in-depth from a business and branding perspective (Dienlin & Metzger, 2016; Kaye, 2015; Solon, 2018). Thus, this study raises the awareness of the emergent managerial implications for all companies, not only for the "big tech" sector.

This study contributes to prior studies by combining the notions of brand authenticity (Fritz, Schoenmueller, & Bruhn, 2017) and privacy leverage point (Culnan & Armstrong, 1999), against the backdrop of surveillance capitalism (Zuboff, 2019).

The relevance of data privacy is argued by Zubbof (2019) in the book, "The Age of Surveillance Capitalism." The economic incentives of harvesting customer's behavioral surplus will increase the relevance of the subject in the future. Thus, similar to how environmental issues have become mandatory in recent times, managers need to be aware of how to implement data privacy in their business models, regardless of the business sector.

This work, therefore, presents different theoretical approaches regarding privacy, the idea of privacy calculus, and the important debate of digital anonymization and digital consent. After expanding on the traditional knowledge of privacy, the study presents the concept of surveillance capitalism, which is a new concept for analyzing the future impact of harvesting personal data. Finally, the literature review presents the managerial implications of the topic with the brand authenticity and privacy leverage point frameworks.

An embedded multi-case study is conducted to understand the actions of both Apple and Facebook regarding data privacy using secondary data in a qualitative approach. The privacy leverage point framework (Culnan & Armstrong, 1999) ascertains whether company actions can lead to strategic competitive advantage, and the brand authenticity framework (Fritz et al., 2017) ascertains whether company actions might be perceived as authentic, which can affect brand image.

The analysis indicated that Apple's privacy strategies were perceived as an authentic strategic competitive strategy, whereas Facebook's were perceived as ambitious and untrustworthy, which did not lead to a strategic competitive strategy.

The study of the managerial implications in handling private data is new and lacks an adequate understanding of the cause and effect of the company actions regarding its reputation. Moreover, since this study is limited to analyzing company actions and communication pieces, further research from the consumer's perspective is recommended.

Literature Review

Privacy

Definition. The definition of privacy is debated among theorists. Solove (2008) claims that privacy is a concept in disarray, essential for a democratic government, critical to our ability to create and maintain different sorts of social relationships with different people, necessary for permitting and protecting an autonomous life, and important for emotional and psychological tranquility. Moreover, he states that the concept is difficult to define because it is exasperatingly vague and evanescent, infected with pernicious ambiguities. Privacy is complex and entangled in competing and contradictory dimensions with various and distinct meanings that the author sometimes despairs about whether it can be usefully addressed at all.

Among the first jurists to write about the subject was Warren and Brandeis (1890) in a Harvard Law Review article, reacting to the intrusion of Warren's family privacy. The author mentions how recent inventions, such as instantaneous photography, and business methods, called attention to the next steps that should be taken for the protection of people's privacy.

Burgoon (1982) states that it is possible to distinguish between physical privacy (freedom from surveillance and unwanted intrusions upon one's physical space), interactional privacy (control over social encounters), psychological privacy (protection from intrusions upon one's thoughts, feelings, attitudes, and values), and informational privacy (the ability to control the aggregation and dissemination of information).

According to Westin (1967), privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means. People withdraw from others for many reasons, such as making autonomous decisions, fostering intimate relationships, or regulating emotions (Westin, 1967). Self-withdrawal is largely about trying to avoid adverse outcomes of communication, which is why it can be considered a form of self-protection behavior (Rogers, 1983).

Privacy calculus. As social beings, people interact with one another to promote social relationships, which requires some form of self-disclosure (Altman, 1975). People regulate their privacy most significantly by either self-withdrawing or self-disclosing (Petronio, 2012). Thus, the choice on whether the information will be handled as public or private can be hard to set depending on contexts or stereotypic situations, which Nissenbaum (2004) calls

contextual integrity. Since there is a huge asymmetry of information and power between companies and users, it is hard for someone to calculate the risks of disclosing personal information correctly.

Laufer and Wolfe (1977) argue that this dilemma is cleared by weighing the potential risks and benefits regarding future consequences. When users weigh perceived benefits as heavier than the risks to privacy, disclosure is likely to occur. Dienlin and Metzger (2016) suggest that disclosure behavior may be primarily motivated by proximate social benefits than by distant risks to privacy.

Regarding disclosure benefits, diversion and entertainment, social relationships, identity construction are necessary. Online social networks are embedded in our social lives; moreover, to maintain social lives, people must disclose information despite privacy concerns (Dienlin & Metzger, 2016).

Concerning the disclosure process, two arguments are regularly employed to justify the extraction of data and mitigate the sensation of risk: data collected is anonymous, and there is no risk to the user; moreover, even if there was a risk, the user already gave consent by accepting the terms and conditions of any digital service.

These two concepts will be discussed in the following topics.

Digital anonymity. According to Ohm (2009), data is anonymized to protect the privacy of subjects when storing or disclosing data. Although many defend the privacy-protecting power of anonymization and hold it out as a best practice, there is evidence to the contrary.

Solon (2018) reports that in August 2016, the Australian government released an anonymized data set of medical billing records, including prescriptions and surgeries of 2.9 million people. Names were removed from the records to protect the privacy of individuals. However, a research team from the University of Melbourne discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries.

This scenario is not limited to governments. Walker (2018) states that working with publicly available metadata from Twitter, a machine learning algorithm was able to identify users with a 96.7 percent accuracy.

Narayanan and Felten (2014) defend the notion that de-identification fails to resist the inference of sensitive information either in theory or in practice and ascertains why attempts to quantify its efficacy are unscientific and promote a false sense of security. Thus, one can either have anonymized data or useful data, but not both (Ohm, 2009).

Cavoukian and Castro (2014) present a different perspective. According to the authors, the risk of re-identification has been greatly exaggerated. Their main argument is that the most famous re-identification was when researchers re-identified Netflix users in an anonymous dataset by comparing the dates and ratings of movies watched by those users with similar, personally identifiable information available on the Internet Movie Database (IMDb). While this case importantly exposed the risks of disclosing de-identified data improperly, the researchers re-identified only two out of 480,189 Netflix users, or 0.0004% of users, with confidence.

That is, a tremendous amount of analysis was necessary to identify a small number of users, which would be impractical for widespread use. Although the author the sensationalism regarding re-identification, it is still a possibility, even if remote. The knowledge barrier in an environment full of technicalities presents divergent opinions, where one must choose which side of the history makes reality less dystopic.

Digital consent. Hoeyer (2009) highlighted the origin of informed consent as a response to the abuses of medical practice in World War II and stated the need to allow people to give, refuse, or withdraw explicit consent. It was especially crucial for this consent to be traceable and communicated to others involved in the individual's direct care.

Article 4 of the GDPR provides the core definition of consent as any freely given specific, informed, and unambiguous indication of wishes by which the data subject, either by a statement or by clear affirmative action, signifies agreement to personal data relating to them being processed (European Commission, 2018).

Affirmative action can be understood as ticking a box on a website, for example. That is the reason pre-ticked boxes or inactivity does not constitute consent. However, it excludes the possibility of implied consent, where merely using a service can be understood as consent.

The biggest issue with consent in the digital world is that it is mandatory for accessing digital services; that is, give us your data or do not use the service at all. Accepting the terms

of service delivery should not be the same as agreeing to give access to personal data (Whitley, 2009). Thus, there is only an illusion of consent in most of the digital world.

Kaye (2015) presents the concept of dynamic consent as a solution to this issue, which provides a tailored option of consent, thus enabling people to choose how and when their data is shared in a non-Boolean way.

Importance. Privacy is a fundamental human right. It is a basis for the development of individuality. It protects personal autonomy, supports healthy functioning by providing needed opportunities to relax, emotionally vent, escape from the stresses of daily life, manage bodily and sexual functions, and cope with loss, shock, and sorrow (Margulis, 2003).

Privacy matters because it provides experiences that support normal psychological functioning, stable interpersonal relationships, and personal development. The lack of the total elimination of privacy may have irreparable consequences to humankind and society.

The rise of the notion of surveillance risks and privacy as a luxury (and not a right) move our economic order to a new phase of capitalism: surveillance capitalism.

Surveillance Capitalism

Zuboff (2019), in her latest book "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power," presents the new concept of surveillance capitalism. It defines a new economic order that claims human experiences as free raw material for hidden commercial practices of extraction, prediction, and sales. At its core, surveillance capitalism is parasitic and self-referential. It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected twist. Instead of labor, surveillance capitalism feeds on every aspect of human experience.

According to Zuboff (2019), during the early periods of surveillance capitalism, behavioral data were put to work entirely on the user's behalf. What was called "user experience" was developed with user data at no cost. During this first period, companies like Google used the data only to optimize its services in a behavioral value reinvestment cycle, as shown in **Figure 01**.

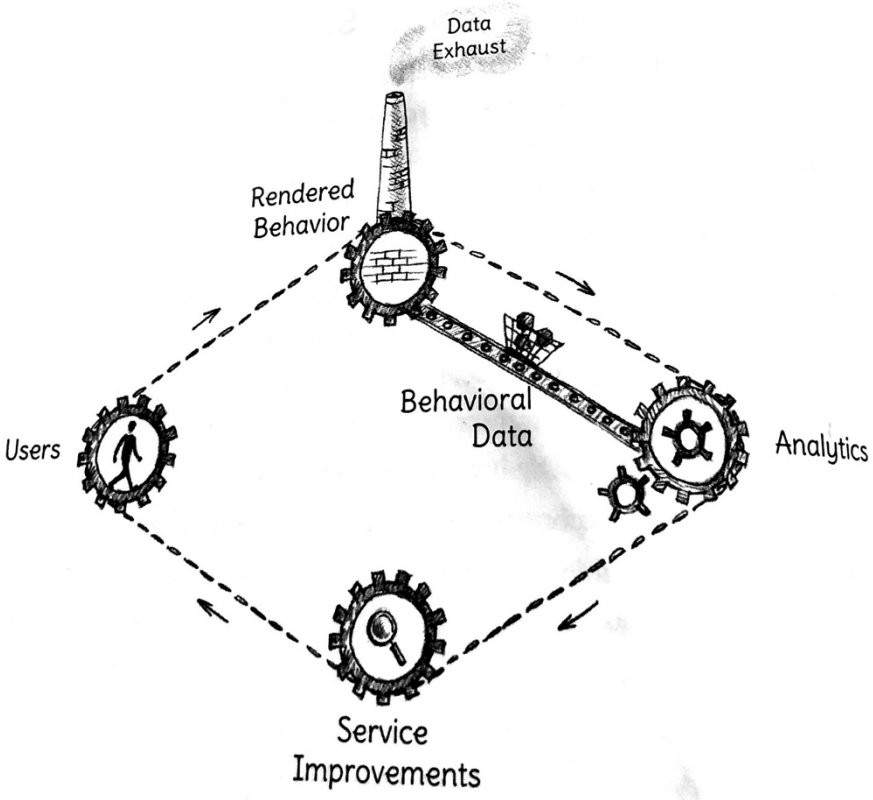


Figure 01. The Behavioral Reinvestment Cycle. Adapted from Zuboff (2019).

Zuboff (2019) states that surveillance capitalism begins with the discovery of behavioral surplus. When companies realized that more behavioral data were rendered than required for service improvements, those companies started developing ways of handling this surplus, such as feeding machine intelligence (the new means of production) that fabricates predictions of user behavior.

Surveillance capitalism unilaterally claims humans experience as free raw material for translation into behavioral data. Although some of these data are applied to products or service improvement, the rest are declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into prediction products that anticipate user actions (Zuboff, 2019). These products are sold to business customers in new behavioral future markets, as shown in **Figure 02**.

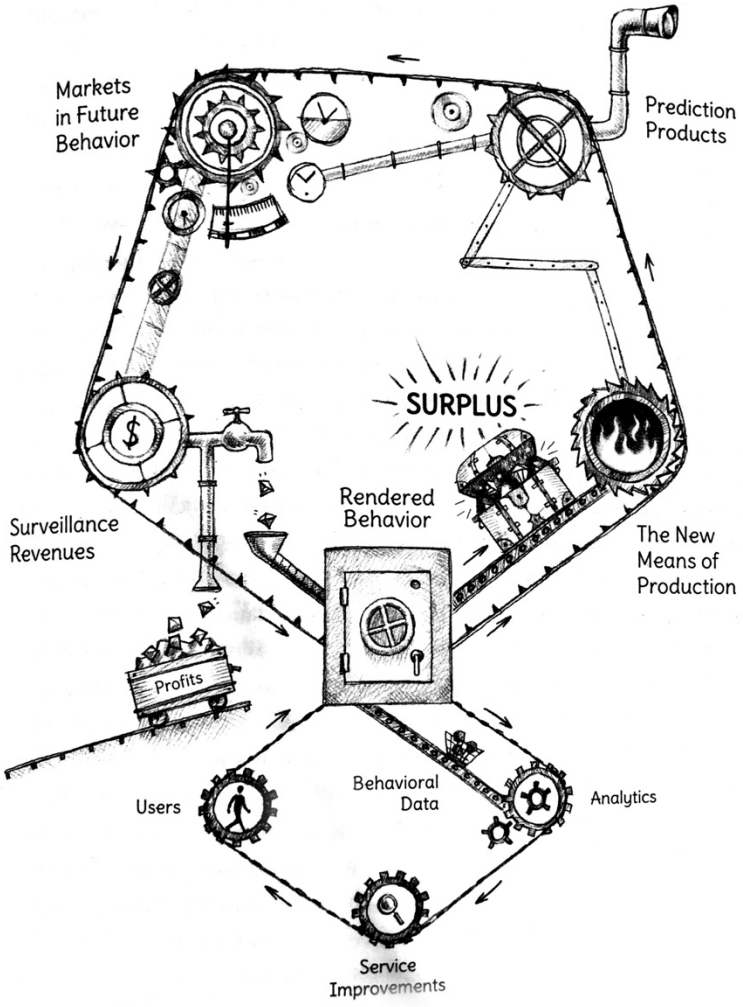


Figure 02. The Discovery of Behavioral Surplus. Adapted from Zuboff (2019).

Zuboff (2019) also claims that surveillance capitalists discovered that the most predictive behavioral data come from intervening in the state of play to nudge behavior towards profitable outcomes. Competitive pressures produced this shift, where automated machines know not only our behavior but also shape our behavior at scale. With this reorientation from knowledge to power, it is no longer enough to automate information flows about us; the goal now is to automate us. Thus, surveillance capitalism births a new kind of power called instrumentarianism. Instrumentarian power knows and shapes human behavior toward other's ends. Instead of armaments and armies, it works its will through the automated medium of an increasingly ubiquitous computational architecture of "smart" networked devices, things, and spaces.

In the second phase of surveillance capitalism, there is the migration of surveillance capitalism from the online environment to the real world, a consequence of the competition for prediction products to approximate certainty. Much of this new work is accomplished under the banner of personalization, a camouflage for aggressive extraction operations that mine the intimacies of everyday life (Zuboff, 2019). Nowadays, we not only have sensors in online services but in products of our everyday life. Smart connected houses, fitness and sleep trackers, smart assistants in televisions, speakers, and even fridges collect data of every aspect of our routine. The claim of personalizing the product to our specific needs is just a way of making people focus on the positive side of the disclosure of personal data. According to the author, we are living in this phase of surveillance capitalism.

The growing presence of sensors in products does not only acts as a way of collecting data from our normal behavior. Zuboff (2019) states that, ultimately, this requires not only amassing vast volumes of data but intervening in our behavior. The shift is from monitoring to what the data scientists call "actuating." Surveillance capitalists now develop "economies of action," as they learn to tune, herd, and condition our behavior with subtle and subliminal cues, rewards, and punishments that draws us toward their most profitable outcomes. This new behavior is more susceptible to the disclosure of personal data by users and facilitates the collection of data by companies, thus lowering the cost of the data acquisition. Given this vicious cycle, the movement accelerates the momentum of data collection. Moreover, the more the data, the better the prediction imperative, as shown in **Figure 03**.

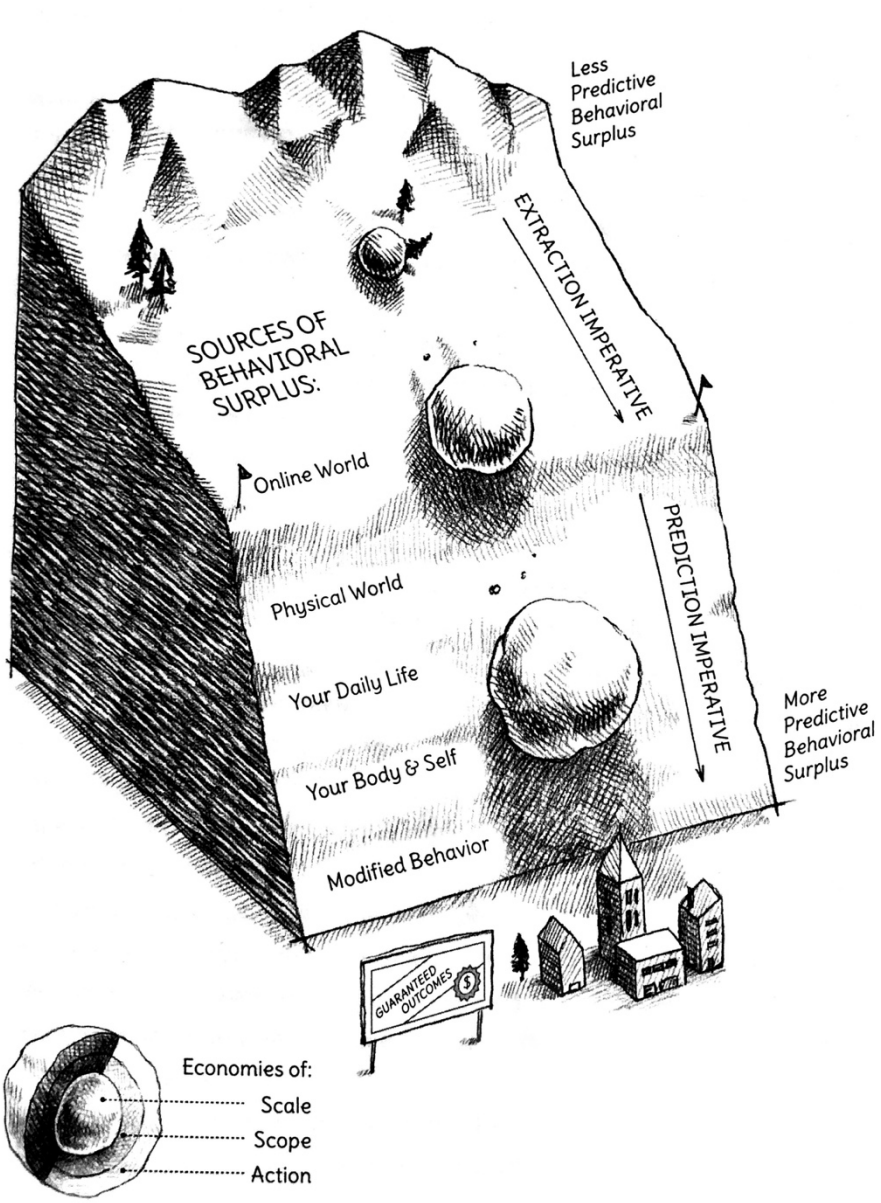


Figure 03. The Dynamic of Behavioral Surplus Accumulation. Adapted from Zuboff (2019).

Zuboff (2019) believes that the final and next stage of the surveillance capitalism will be the rise of instrumentarian power in a ubiquitous, sensate, networked, and computational infrastructure called Big Other. Totalitarianism is the transformation of a state into a project of total possession. Instrumentarianism (and its materialization into the "Big Other") signals the transformation of the market into a project of total certainty. In this scenario, the author predicts a utopian future, which seems too distant and radicle to be predicted with the information we have in the present. Nevertheless, it is still valid more as a reflection piece than a concept.

Unlike traditional capitalism, surveillance capitalism products and services are not the objects of value exchange. They do not establish constructive producer-consumer reciprocities. Instead, they are the "hooks" that lure users into their extractive operations in which personal experiences are scraped and packaged as the means to other's ends. Mostly, free services and information in exchange for personal data are collected without user consent. Many inbound marketing strategies take advantage of bait offers to lure users in collecting their personal data.

Surveillance capitalism operates through unprecedented asymmetries in knowledge and power that accrues to knowledge. Surveillance capitalism knows everything about us, whereas their operations are designed to be unknowable to us. They accumulate vast domains of new knowledge from us but not for us. As long as surveillance capitalism and its behavioral future markets are allowed to thrive, ownership of the new means of behavioral modification eclipses ownership of the means of production as the fountainhead of capitalist wealth and power in the twenty-first century (Zuboff, 2019).

The rapid growth of the surveillance capitalism actions apparently occurred because it was an unprecedented phenomenon. Zuboff (2019) explains that when we encounter something unprecedented, we automatically interpret it through the lenses of familiar categories, thereby rendering invisible precisely that which is unprecedented. This situation contributes to the normalization of the abnormal, such as the incorporation of smart sensors in our daily routine.

Finally, Zuboff (2019) highlights that surveillance capitalism is logic in action and not technology. This distinction is vital because surveillance capitalists want people to think that their practices are inevitable expressions of the technology they employ.

For example, in 2009, it was discovered that Google kept user search history indefinitely. The Google CEO said it was normal behavior for search engines. However, the reality is that the search engine does not retain data; the surveillance capitalist does. Google, for instance, camouflages the concrete practices of surveillance capitalism and the specific choices that impel its brand of search into action. Most significantly, it makes surveillance capitalism practices appear to be inevitable when they are actually a meticulously calculated and lavishly funded means to self-dealing commercial ends.

Zuboff (2019) believes that if the digital future is aimed to be the home of humanity, then humans should work to make it so by fighting for these actions to be heavily regulated and followed closely by government agents. The disclosure of data may be necessary for the

future of connected things. However, we can still hold the right of opting to disclose or retain personal information, given that such data should be handled and stored by super computational infrastructures owned by the people and not a few organizations.

Privacy as a Competitive Advantage

Culnan and Armstrong (1999) recognize that the process of gathering personal data from users can strain customer-company relationships. The growing demand for user data can be viewed as a risk of rising tensions. The author argues that consumers are willing to disclose personal information when fair procedures address their concerns about privacy, and as a consequence, companies can gain competitive advantage by behaving ethically.

Based on how transaction data is used, the information as an organizational resource can create either positive or negative outcomes for a firm. In positive terms, the use of transaction data to yield better customer service, higher quality products, and new products that reflect consumer preferences creates benefits for both consumers and the firm (Culnan & Armstrong, 1999). The satisfaction from the service quality can induce customers to continue using the service and disclosing data. This process is called procedural fairness, in which the user perceives the fair and consistent use of his data (Lind & Tyler, 1988).

However, if the data is not treated fairly and consistently, it is expected that the user will defect or engage in bad word of mouth (Culnan & Armstrong, 1999). Thus, the privacy leverage point, as seen in **Figure 04**, provides a managerial opportunity for firms to build trust with their customers as they collect and use personal information, thereby making customers willing to disclose personal information by minimizing the risks of disclosure.

In other words, the privacy leverage point helps the privacy calculus done by the user. Thus, by building a higher trust and better customer relationships, the company can retain and attract new users and maintain a competitive advantage from its competitors.

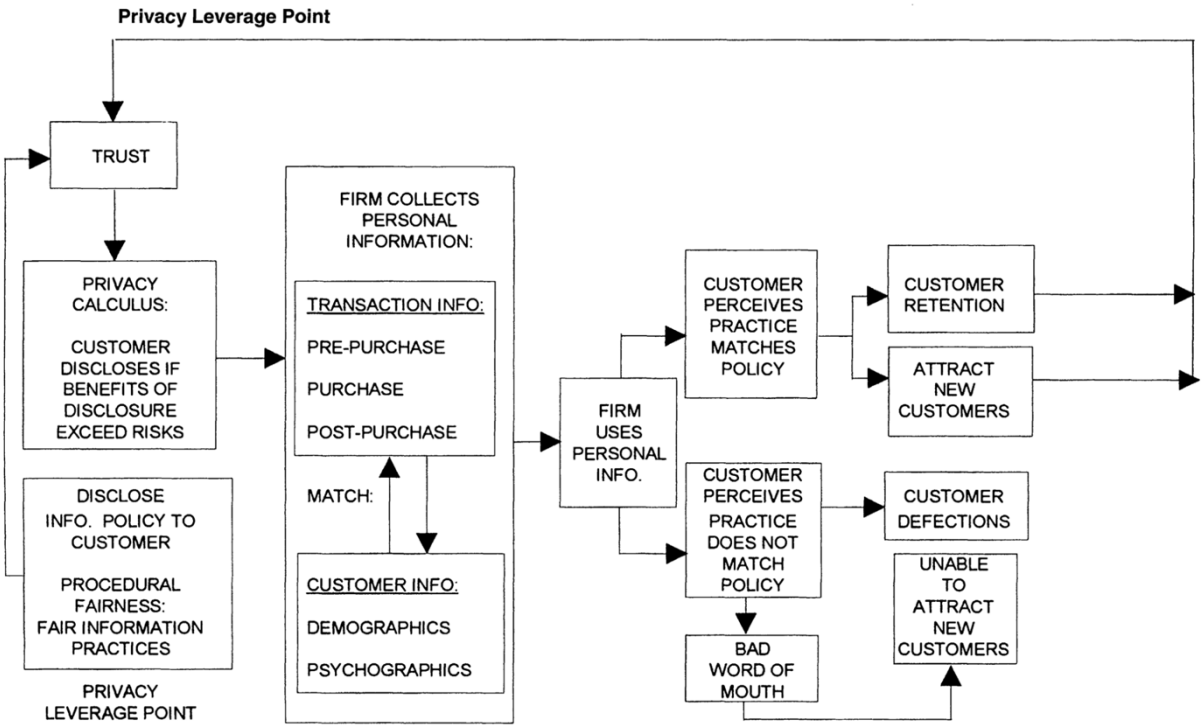


Figure 04. Privacy Leverage Point Framework. Adapted from Culnan and Armstrong (1999).

At the same time, to incorporate the privacy leverage point in its branding process, a company's privacy statement must be perceived as authentic. Brand authenticity, according to Fritz et al. (2017), is influenced by variables, such as brand heritage, brand nostalgia, brand commercialization, brand clarity, social commitment, brand legitimacy, actual self-congruence, ideal self-congruence, and employee passion. These variables, with the involvement of the company's active branding process, create brand authenticity, which is essential for the brand relationship quality.

Fritz et al. (2017) define brand heritage as the perceived anchoring of a brand to its tradition and how the company position itself on its heritage rather than the fact that the brand has a long history. Brand nostalgia is defined as the consumer's perception of the nostalgic brand staging. Brand commercialization focuses on how the company channels its brand's values and norms into its financial success. Brand clarity depicts the articulated clarity of the brand's communication style, and social commitment represents the company's assumption of social responsibility. Brand legitimacy describes the consumer-brand fit, in the sense of brand

community. The variables, actual and ideal self-congruence, refer to how customers identify themselves (their perceived and real image) with the company's communicated image. Finally, employees are the best to evaluate the internal culture of a company. Therefore, the perceived employee passion is an indicator of the perceived enthusiasm and eagerness of the brand's employees.

Furthermore, given these variables in the attempt to understand how companies actively try to position themselves, it is possible to analyze the quality of the brand relationship, as seen in **Figure 05**:

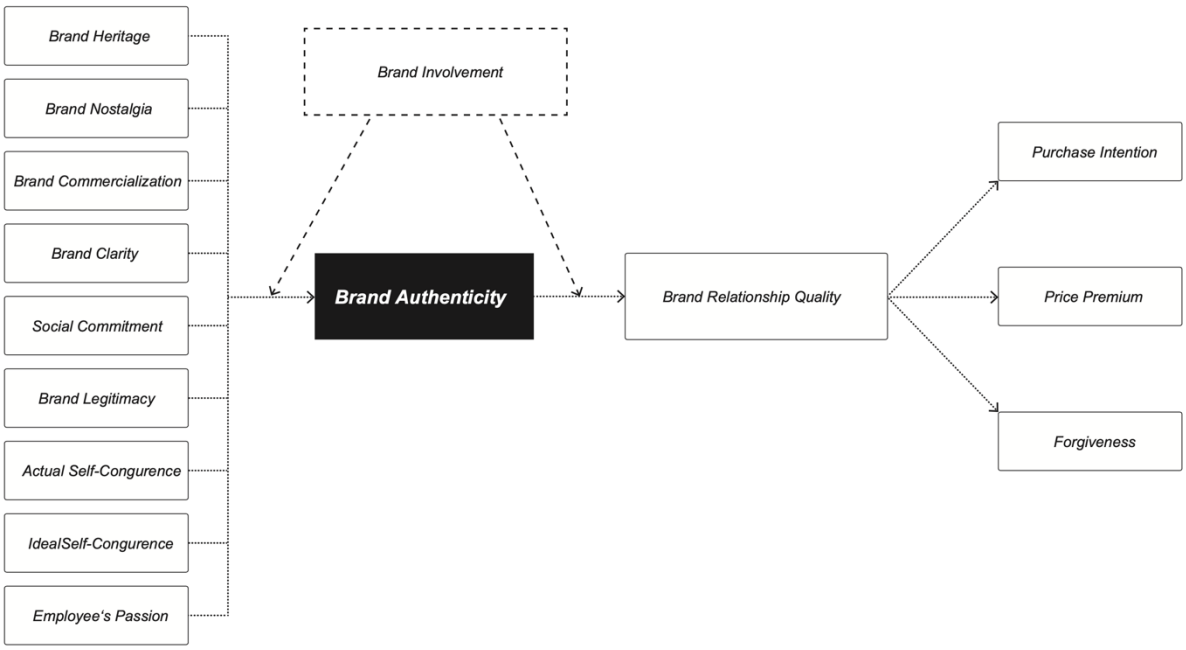


Figure 05. Brand Authenticity Framework. Adapted from Fritz, Schoenmueller, and Bruhn (2017).

It is in the company's best interest to harvest a good brand relationship with its customers. As long as the quality is high, the brand will aim for a better price premium and better purchase intention. Moreover, in the case of an incident, the higher the quality of the relationship, the greater the chances of forgiveness from its customers.

Methodology

In order to answer a research question, according to Creswell (2014), the methodologic planning of a study needs to set a philosophical worldview assumption, the research design that is related to this worldview and the specific methods of research that translate that approach in practice.

A pragmatic worldview (Creswell, 2014) is employed in this study since the goal is to identify consequences rather than antecedent conditions of the privacy scenario in these companies. The presentation and grounding in a vast and sometimes conflicting theoretical background for privacy demonstrates a pluralistic approach to the subject.

Since a qualitative approach was chosen for this study, a correspondent research design was chosen. The historic origin for qualitative research comes from anthropology, sociology, the humanities, and evaluation. The most common qualitative research designs are narrative research, phenomenology, grounded theory, ethnographies and case study worldview (Creswell, 2014). This study chose to build a case analysis.

Case study research is an investigation and analysis of a single or collective case, intended to capture the complexity of the object of study. Multiple data collection and analysis methods are adopted to further develop and understand the case, shaped by context and emergent data (Stake, 1995).

Qualitative research with secondary data is employed to answer the research question. Secondary data previously collected and made available for purposes other than those of the problem at hand and can easily be found at little cost. Although they rarely provide all the answers to a nonroutine research problem, they help identify, better define, develop an approach to problems, and formulate an appropriate research design (Malhotra, 2012). The secondary data collected will be used to build and analyze a case study of how Apple and Facebook handle data privacy and if this behavior results in a competitive advantage.

Having set the philosophical worldview assumption (pragmatic), the research design (case study) and the specific methods of research (desk research with secondary data), it is important to decide the type of case analysis this study will use between the four types Yin (2014) presents: single or multiple cases. Whether single or multiple, it can also be holistic or

have embedded subcases within an overall holistic case. The resulting two-by-two matrix leads to four different case study designs, as shown in **Figure 06**:

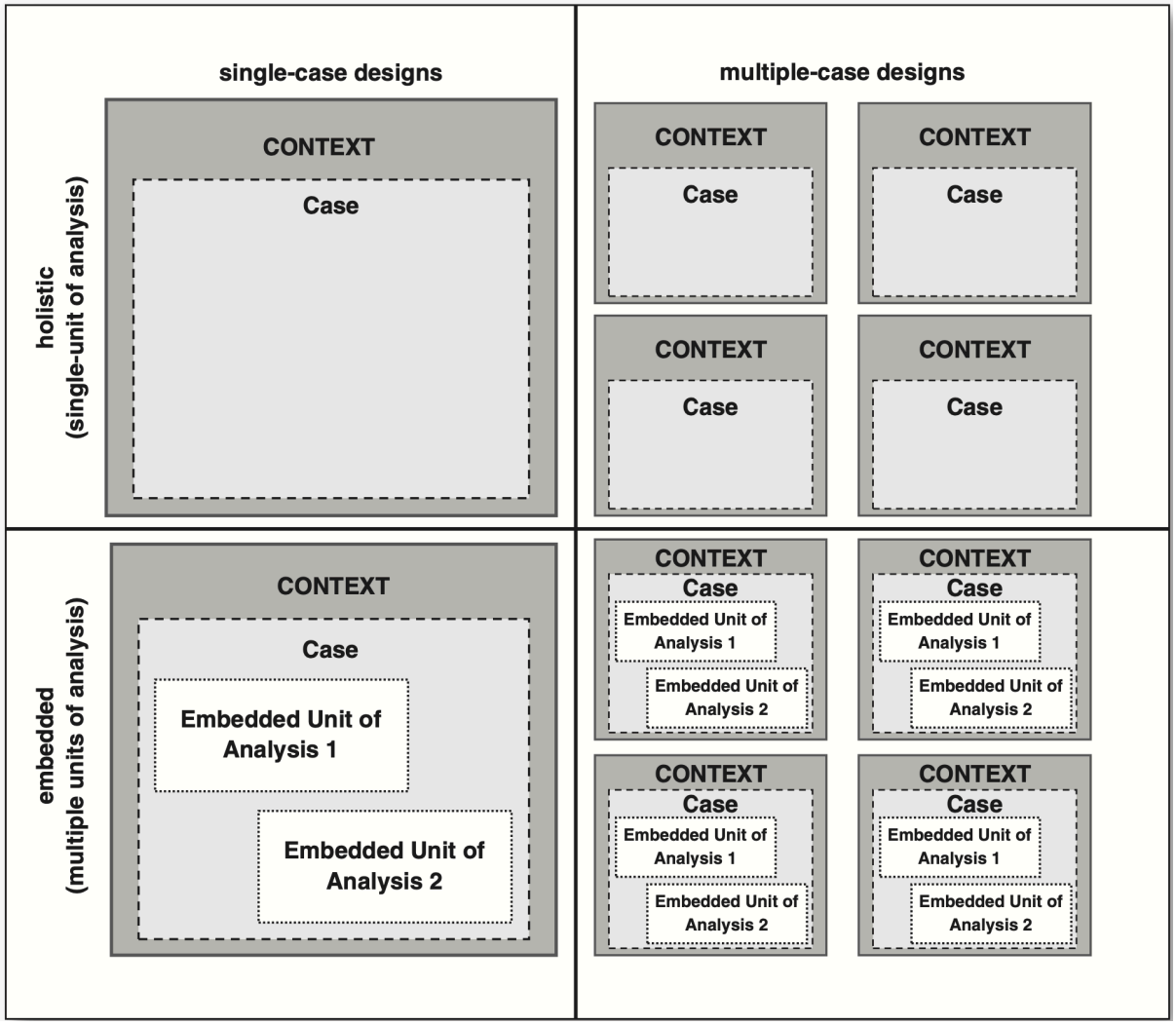


Figure 06. Case Study Types. From Yin (2014).

For this study, a multi-case design will be used, since Apple's and Facebook's cases towards user's privacy will be studied. Each company will have its context presented and their historic with privacy described. Moreover, an embedded approach will be used as two units of analysis will be used for each company: the privacy leverage point framework (Culnan & Armstrong, 1999) and the brand authenticity framework (Fritz et al., 2017).

Since this study aims to analyze these two companies' case through two pre-existent theorical framework, a deductive approach was chosen to analyze the case studies. These companies were chosen because of their relevance to our daily lives. While Apple is mainly focused on hardware, Facebook's core business is software and services. This dichotomy, while being in the same sector and being exposed to data privacy issues, can provide a good discussion to the study. Also important to the subject are Google and Amazon; even though they were considered, they were not included in the main discussion.

Although Google has great relevance in the data privacy scenario, Zuboff (2019) bases most of her thesis on Google's history and behavior. Thus, considering Google in this study would be repetitive since surveillance capitalism is used as a background topic of discussion.

Amazon's recent growth and the projection of becoming one of the most innovative and important companies in the world could justify its selection. However, since Amazon's services are still limited to some specific countries, and its offering is not consistent everywhere, this study only examines Apple and Facebook, which have a strong global presence and a streamlined worldwide offering.

The case study aims to understand how Apple and Facebook have communicated their attitude toward personal data handling. For this, multiple sources were accessed, such as news portals and marketing pieces from the companies. Moreover, the financial reports of the respective companies were obtained from their websites and analyzed to understand how they position themselves strategically regarding privacy.

Furthermore, the Privacy Leverage Point Framework (Culnan & Armstrong, 1999) was used to identify if such companies were capable of leveraging data privacy as a competitive strategy.

More so, each company was analyzed through the Brand Authenticity Framework (Fritz et al., 2017) to understand whether their efforts with data privacy could be incorporated into their branding processes in a way that could be perceived as authentic to consumers; thus, Fritz et al. (2017)'s variables were analyzed as shown in **Table 01**.

Table 01

Influence of identified variables into brand authenticity according to the Brand Authenticity Framework

Variables	Influence on the brand authenticity
Brand Heritage	Within the marketing literature, brand heritage is closely associated with brand authenticity (Brown et al., 2003; Peterson, 2005). According to Fritz et al. (2017), an explanation for brands which communicates their heritage being perceived as more authentic is the suggestion of their durability and consistency. Through this, a brand appears to be more reliable and continuous, indicating, for example, that a brand has a consistent standard of quality. Therefore, communicating and celebrating the company's past, can be seen as a positive effect on brand authenticity. This study aims to understand how Apple and Facebook communicate their heritage. The companies' recent stories and incidents with data privacy were analyzed to understand its heritage with the topic.
Brand Nostalgia	It is assumed that brand nostalgia has a positive effect on brand authenticity. According to Peterson (2005), brands are perceived as more authentic if their communicative appearance involves "former" values. Thus, a brand's communication style that emphasizes a tie with the past can be assumed to be perceived as original, reliable, continuous and natural, as the nostalgic staging connotes stability. Therefore, this study aims to understand how Apple and Facebook treats nostalgia in their communication.
Brand Commercialization	Brands that are regarded as being commercial are known for their intensive, even aggressive, marketing actions (Thompson and Arsel, 2004). In contrast, authentic brands appear to be disinterested in or unconcerned with commercial considerations (Beverland, 2006). Brands which subordinate their values and norms to interests of profit maximization (i.e. brand commercialization) are therefore assumed to have a negative impact on brand authenticity. Therefore, this study aims to understand how data privacy actions connects to Apple's and Facebook's business strategy. The

financial reports of the respective companies were analyzed to understand how data privacy correlates to their business model.

Brand Clarity

According to Fritz et al. (2017), it is expected brand clarity to have a positive effect on brand authenticity. Consistency as a quality of a brand's marketing strategy and communication activities enhances brand clarity and the perception that a brand keeps its promises. However, the presence of contradictions in a brand's appearance creates conflicting signals that undermine the brand's image by weakening brand characteristics such as the brand's originality or naturalness. Moreover, it can be assumed that brand clarity is judged as a sign of reliability by the consumers and can thus positively influence a brand's authenticity. Therefore, this study aims to understand if the promises from the privacy communications are met by Apple's and Facebook's actions.

Social Commitment

Concerning the variable social commitment, Fritz et al. (2017) assume a positive effect on the perceived brand's authenticity, as the assumption of social responsibility is associated with genuine, unique and credible characteristics – aspects describing the brand authenticity dimensions: naturalness, sincerity and, in this context, it is assumed that a company's commitment to social engagement ascribes high moral values to the brand, enhancing perceptions of its authenticity. Therefore, this study aims to understand how social commitment is linked to Apple's and Facebook's business practices. The efforts of each company in contributing to the society were analyzed through their financial reports and the material available at their web sites.

Brand Legitimacy

Fritz et al. (2017) expects brand legitimacy to have a positive effect on brand authenticity. According to self-determination theory, humans strive to satisfy their need for relatedness, which describes a sense of belonging and being accepted by significant others. The more a brand represents the values and norms of the important others, the higher the brand's perceived cultural fit will be, thereby impacting consumer preferences (Rose et al., 1994). Therefore, this study aims to understand if Apple and Facebook incorporated data privacy values and norms into their actions.

Employee's Passion	With regard to the employee-specific variable, Fritz et al. (2017) assume that a positive relationship exists between employee's passion and brand authenticity. Building on research that verifies a positive link between consumer's perception of the brand's employees and the perception of the brand (Värlander, 2009), it is assumed that passionate employees are perceived as authentic, which in turn will be attributed to the brand. Therefore, this study aims to understand Apple and Facebook employee's passion. Both companies were analyzed using employee satisfaction rankings. Moreover, the study ascertained whether employees were responsible for reporting malpractices in data handling.

Adapted from "Authenticity in branding – exploring antecedents and consequences of brand authenticity" by Fritz, K., Schoenmueller, V., & Bruhn, M., 2017, European Journal of Marketing, 51(2), p. 324-348.

The variables of actual self-congruence and ideal self-congruence were not analyzed in this study because they reflect consumer behavior and not direct company actions. Since this study is not analyzing direct customer behavior or opinions, they were excluded.

Results

Apple

Overview. Apple was founded on April 1, 1976, by Steve Jobs and Steve Wozniak, to change the way people view computers. The goal was to make computers small enough for people to have them in their homes or offices, different from the idea at the time that computers should be big and used only by corporations. Apple Inc. has pioneered its way through the industry, not only once with the computer, but several times throughout its existence. Steve Jobs believed in pushing the boundaries of creativity to produce interesting and valuable products for society. After more than 30 years, Apple has had a profound impact on technology and innovation; it influences not only how computers are used but for which activities they are used.

Despite the initial success of the company, Steve Jobs left the company in 1985 to found his own software company, NeXT, as a result of internal political conflicts at Apple. Through the rest of the 1980s, Apple was still doing well, and, by the 1990s, the company had made its biggest profits yet. This situation was, however, largely due to the plans Jobs had already set in motion before he left. Over a few years, Apple's market share suffered slowly after its peak in 1990, and, in 1996, experts believed the company to be doomed. The company was lost in an extensive catalog of products and services, lacking innovation and business focus.

It was not until 1997, when Apple was desperately in need of an operating system, that it bought NeXT Software (Jobs company). Jobs became an interim CEO, and changed the scenario at Apple, introduced the iBook, a personal laptop, and branching out to MP3 players (the iPod) and a media player software (iTunes).

The iPod became a cultural phenomenon and redefined the music sector. Although computers were still an important part of Apple, its music-related products became the company's most profitable, until the launch of the iPhone, the company’s current core revenue product. As the iPod redefined the music industry, the iPhone set a new default for the mobile industry. The company also launched the iPad, a personal tablet, believing it would be the next core for the company; however, it never surpassed the iPhone's cultural and financial importance.

The death of Steve Jobs on October 5, 2011, was a milestone for the company, which was the moment the doubt about the future of the company was mostly raised. Under Tim Cook's command, however, Apple became one of the most valuable companies in the world.

Tim Cook launched the Apple Watch, a smartwatch, starting the company's investment in the wearables sector, and also made the iPad a great substitute for the personal computer.

With the rise of competitors and lack of constant innovation, the iPhone growth had its first decline under Cook's administration during the Q1 2019 fiscal quarter, which includes the 2018 holiday shopping season. Apple reported revenue of $84.3 billion, which was a decline of 5 percent from one year ago; it was the first decline for both revenue and profit in a holiday quarter that Apple has posted since the iPhone's introduction more than a decade ago (Welch, 2019).

The decline in revenue and sales prompted a fast response from the company, calling a general staff meeting to discuss the future of the company and produced a public letter to investors. Four months after, Apple announced in a keynote that it would start investing in the service sector, with the launch of Apple TV+, a video streaming service with original content produced by Apple itself; Apple News+, a subscription service for the most famous magazines and newspapers; Apple Arcade, a curated subscription service of mobile games; and Apple Card, an credit card created by Apple, expanding the Apple Pay service.

Apple and privacy. Although Apple has confronted Google and Facebook since the 2000s by stating that Apple sells computers, while others sell user data, it was only from 2014 that privacy and Apple started to be correlated in the news, around which time iOS8 was launched.

Apple and the government had been at odds for more than a year since the debut of Apple's encrypted operating system, iOS 8, in late 2014. It added stronger encryption than before in smartphones. It encrypted all user data—phone call records, messages, photos, and contacts—with the user passcode. The encryption was such that not even Apple could break it (Kahney, 2019). The discussion of the need for a government backdoor in the iPhones started to be raised by local authorities, especially in the US.

The most polemic episode occurred in 2016 when the FBI asked Apple to unlock the iPhone used by the man responsible for the terrorist attack in San Bernardino, California, in December 2015, where 14 people were killed and 22 injured. Apple replied by saying that it

was not possible and that there were no backdoors, and they would never develop one in its products because once it was developed, anyone (e.g., governments, dictators, terrorists, and hackers) could possibly have access to it. The FBI made this a public matter, saying Apple was defending terrorists instead of protecting America, which made Apple publish an open letter saying that their bigger commitment was with privacy and security of their client's data (Khamooshi, 2016).

After this incident, Apple was forced to make privacy a public discussion point. However, it was only in 2019 that this speech got stronger. Apple started 2019 with a fascinating billboard in Las Vegas (see **Appendix A**) in a building next to the venue of the CES (Consumer Electronics Show), which is an electronic fair Apple does not regularly participate in; however, Google and Facebook are always present. Positioned not far from the convention center was a sign which stated that "what happens on your iPhone, stays on your iPhone," a reference to the famous "what happens in Vegas stays in Vegas." The move cast an Apple-shaped shadow over the convention (Ingraham, 2019).

It can be argued that Apple started to be more aggressive in the data privacy field only after its iPhone's sales stop growing. Moreover, it is a strategy to better position its new data concerned services, which were launched later in 2019.

Apple services were pitched not only as intuitive but also "designed to keep your personal information private and secure." As each new product was presented in its launch, Tim Cook emphasized how careful they were about the data involved and how much they prized the user's privacy. Apple affirmed that they would never have access to the kind of news read on Apple News+, the kind of series watched on Apple TV+, or where one spends money with the Apple Card (Brandom, 2019). Since there is a serious lack of trust in the tech industry, Apple wants to differentiate itself from the competitors as the only tech company people can trust, which can be very rewarding to the company since it has always invested in a closed ecosystem strategy. Customers that have Apple products tend to agree with the whole offering of the company.

However, Apple has also been criticized for privacy breaches, such as the FaceTime bug, which allowed people to access the iPhone microphone without user consent (Bohn, 2019). Moreover, Apple was recently criticized for allowing contractors to listen to voice recordings of Siri users to grade them (Hern, 2019). The problems were rapidly addressed and

fixed. In both cases, Apple apologized and changed its process in favor of user privacy. The company even made the sharing of audio snippets from Siri optional (see **Appendix B**), which was not made by Google Assistant or Amazon Alexa, its biggest competitors.

Apple's efforts with data privacy were reinforced with the launch of the iPhone 11, iOS 13, and macOS Catalina. The company released an easy to read and attractive looking webpage explaining its position on data privacy and how its services, software, and devices are designed to properly handle user data. It also dedicated two of the six ads of the new iPhone 11 to Apple's care for data protection (see **Appendix C**).

The Apple privacy website (see **Appendix D**) presents privacy as a fundamental human right and a core value of Apple. According to them, the devices are important in the lives of many users, and what they share from those experiences, as well as whom they share it with, should be up to them. For that, Apple has some general strategies to protect user data:

***Web browsing*.** Safari uses Intelligent Tracking Prevention to stop advertisers from following the user from site to site.

***Location data*.** The Maps app does not associate data with the Apple ID, and Apple does not keep a history of where the user has been.

***Photos*.** The Photos app uses machine learning to organize photos on the device. Every photo stored on the cloud is encrypted; Apple cannot access them. Given that the processing takes place locally, it is not necessary to share them with Apple or anyone else.

***Siri recordings*.** The Apple ID is not connected to Siri, and the requests made are associated with a random identifier.

***Apple news+*.** Apple News leaves what is read off the record. Apple News delivers content based on interests, but it is not connected to any identity. Thus, Apple does not know what is read.

Apple card. The Wallet and Apple Pay apps hide purchases. Credit and debit card numbers are hidden, and Apple does not keep information that can be tied back to the user.

Health. The Health app keeps records under wraps. The user can control which information goes into the Health app and with whom it is shared.

Sign in with Apple. "Sign in with Apple" is a convenient way to sign in to apps and sites while having more control over the information shared. Apps are restricted to asking only for the user's name and email address, and Apple will not track app activity or build a profile of the user. This system was a great way of limiting Google's online presence.

Messaging. End-to-end encryption protects iMessage and FaceTime conversations across all devices. Messages are encrypted on the device; thus, there is no way for Apple to read the messages when they are in transit between devices.

On-device intelligence. Apple uses machine learning to enhance user experience and privacy by using on-device processing; all the data is gathered using only the device. Moreover, it is never sent to Apple. The A13 Bionic chip and the Neural Engine in iPhone can recognize patterns, make predictions, and learn from experience. Therefore, the device can create personalized experiences without having to analyze personal information on Apple servers.

By analyzing Apple's position with data privacy, it can be argued that the company has a privacy leverage point. According to Culnan and Armstrong (1999), the actions by the company, especially the on-device intelligence strategy, play in favor of the user privacy calculus. Since the benefits of disclosing data to Apple seem to be less risky than the benefits of using their products and services, it is perceived that the company treats user data with procedural fairness. Therefore, customers perceive that the practice matches the policy. This perception may lead to customer retention and the attraction of new customers, thereby generating a privacy leverage point.

Apple's brand authenticity. Apple's move to communicate their care for personal privacy data was analyzed using the Brand Authenticity Framework (Fritz et al., 2017).

Brand heritage. Although Apple has invested heavily in data privacy, it also faced some unfortunate incidents. Even so, the company always responded with a good level of responsibility. In the San Bernardino case and the Siri and FaceTime incidents, Apple maintained a good level of consumer relationship quality because of the standard and persistent position regarding the rights of the customer. Thus, just as Fritz et al. (2017)'s framework predicted, Apple was forgiven.

Brand nostalgia. Apple is a company that proudly remembers and celebrates its past, mainly because of the trajectory of Apple's former CEO, Steve Jobs, who is recognized as a visionary and still impacts the company until today. Not only that, the company is proud of

being responsible for the revolution of the personal computer market. For example, in 2014, the company celebrated the 30th anniversary of the Mac (see **Appendix E**). Being proud of its history impacts positively on the perception of its present acts as trustworthy.

***Brand commercialization*.** For almost a decade, Apple's core revenue product is the iPhone. Although the smartphone has been losing share in the company's revenue, it still represents 54% (see **Appendix F**). It is reasonable to believe in Apple's privacy claim because the company does not profit mostly on its services, which represents 20% of its revenue. For the time being, hardware sales still comprise most of the company income, resulting in lower business pressure for the exploitation of the behavioral surplus.

Brand clarity and legitimacy. Apple has been silently making the case about privacy for some time. It was the first company to build a dedicated microchip that would encrypt biometric data (first the fingerprint with Touch ID and now the mathematical representation of the user's face with Face ID). Different from Google and Amazon, Apple does all the AI processing in the device, thus making sure that what must go through Apple's servers is encrypted, and the company cannot read it. Moreover, the company has been successful in simply and directly communicating these efforts customers. **Appendices A, B, C,** and **D** presents examples of communications that are easy to understand and enjoyable to look at.

***Social commitment*s.** Since customers perceive the company as a whole and not only regarding the privacy matter, the social commitment of an enterprise is important to help customers believe that corporate actions can be done in favor of the society rather than just aiming for profit. Apple communicates a lot about its environmental efforts (see **Appendix G**), saying that genuinely innovative products leave their mark on the world instead of the planet. The company has invested in recyclable energy and launched a trade-in policy, in which the customers receive credit during purchases if they give out an old device for recycling. This strategy is excellent since the company is developing its new products with 100% recyclable aluminum. Given these efforts, the company is recognized as a critical environmental player in the tech industry.

Employee passion. Apple has a strong culture of secrecy; thus, it is hard to have access to employees' vision of the company. The secrecy is pointed by the Glassdoor 2019 Best Places to Work award, in which Apple took the 71st position. Apple is not present in the Fortune 100 Best Companies to Work For. Although this is not an outstanding position, Apple is known for

having advocate employees. One example of this is that Apple has not witnessed any leak of user data malpractice from an employee complaint.

In general, after analyzing these variables, it is possible to say that Apple's moves towards data privacy have a high chance of being perceived as authentic since most it correlates with the speech and the actions of the company. Apple has long been leading the way of how to position a company through a believable privacy claim.

However, whether their claim will stand the test of time remains to be seen because it is easier to defend something when it does not affect your core business directly. With the slow-growing previsions for the iPhone lines and with the massive investment in services, it must be monitored if the privacy claim will still be defended when services hold a more significant share of Apple's revenue (given the current position on hardware).

Facebook

Overview. Facebook was launched on February 4, 2004. The creators were students at Harvard University. Initially, the service was simple and only worked on campuses; it worked like a digital yearbook for Harvard students. Although launched in 2004, Facebook originates from another site.

In 2003, Mark Zuckerberg already had a relatively praised website called FaceMash. It compared photos of university students and let people compare two photos and choose the most beautiful person between them. The site was a success, but raised many complaints; thus, it was taken down. Another barrier for this tool was that it used the institution's database without authorization; the university issued a warning, and Mark apologized.

In January 2004, Mark began to write new code, which became the first version of Facebook; it was entirely coded in his dorm. The concept was quite straightforward: a directory that had the profiles and pictures of all Harvard students. At that time, one could add friends and check out their profile information. In March, it expanded to Stanford, Columbia, and Yale.

With no campus space, the team moved to Palo Alto, California. Mark had a very young team at the time. Dustin Moskovitz is a co-founder and was the first head of technology and

later engineering. The third of the pioneers is Chris Hughes, a company spokesperson for many years. There is also the Brazilian, Eduardo Saverin, who was the chief financial officer.

Facebook's first controversy came during its first year. The twins, Tyler and Cameron Winklevoss, and the programmer, Divya Narendra, alleged that they came up with a Facebook-like idea in 2002, ConnectU. According to them, almost all the code was ready, and Mark joined the team for a few weeks, but dropped the project, launching Facebook sometime later. The twins sued Zuckerberg for stealing the idea, and in 2008 received about $65 million in a settlement.

The year of expansion proved to be 2005; the site opened registrations for high school students and removed the "The" from the name, becoming just Facebook. It finally implemented photo posting in October and, in December, the ability to tag friends on images. In April 2006, the mobile version of the network went live and, in September, the news feed debuted. The next year marked the launch of the marketplace marketing, video posting, people, or business pages. Moreover, it was the year of the first F8, which is an annual conference with announcements of new Facebook features.

In 2008, Facebook began internationalization with a Spanish version and Connect, which is a way of using the Facebook account as a signing-in feature to other services. February 2009 marks the implementation of the most notable feature: The "Like" button. In the next year, a series of protests in the Arab world (the Arab Spring) alerted the world to the importance of social networking in politics.

The first significant acquisition of the company was made in 2012, when Instagram, a social network focused primarily on images, was bought for $1 billion. The year also marks the initial public offering of the brand shares, which, at the time, was the biggest Internet company in the United States. The next acquisition takes place in 2014 for $19 billion when WhatsApp, a multiplatform instant messaging app, joined the Facebook group. Later that same year, the virtual reality company, Oculus Riff, was acquired. The Facebook interface evolution can be seen in **Appendix H**.

In 2019 Facebook revealed its intention of creating a new cryptocurrency called Libra, which would be a global standard, allowing people from all over the world to exchange money with lower rates. Initially, the project was designed with the sponsorship of the biggest online financial companies, such as PayPal, Visa, Mastercard, eBay, Stripe, and Mercado Pago, in

mind. However, all of them withdrew from the Libra Association after the negative response from the North American government about Facebook's plans. Currently, it is unclear how this project will develop.

Facebook remains the world's largest social network. With more than 2.5 billion active users, it is unlikely to be overthrown in the short term, but criticism has never been stronger. Many people have deleted their profile or switched to small competitors because they do not like the content or the lack of privacy on the network.

Facebook and privacy. Facebook's relationship with privacy has been complicated from its start. The site that preceded the social network, called FaceMash, accessed and published photos from Harvard students without their consent. Since then, Facebook has been involved in several polemic incidents, the most famous of which is the Cambridge Analytica case.

In 2018, Facebook announced that it had suspended its Strategic Communication Laboratories (SCL), along with its political data analytics firm, Cambridge Analytica, for violating its policies around data collection and retention. These were the same companies that participated in the Donald Trump's 2016 presidential election campaign.

It was discovered that they could better target users for political ads because of a base of user data illegally obtained through an app named "thisisyourdigitallife" that promised to predict aspects of users' personalities. About 270,000 people downloaded it and logged into Facebook, thereby giving the company access to information about their city of residence, Facebook content they had liked, and information about their friends. This situation allowed Cambridge Analytica to access as many as 50 million Facebook profiles (Newton, 2018). These events were made public after an unidentified former worker from Cambridge Analytica reported. According to him, Facebook was years ago aware of the cache of user data Cambridge Analytica had and asked the company to delete it; however, Facebook never followed up or confirmed the deletion of the data.

Facebook quickly responded to the incident, claiming that they would revoke SCL's and Cambridge Analytica's access to Facebook apps and would no longer allow third-party data for targeting ads to mitigate potentially vulnerable ad practices (Statt, 2018). Even so, the market response was strong. The company's market value dropped by nearly 7 percent, which is the most that Facebook has fallen in a single day in over six years (see **Appendix I**).

Mark Zuckerberg apologized for the incident, saying that it was a significant breach of trust, and Facebook would now be responsible for making sure that it does not happen again. The CEO also promised to raise the number of people working on security and community operations from 15000 to 20000 (Newton, 2018).

The next chapter of the scandal was the Zuckerberg appearance before the Senate, where he defended the web tracking behavior of the Facebook algorithm. According to him, the first reason for tracking is security. If Facebook did not track people, the platform could not prevent someone from downloading every public Facebook page. Even if someone is not logged in, Facebook tracks certain information, like how many pages are being accessed, as a security measure. Ad targeting was presented as a secondary reason.

However, the event was shocking because it showed how the Senators knew little about the topic. They posed fundamental questions about the features of the data collection and advertising practices, thereby failing to discuss more profound questions about how Facebook uses the data it collects (Davies, 2019).

Since the Cambridge Analytica scandal, very little seemed to have changed. Facebook was fined a record penalty of $5 billion by the Federal Trade Commission (FTC) for deceiving users about their ability to keep their personal information private (Lomas, 2018). Since the market expected a higher fine, the company stock price rose despite the record fine.

Despite the public discussion, the promises of change, and the declarations in front of the Senate, Facebook continued to be involved in privacy breaches. A former Facebook employee reported that users' telephone numbers that were given for the configuration of the two-factor authentication, a security technique that adds a second layer of authentication to help keep accounts secure, were being used to target ads (Constine, 2019).

In a more controversial report, another former employee revealed that Facebook had been secretly paying people to install a Facebook Research VPN that lets the company access the phone and web activity of users (see **Appendix J**). Since 2016, Facebook has been paying users ages 13 to 35 up to $20 per month to sell their privacy by installing the Facebook Research app (Schiffer, 2019). The program was through the beta testing services Applause, BetaBound, and uTest to cloak Facebook's involvement, which is referred only as Project Atlas. After a strong wave of criticism, Facebook canceled the Project Atlas and launched the Viewpoints app (Peters, 2019). Rather than focus on the use of third-party apps, it gives money rewards to

users after completing tasks, such as filling out surveys and testing new products. The first available survey concerned well-being and technology.

The public image and trust of Facebook have been suffering; one evidence of it was the #deleteFacebook movement. Celebrities and well-known businesspeople participated in the online movement that tried to raise awareness of the company's malpractices with user data. Even WhatsApp co-founder, Brian Acton, participated in the movement (see **Appendix K**).

As an attempt to change this narrative, Facebook launched a new interface for the user privacy setting, simplifying settings that were earlier fragmented (see **Appendix I**). This new design helped the user to understand the people to whom their posts were shared, which apps were connected to the account, and which personal information was stored on Facebook. Although it was a good improvement to the platform, it did not change how Facebook handled data, which was only disclosure in a centralized way to store static data.

In a second and most recent attempt to improve the company's image, Zuckerberg addressed, in an open letter, his vision about the principles around building a privacy-focused messaging and social networking platform. In a very straightforward letter, he stated that he sees a change in how people deal with social networks and that their products should follow the same pattern of private, encrypted, and safe sharing of information (Zuckerberg, 2019). In his open letter, he defends the following:

Private interactions. People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.

Encryption. People's private communications should be secure. End-to-end encryption prevents anyone (including Facebook) from seeing what people share.

Reducing permanence. People should be comfortable being themselves and should not have to worry about what they share, given that it could be used to hurt them in the future. Facebook will not keep messages or stories for longer than necessary.

Safety. People should expect that Facebook will do everything possible to keep them safe within the limits of what is possible in an encrypted service.

Interoperability. People should use any of the Facebook apps to reach their friends, and they should communicate across networks easily and securely.

Secure data storage. People should expect that Facebook will not store sensitive data in countries with weak records on human rights, such as privacy and freedom of expression, to protect data from being improperly accessed.

Although all those promises match the customer's expectations, none of them were previously applied. These were only promises of a future platform. Doubts about the accuracy of these affirmations rose, especially after the California Attorney General, Xavier Becerra, said that Facebook has refused to comply with its subpoenas to provide more information regarding its investigation into another company's alleged privacy violation (Kelly, 2019). Moreover, since most of Facebook's revenue comes from advertising, it is unclear how it would profit if all the promises were delivered.

Given Facebook's position regarding data privacy, it can be argued that the company does not have a privacy leverage point. According to Culnan and Armstrong (1999), several privacy incidents the company has faced, and the kind of response it presented, do not show procedural fairness, thereby raising the privacy calculus done by the user. Since it is perceived that practice does not match policy, users participate in bad word of mouth and do not create a privacy leverage point, thus hurting the company's trust image.

However, as opposed to the framework, Facebook has not seen a drop in the number of users, which is a direct consequence of the oligopoly power that the company exercise in this sector. Despite the drop of users from the #deleteFacebook movement, the number of new users from developing markets was higher. Furthermore, since April 2018, which was the first full month after news of the Cambridge Analytica scandal broke in, actions on Facebook, such as likes, shares, and posts, dropped by almost 20%, according to the business analytics firm Mixpanel (see **Appendix M**).

Although the number of users has not changed significantly, Facebook has seen the rise of a competitor. The TikTok mobile app reached 1.5 billion downloads in 2019, making it the third most downloaded app in the world, and the only one not owned by Facebook in the top 5; Instagram is the fourth most downloaded app (Hamilton, 2019).

Moreover, despite the insignificant effect on the number of users, the lack of trust in Facebook is affecting its diversification strategy. The public and governmental concern of the company's plans of creating a global cryptocurrency scared all of its biggest partners. Now the future of Libra is unknown.

Facebook's brand authenticity. Facebook CEO's promises were bold but were received with much skepticism. This study analyzed Facebook using the Brand Authenticity Framework (Fritz et al., 2017).

Brand heritage. Facebook has a negative heritage when it comes to data privacy. The Cambridge Analytica case alone is already enough to illustrate how damaged the brand heritage is right now. Moreover, Zuckerberg's defense of the company's tracking behavior in front of the Senate only reinforces his real mindset.

Brand nostalgia. Facebook does not celebrate its past. Quite the contrary, since its origins came from the exploitation of the Harvard students' data without their consent and, with the recent privacy scandals, Zuckerberg's statements are centered mainly on the future of the company rather than its past.

Brand commercialization. Facebook's business model puts a significant doubt on whether Zuckerberg's promises are possible. Its main revenue source is from advertisers that can create segmented filters. This revenue source represents 98.9% of the company's revenue (see **Appendix N**). It is hard to believe that Facebook would make any change to the handling of user data, which could harm its advertisement system.

Brand clarity and legitimacy. It is hard to credit Zuckerberg's promises as legit since the company has been directing its efforts to advertisers and not users. One good example of this kind of mindset was when Instagram, a Facebook product, changed the way it would show the user's photo grid from a linear to a relevancy format, adding ads in the middle of the content. The repercussion of this change was massively negative. However, Facebook insisted on maintaining it (Lua, 2018). The same can be seen with Facebook's newsfeed; although it keeps changing for improvement, user feedback only goes down every time they conduct a new survey (Tassi, 2019).

Social commitment. Although the company has some interesting educational programs, such as the hack labs, these actions are obscured by the recurring scandals on the media. Facebook is not recognized as a positive social agent, especially after the Cambridge Analytica

case, where the public opinion turned against Facebook after people realized the seriousness and vastness of the privacy breach. Moreover, as it was linked to the Trump Presidential Election, it only made the case more polemic.

Employee's passion. Despite all the polemics, Facebook is recognized as a great place to work. Facebook was 7th in the Glassdoor 2019 Best Places to Work award but was not present in the Fortune 100 Best Companies to Work For. Although this is a great position, Facebook is noted for having employees that leak the company's malpractices in the handling of user data.

Generally, after analyzing these variables, it is possible to say that Facebook's actions towards data privacy have a low chance of being perceived as authentic since most of its users do not correlate company statements with the actions of the company. To be trusted, the company will have to act and be recognized by the results of its new policies.

Since these variables do not contribute positively to brand authenticity, the company's active involvement is mandatory to ensure a good brand relationship quality. That is, their actions will weigh more than their open letters.

In Facebook's case, data privacy was not a strategic advantage for its brand. During the first rounds of developing the business model of Libra, Facebook's bad reputation loomed negatively on the initiative, thus driving away its partners and weakening its new product even before it was launch. In less than three weeks, Libra went from the revolution of digital payments to a colossal "incognita." Insisting on the idea, Facebook launched Facebook Pay, which is considerably smaller in scope and relevance than Libra could have had.

Conclusions

The numerous data-related incidents reported by the media in the last couple of years is evidence of the relevance of the data privacy topic. The conflicts from the harvesting of customers' private data will define the fight for a human future at the new frontier of power (Zuboff, 2019). There is no doubt that the subject has reached an unprecedented awareness level with the tendency of increasing, given the economic incentives that harvesting customer's behavioral surplus can provide. Therefore, managers need to be aware and participate in the construction of this discussion.

Using the privacy leverage point framework (Culnan & Armstrong, 1999), it was possible to reach the conclusion that Apple is well positioned in the privacy perspective. The company has constructed a consistent timeline of actions, especially with the San Bernardino case, in which the direct conflict with the government in defense of the customer's privacy rights reflected positively on the business's image.

However, the brand authenticity framework (Fritz et al., 2017) renders Facebook's promises of privacy commitment as not believable. The main argument against the company is its bad heritage regarding the topic and the composition of its revenue. Since Facebook is organized toward profiting from ads, it seems that its customers are the advertisers and not the users. With this reality in mind, it is hard to believe in Zuckerberg's attempt at positioning Facebook as a privacy concerned company. As he likes to state: the future is private. But, is it really?

Apple is in a very comfortable position, while the hardware sales generate the core revenue of the company. However, as the firm shifts towards a service-focused company and iPhone sales continue to drop, whether the market pressures will induce a data policy change remains to be seen. Even so, Apple's on-device intelligence is competitive and provides a different approach to user data processing, which is not used by its main competitors. The company can do it thanks to its level of vertical integration. Since Apple designs and manufactures its security chips, the corporation has reached a great position of advantage.

Data privacy is already being used as a strategic competitive advantage, as in the Apple case. However, it is important to pay attention to the authenticity of the move. The brand map of the company must incorporate this positioning attempt; otherwise, it can shift from a

strategic competitive advantage to a strategic competitive disadvantage, like in Facebook's case.

The communication of data privacy as a strategic advantage can hurt a brand when it is not perceived as authentic. Facebook suffered this with the Libra attempt and has been facing lower engagement since the Cambridge Analytica case. Thus, the only option for rescuing the quality of the brand relationship is with a consistent action plan from the company towards its brand image.

The study of managerial implications in private data handling is new and lacks an in-depth understanding of the cause and effect of the company actions regarding its brand reputation. Moreover, since this study is limited to analyzing company actions and communication pieces, further studies on the consumer perspective are recommended. This study employed the assumption that customers value data privacy handling as an advantage, which has to be confirmed through additional quantitative research.

For future studies, it is important to understand whether the impacts of user data handling may equally impact companies from sectors other than technology enterprises. Moreover, it is important to understand whether users from developing markets value their digital privacy or prioritize their access to online services regardless of the privacy implications. In other words, an interesting and important scope for further studies is if the privacy calculus and the brand authenticity framework are consistent across developed and developing markets and industry sectors.

The concept of surveillance capitalism; and the highlight it presents of the economic incentives there are to harvest users' data, are a good reason of why the business sector should pay attention to how this market will be regulated in the future. Since data may be the new valuable commodity, companies should be prepared not to only be able to capture and analyze this data strategically, but also position itself on how the data is handle and protected. As this market grows, more and more sectors will be impacted by the need of handling data, therefore, the discussion of user data as a competitive advantage will be relevant across-sectors and not only limited to "big-tech".

Research on these topics may mold the future of how companies treat user data and how it may impact relations in an information-based society. The recent data breaches revealed the importance of the topic to the public. As the thunder from a bigger storm that may yet be

looming ahead, they served as a warning. Amnesty International states that the Facebook and Google surveillance is an assault on privacy because millions of people have no meaningful choice but to access the online public space on terms dictated by them and not governments (Schiffer, 2019). Studies on data privacy and its use in branding processes can bring valuable data to this discussion and help governments regulate them effectively.

"If there were no thunder, men would have little fear of lightning."

— Jules Verne, Twenty Thousand Leagues Under the Sea

References

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Beverland, M.B. (2006). The real thing: branding authenticity in the luxury wine trade. *Journal of Business Research*, 59(2), 251-258.

Bohn, D. (2019, January 28). Serious FaceTime bug allows you to listen remotely before anyone answers — Apple to fix 'later this week'. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2019/1/28/18201383/apple-facetime-bug-iphone-eavesdrop-listen-in-remote-call-security-issue

Brandom, R. (2019, March 26). Apple wants to be the only tech company you trust. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2019/3/26/18282158/apple-services-privacy-credit-card-tv-data-sharing

Brown, S., Kozinets, R.V. and Sherry, J.F. Jr. (2003). Teaching old brands new tricks: retro branding and the revival of brand meaning. *Journal of Marketing*, 67(3), 19-33.

Burgoon, J. K. (1982). *Privacy and communication*. Communication Yearbook, 6, 206–249.

Cavoukian, A. and Castro, D. (2014). Big Data and Innovation, Setting the Record Straight: De-identification Does Work. Office of the Information and Privacy Commissioner. Ontario, Canada.

Chaudhry, A. (2019, November 20). Uber will start audio-recording rides as a safety measure. Retrieved November 20, 2019, from The Verge website: https://www.theverge.com/2019/11/20/20974814/uber-audio-recording-rides-safety-rideshare-lyft

Constine, J. (2019, January 29). Facebook pays teens to install VPN that spies on them. Retrieved November 01, 2019, from TechCrunch website: https://techcrunch.com/2019/01/29/facebook-project-atlas/

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches*. 4th ed. Thousand Oaks, California: SAGE Publications.

Culnan, M. and Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104-115.

Davies, R. (2019, July 24). Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint. Retrieved November 01, 2019, from The Guardian website: https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint

Dienlin, T. and Metzger, M. J. (2016), An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample, *Journal of Computer-Mediated Communication*, 21, 368–383.

Fritz, K., Schoenmueller, V., & Bruhn, M. (2017). Authenticity in branding – exploring antecedents and consequences of brand authenticity. *European Journal of Marketing*, 51(2), 324–348.

Garrahan, M., & Kuchler, H. (2018, March 18). Facebook in storm over Cambridge Analytica data scandal. Retrieved March 25, 2019, from Financial Times website: https://www.ft.com/content/828e50ac-2ace-11e8-a34a-7e7563b0b0f4

Hamilton, I. A. (2019, November 18). TikTok hit 1.5 billion downloads, and is still outperforming Instagram. Retrieved November 18, 2019, from Business Insider website: https://www.businessinsider.com/tiktok-hits-15-billion-downloads-outperforming-instagram-2019-11

Hern, A. (2019, August 29). Apple apologises for allowing workers to listen to Siri recordings. Retrieved November 01, 2019, from The Guardian website: https://www.theguardian.com/technology/2019/aug/29/apple-apologises-listen-siri-recordings

Hoeyer, K. (2009). Informed Consent: The Making of a Ubiquitous Rule in Medical Practice. *Organization*, 16(2), 267–288.

Ingraham, N. (2019, January 05). Apple took out a CES ad to troll its competitors over privacy. Retrieved November 01, 2019, from Engadget website: https://www.engadget.com/2019/01/05/apple-ces-2019-privacy-advertising/

iPhone Privacy. (n.d.). Retrieved March 25, 2019, from Apple website: https://www.apple.com/privacy/

Kahney, L. (2019, April 16). The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No. Retrieved November 01, 2019, from Wired website: https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi

Kaye, J., et al. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetic*, 23, 141–146.

Kelly, M. (2019, November 06). Facebook isn't complying with privacy probe, California attorney general says. Retrieved November 10, 2019, from The Verge website: https://www.theverge.com/2019/11/6/20951936/facebook-cambridge-analytica-investigation-california-court-order-documents

Khamooshi, A. (2016, March 21). Breaking Down Apple's iPhone Fight With the U.S. Government. Retrieved November 01, 2019, from The New York Times website: https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22–42.

Lind, E. A. and Tyler, T. R. (1988). *The Social Psychology of Procedural Justice*, New York: Plenum Press.

Lomas, N. (2018, September 27). Yes Facebook is using your 2FA phone number to target you with ads. Retrieved November 01, 2019, from TechCrunch website: https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/

Lua, A. (2018, June 14). How the Instagram Algorithm Works in 2019: Everything You Need to Know. Retrieved November 01, 2019, from Buffer website: https://buffer.com/library/instagram-feed-algorithm

Malhotra, N. K. (2012). *Pesquisa de Marketing. Uma orientação aplicada.* Porto Alegre: Bookman.

Narayanan, A. and Felten, E. W. (2014, July 9). No silver bullet: De-identification still doesn't work. Retrieved November 01, 2019, from IAPP website: http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf

Newton, C. (2018, March 16). Facebook suspended Donald Trump's data operations team for misusing people's personal information. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2018/3/16/17132172/facebook-cambridge-analytica-suspended-donald-trump-strategic-communication-laboratories

Newton, C. (2018, April 10). The 5 biggest takeaways from Mark Zuckerberg's appearance before the Senate. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119-157.

Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701.

Peters, J. (2019, November 25). Facebook launches new market research app after shutting down its controversial VPN service. Retrieved November 25, 2019, from The Verge website: https://www.theverge.com/2019/11/25/20982367/facebook-viewpoints-new-market-research-app-study-survey-rewards

Peterson, R.A. (2005). In search of authenticity. *Journal of Management Studies*, 42(5), 1083-1098.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Quach, K. (2017, July 26). iRobot just banked a fat profit. And it knows how to make more: Sharing maps of your homes. Retrieved November 01, 2019, from The Register website: https://www.theregister.co.uk/2017/07/26/irobot_q2_fy2017_roomba_maps/

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, R. E. Petty, & R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153 – 177). New York: Guilford Press.

Rose, G.M., Shoham, A., Kahle, L.R. and Batra, R. (1994). Social values, conformity, and dress. *Journal of Applied Social Psychology*, 24(17), 1501-1519.

Schiffer, Z. (2019, November 08). WhatsApp co-founder Brian Acton still thinks you should delete Facebook. Retrieved November 10, 2019, from The Verge website:

https://www.theverge.com/2019/11/8/20955638/whatsapp-brian-acton-facebook-delete-mark-zuckerberg-signal-encryption

Schiffer, Z. (2019, November 20). WhatsApp co-founder Brian Acton still thinks you should delete Facebook. Retrieved November 20, 2019, from The Verge website: https://www.theverge.com/2019/11/20/20974832/facebook-google-surveillance-data-assault-privacy-amnesty-international

Singer, N. (2018, July 26). Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says. Retrieved November 01, 2019, from The New York Times website: https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html

Solon, O. (2018, July 13). 'Data is a fingerprint': why you aren't as anonymous as you think online. Retrieved November 01, 2019, from The Guardian website: https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy

Solove, D. (2008). *Understanding Privacy*. United States: Harvard University Press.

Stake, R. E. (1995). *The art of case study research*. United States: Sage.

Statt, N. (2018, March 28). Facebook will no longer allow third-party data for targeting ads. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2018/3/21/17150158/mark-zuckerberg-cnn-interview-cambridge-analytica

Tassi, P. (2019, January 18). Facebook Is Terrible Not Because It's Evil, But Because It's Terrible. Retrieved November 01, 2019, from Forbes website: https://www.forbes.com/sites/insertcoin/2019/01/18/facebook-is-terrible-not-because-its-evil-but-because-its-terrible/

Thielman, S. (2017, January 10). Your private medical data is for sale – and it's driving a business worth billion. Retrieved November 01, 2019, from The Guardian website: https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns

Thompson, C.J. and Arsel, Z. (2004). The starbucks brandscape and consumers' (anticorporate) experiences of glocalization. *Journal of Consumer Research*, 31(3), 631-641.

Tieman, S. (2016, October 16). Lessons from the front lines of digital advertising. Retrieved November 01, 2019, from Accenture website: https://www.accenture.com/us-en/insights/digital/see-people-not-patterns

Värlander, S. (2009). The construction of local authenticity: an exploration of two service industry cases. *Service Industries Journal*, 29(3), 249-265.

Walker, C. S. (2018, July 9). Twitter's vast metadata haul is a privacy nightmare for users. Retrieved November 01, 2019, from Wired website: https://www.wired.co.uk/article/twitter-metadata-user-privacy

Warren, S. D and Brandeis, L. D. (1890), The Right to Privacy, *Harvard Law Review*, 4, 193-220.

Waters, R. (2019, March 28). Five things we learnt from Apple's latest launch. Retrieved March 28, 2019, from Financial Times website: https://www.ft.com/content/06c37e6c-516e-11e9-b401-8d9ef1626294

Welch, C. (2019, January 29). Apple's iPhone sales revenue fell 15 percent during holiday quarter. Retrieved November 01, 2019, from The Verge website: https://www.theverge.com/2019/1/29/18201562/apple-earnings-iphone-sales-revenue-fall-drop-holiday-quarter-q1-2019

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Whitley, E. A. (2009). Informational privacy, consent and the “control” of personal data. *Information Security Technical Report*, 14 (3), 154-159.

Whittaker, Z. (2017, July 14). Homeland Security says Americans who don't want faces scanned leaving the country "shouldn't travel". Retrieved November 01, 2019, from ZD Net website: https://www.zdnet.com/article/americans-depart-us-faces-scanned-privacy-worries/

Yin, R. K. (2014). *Case Study Research Design and Methods*. United States: Sage.

Zuboff, S. (2019). *The Age of Survaillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. United States: Public Affairs.

Zuckerberg, M. (2019, March 6). A Privacy-Focused Vision for Social Networking | Facebook. Retrieved March 25, 2019, from https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

2018 reform of EU data protection rules. European Commission. May 25, 2018. url: ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

Appendix

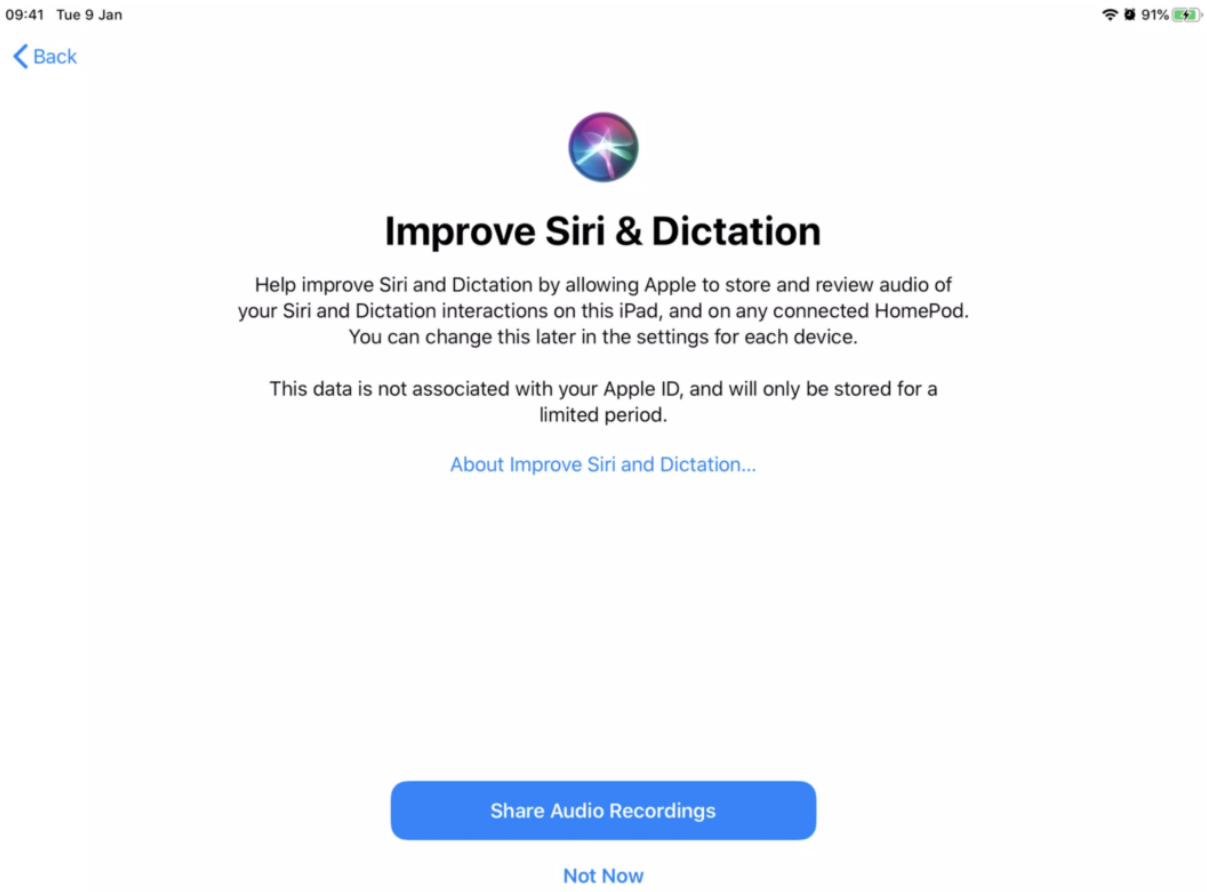
APPENDIX A

Apple Privacy Billboard

Source: Ingraham (2019)

APPENDIX B

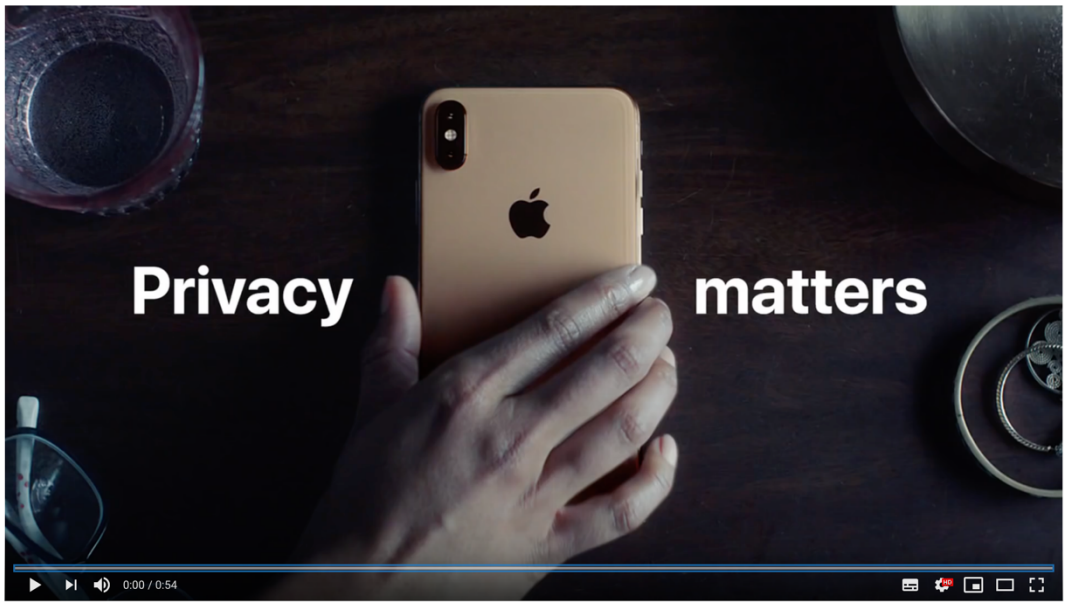
Apple Updated Layout Offering the Sharing of Audio Recordings



Source: Hern (2019)

APPENDIX C

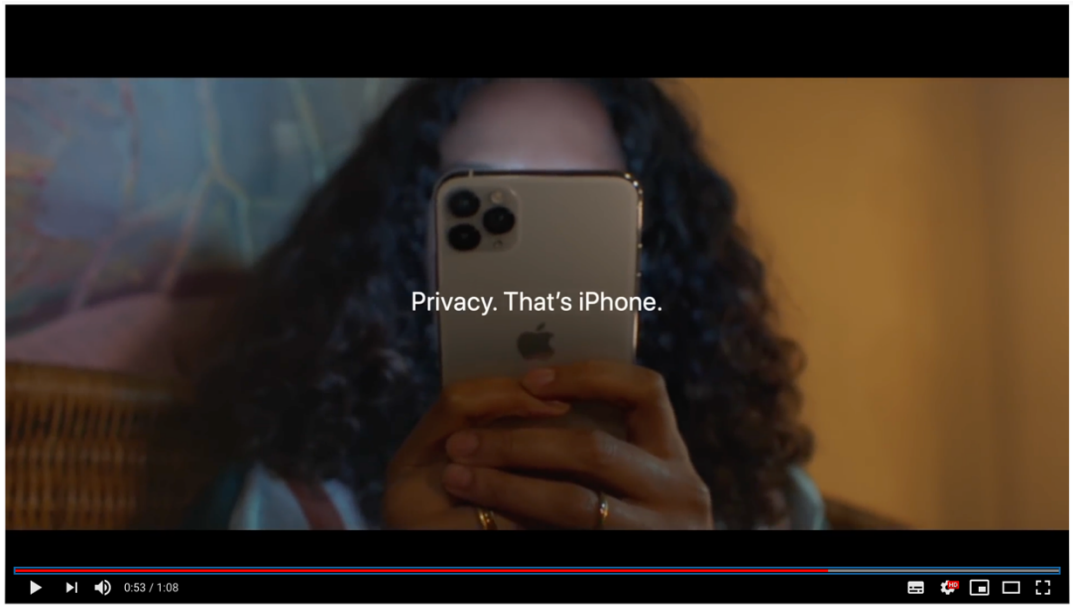
Apple Privacy Ads



Privacy on iPhone — Private Side

29.300.271 visualizações • 14 de mar. de 2019 89 MIL 24 MIL COMPARTILHAR SALVAR

Source: https://www.youtube.com/watch?v=A_6uV9A12ok



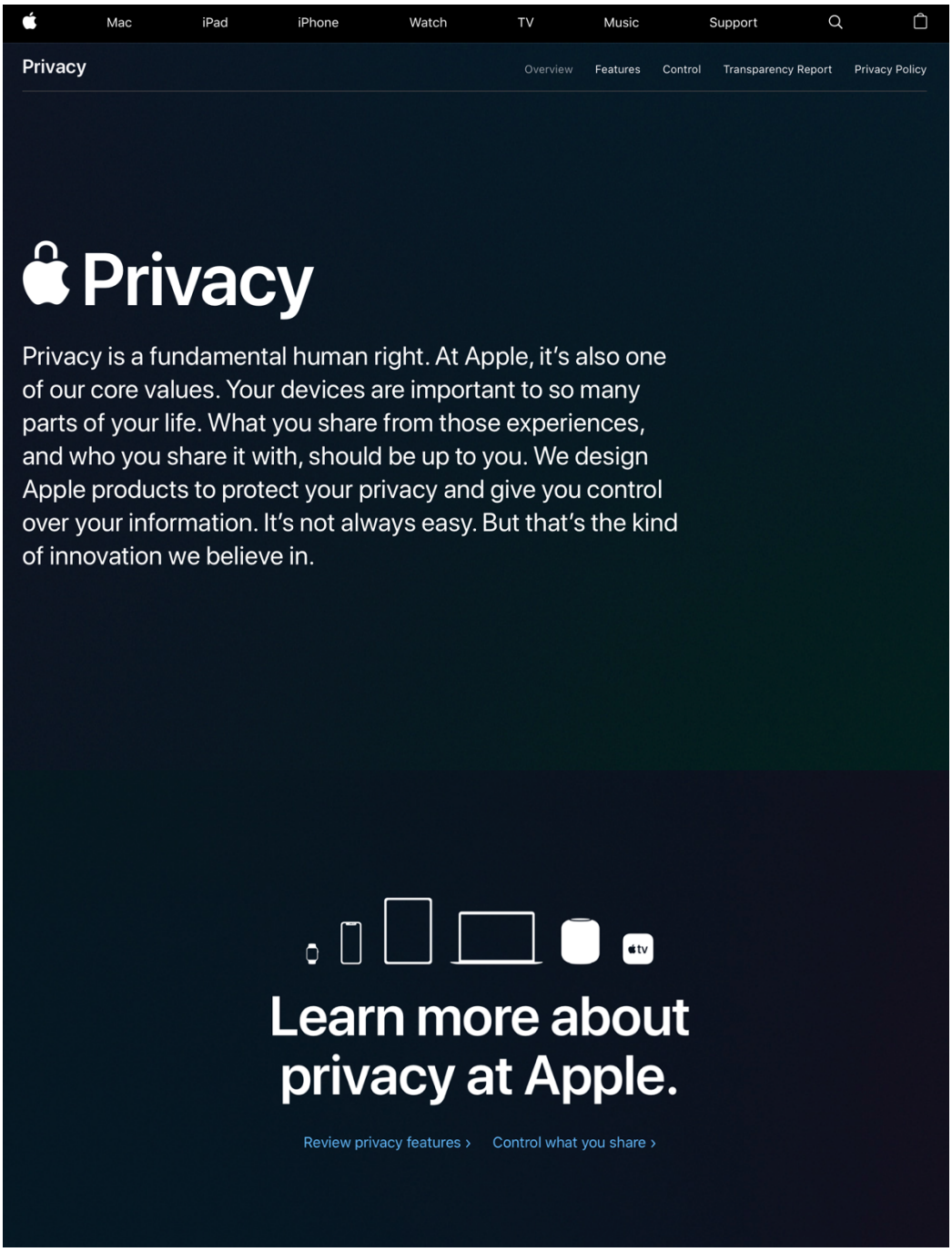
Privacy on iPhone — Simple as that — Apple

24.392.075 visualizações • 25 de out. de 2019 50 MIL 14 MIL COMPARTILHAR SALVAR

Source: https://www.youtube.com/watch?v=Py0acqg1oKc

APPENDIX D

Apple Privacy Page



Source: https://www.apple.com/privacy/

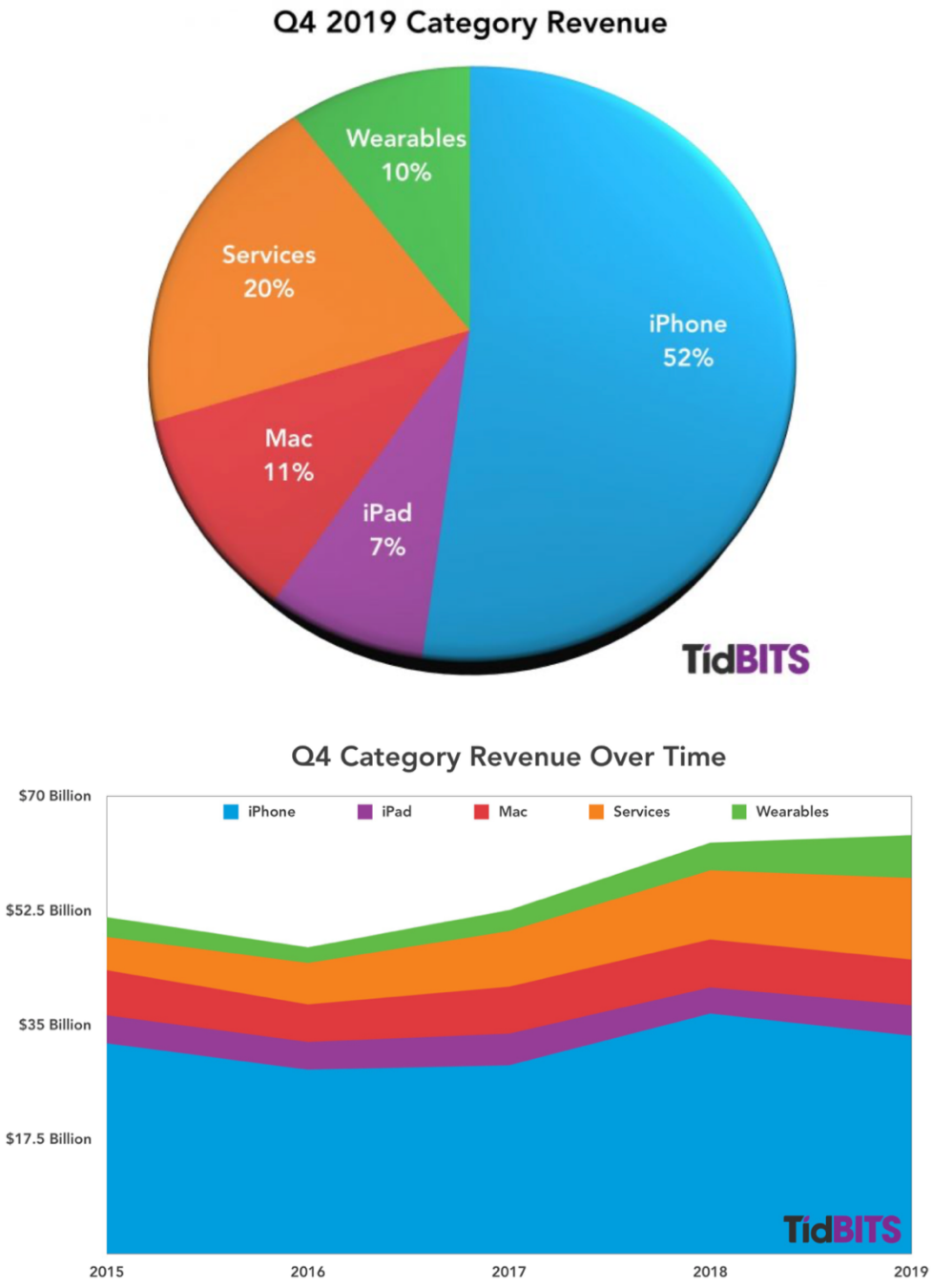
APPENDIX E

Apple 30th Mac Anniversary Page

Source: https://www.dailymail.co.uk/sciencetech/article-2545442/Happy-birthday-Mac-Apple-celebrates-30-years-groundbreaking-computer.html

APPENDIX F

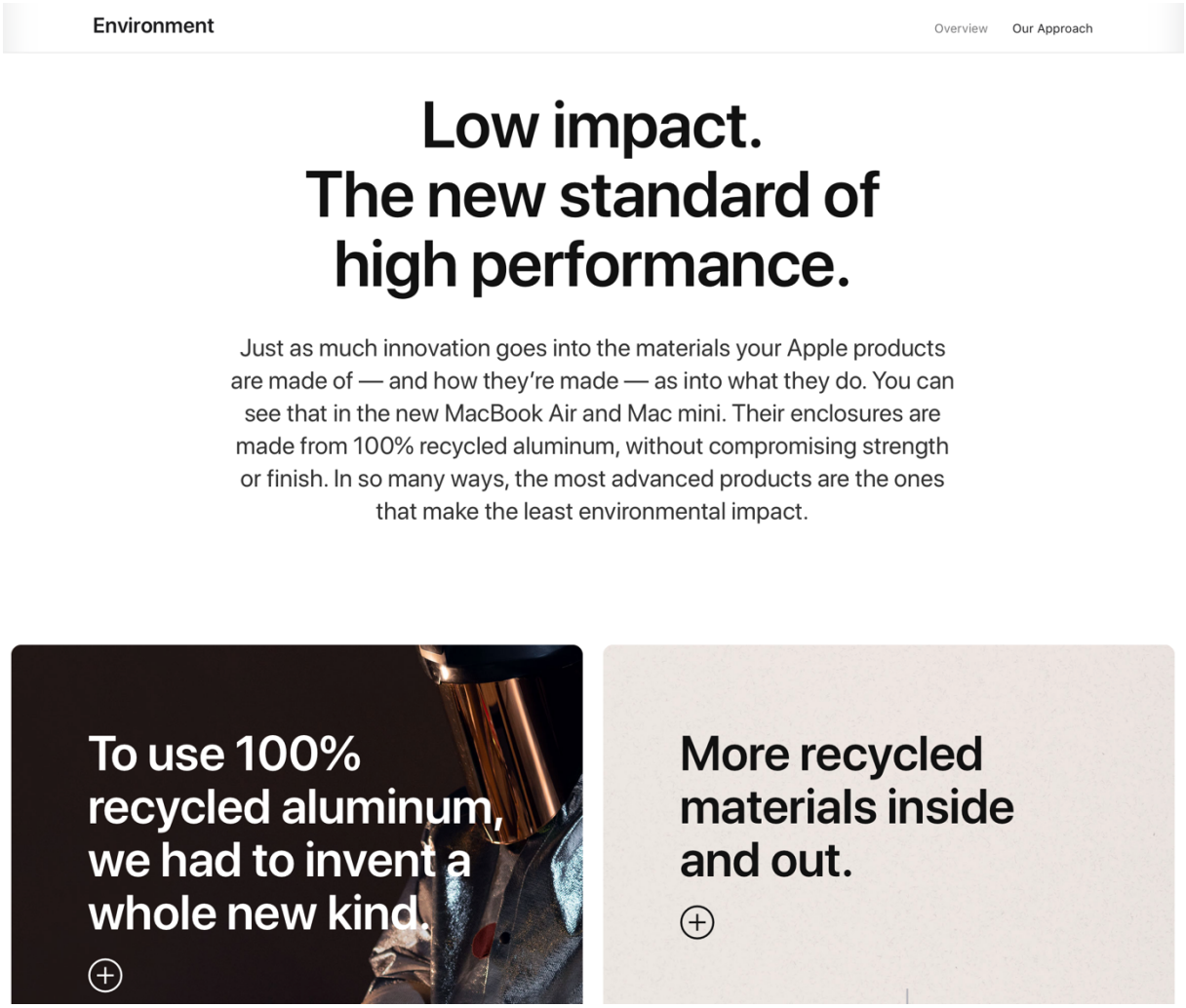
Apple Revenue Composition



Source: https://tidbits.com/2019/10/30/apple-q4-2019-breaks-records-despite-slipping-iphone-sales/

APPENDIX G

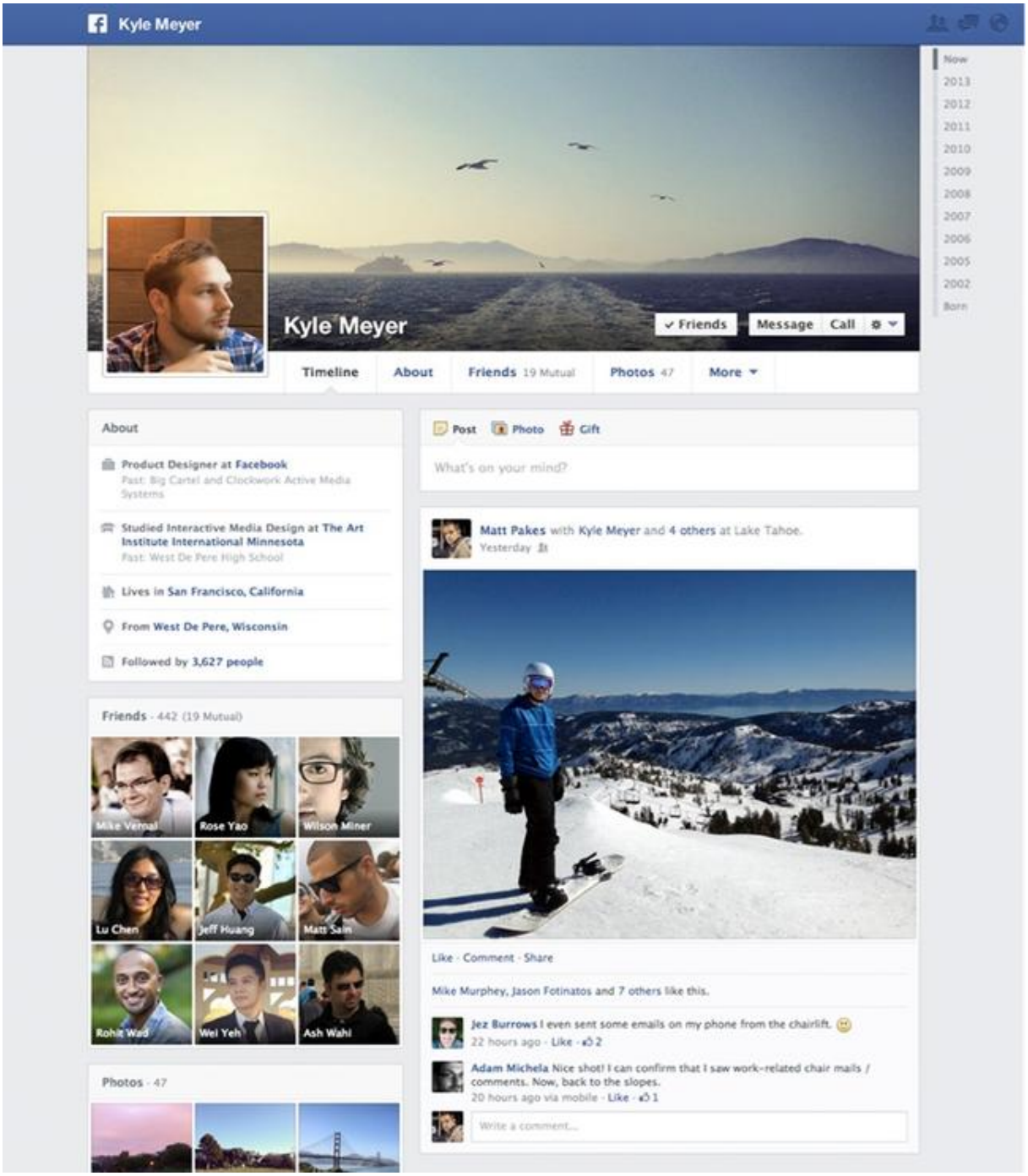
Apple Environment Page



Source: https://www.apple.com/environment/

APPENDIX H

Facebook Page Layout Evolution



Source: https://www.pcmag.com/feature/320360/10-years-later-facebook-s-design-evolution/11

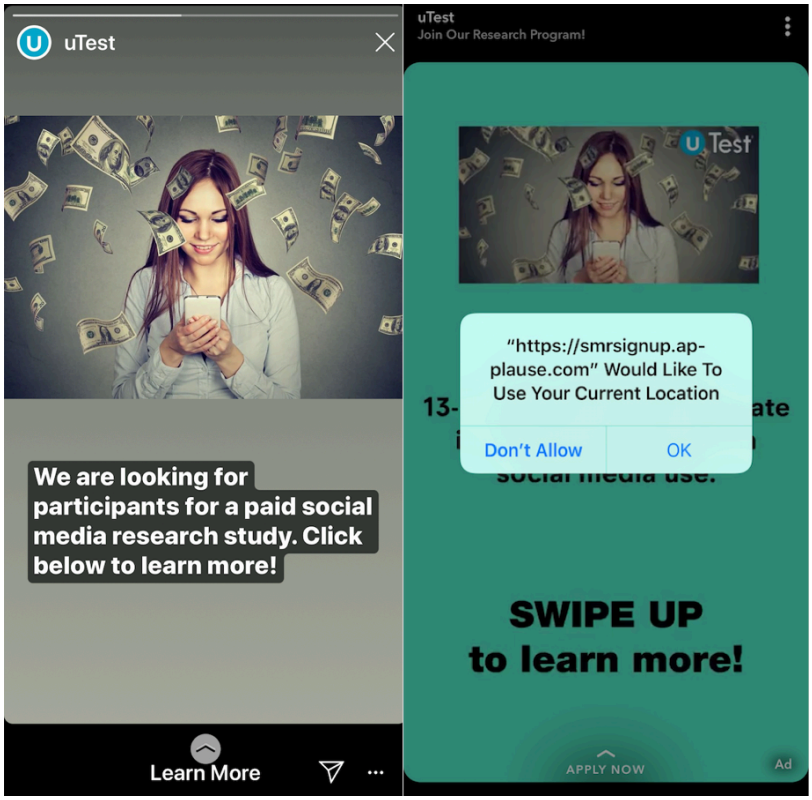
APPENDIX I

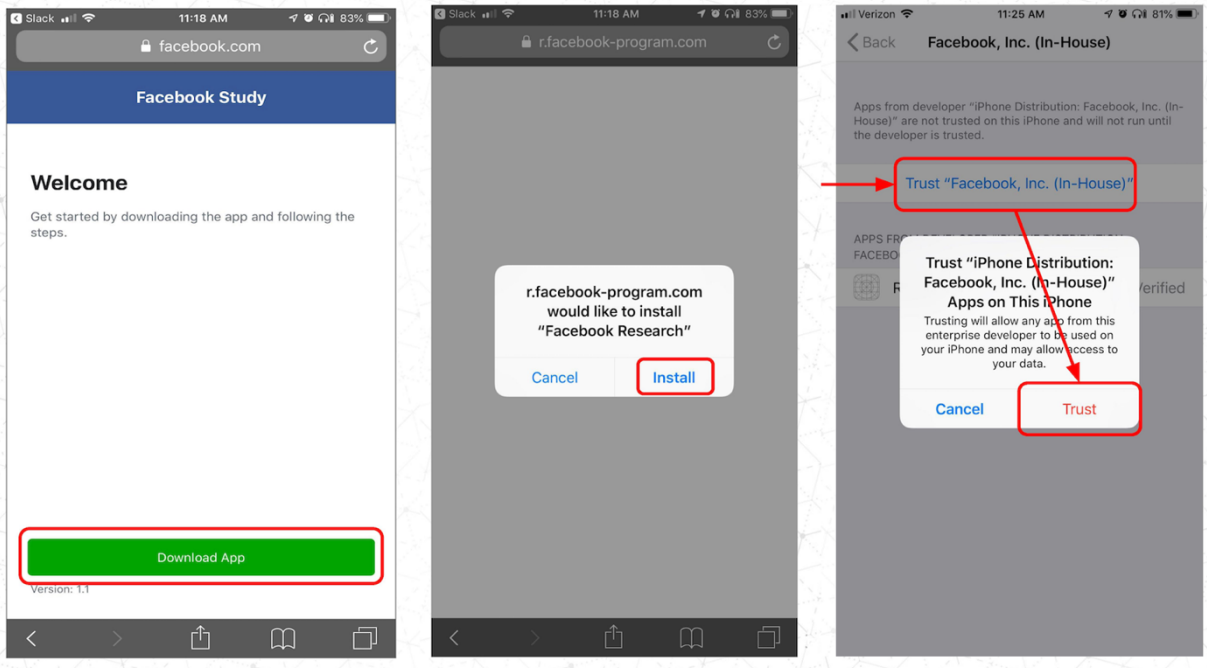
Facebook Market Value After Cambridge Analytica

Source: https://www.theverge.com/2018/3/19/17139642/facebook-stock-fall-market-cap-data-breach-cambridge-analytica

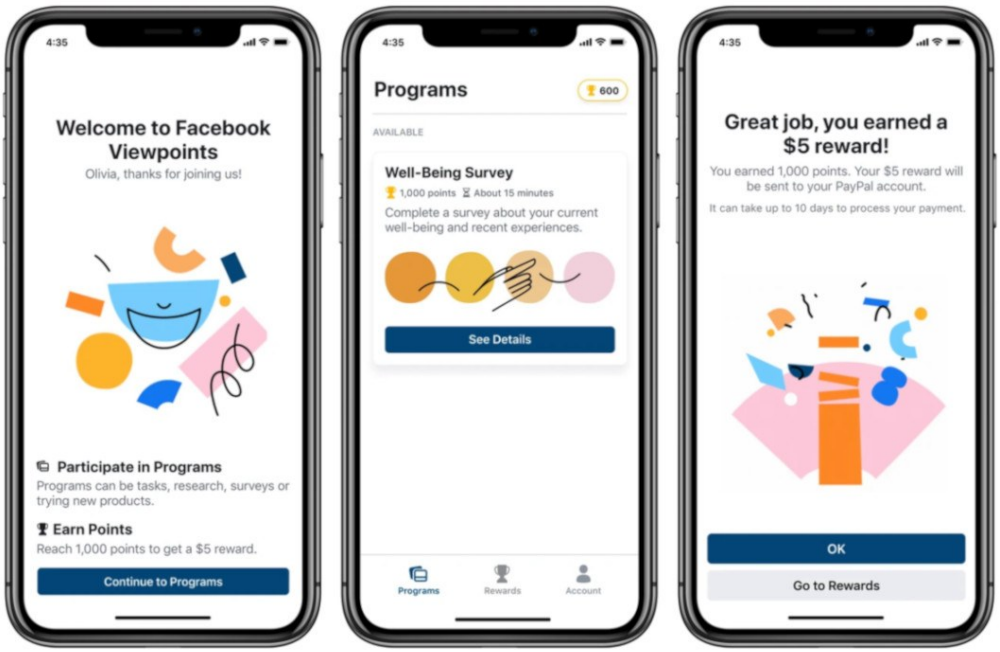
APPENDIX J

Facebook Project Atlas In Action





Source: Constine (2019)



Source: Constine (2019)

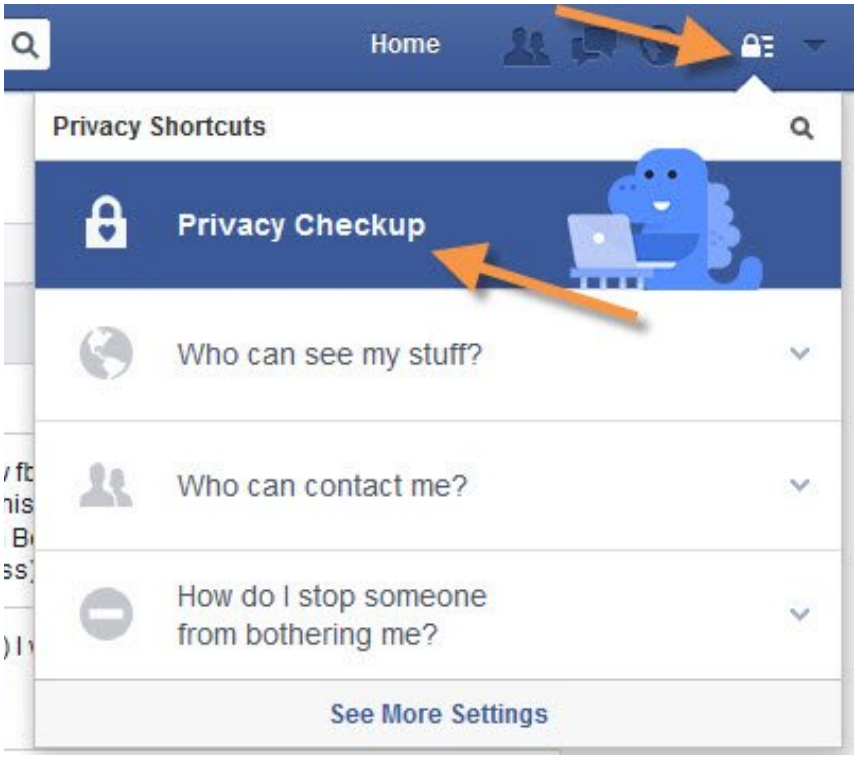
APPENDIX K

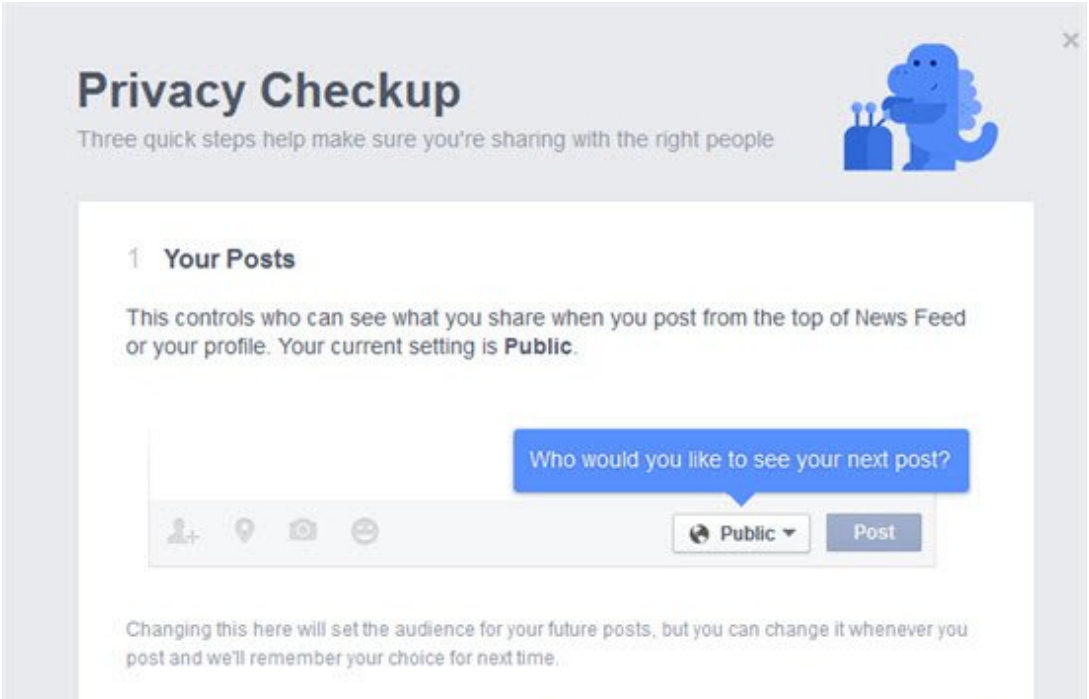
#deleteFacebook Social Posts

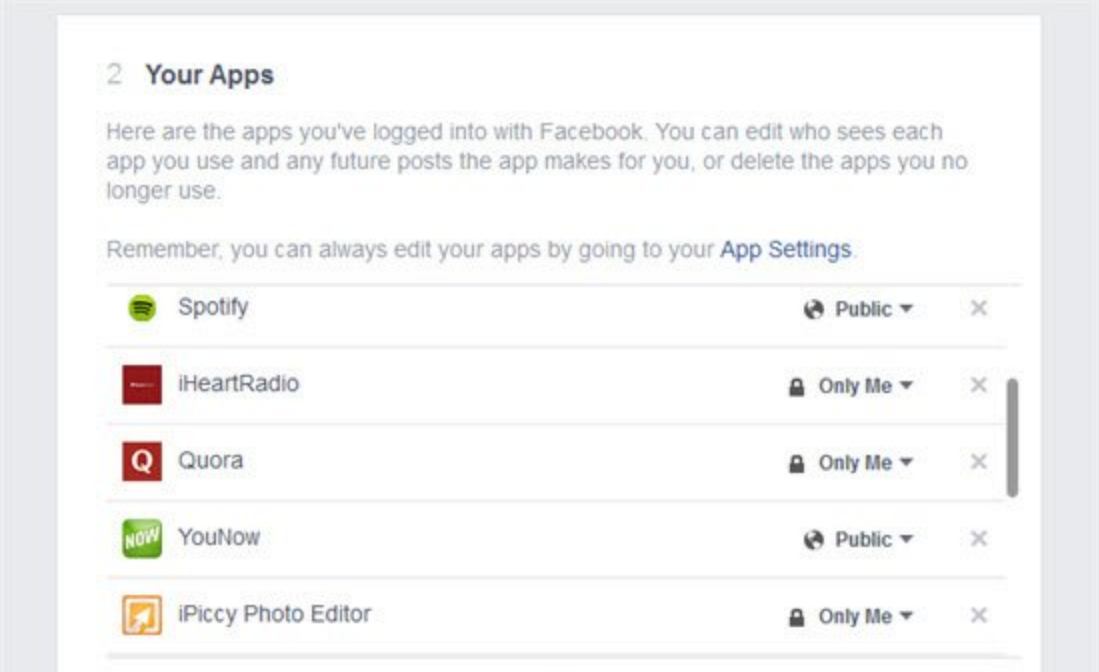
Source: Schiffer (2019)

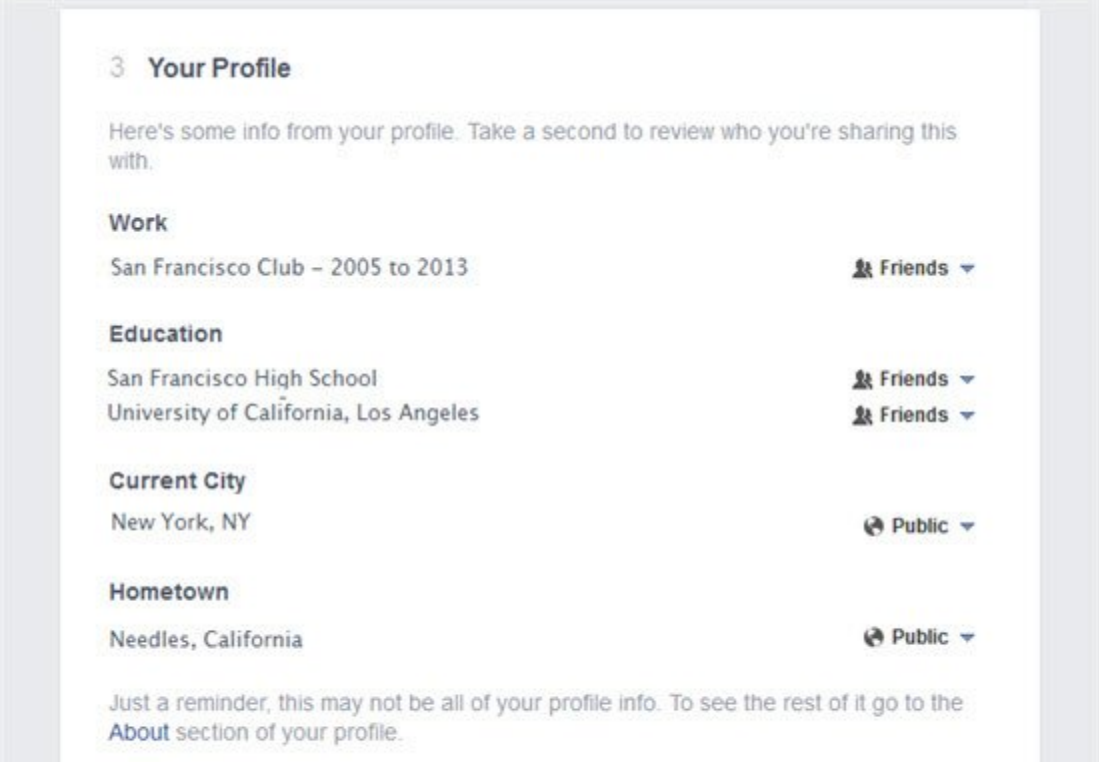
APPENDIX L

Facebook New Privacy Checkup Tool





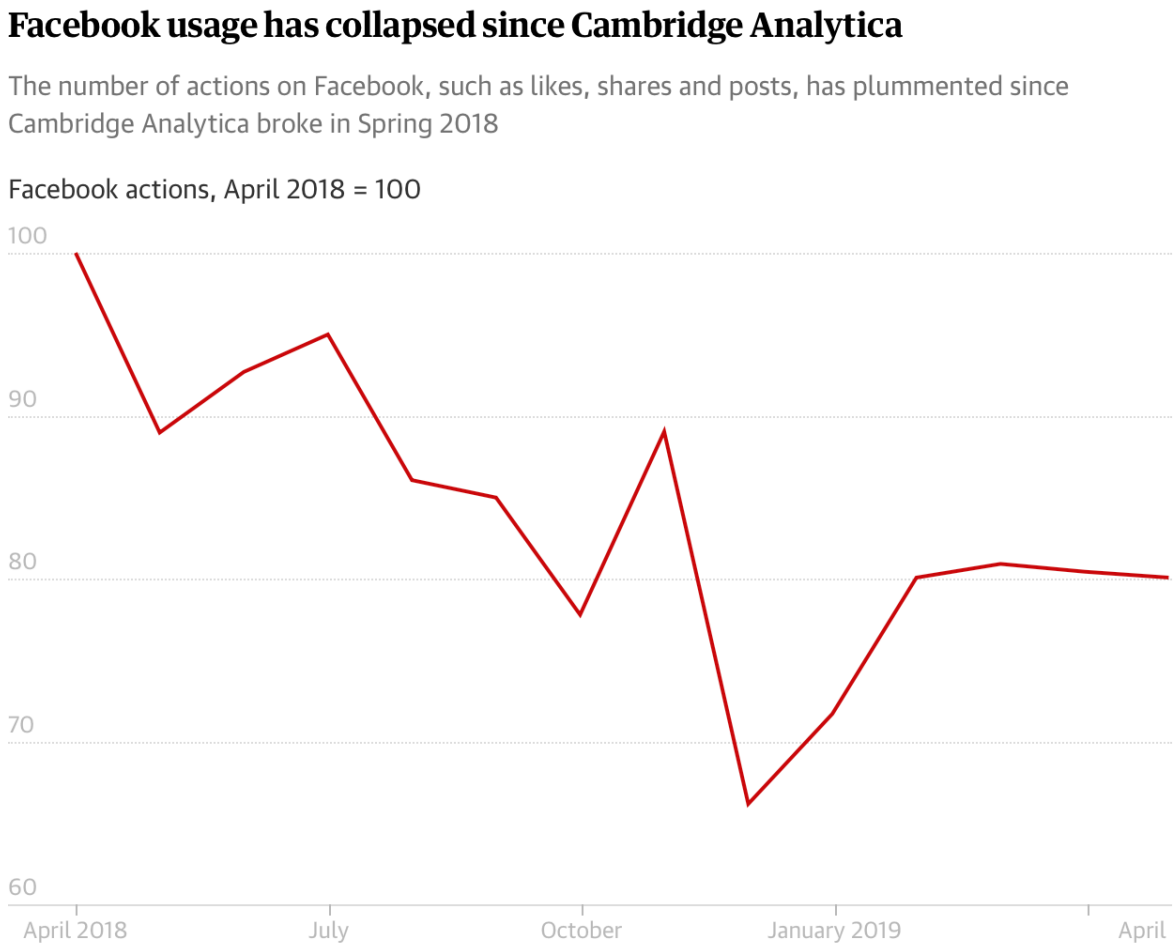




Source: https://www.trishtech.com/2014/09/facebook-privacy-checkup-three-step-facebook-privacy-tuneup/

APPENDIX M

Facebook Usage After Cambridge Analytica



Source: https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows

APPENDIX N

Facebook Financial Highlights Q1 2019

First Quarter 2019 Financial Highlights

In millions, except percentages and per share amounts	Three Months Ended March 31,		Year-over-Year % Change
	2019	2018	
Revenue:			
Advertising	$ 14,912	$ 11,795	26 %
Payments and other fees	165	171	(4) %
Total revenue	15,077	11,966	26 %
Total costs and expenses*	11,760	6,517	80 %
Income from operations*	$ 3,317	$ 5,449	(39) %
Operating margin*	22 %	46 %	
Provision for income taxes	$ 1,053		
Effective tax rate*	30 %		
Net income*	$ 2,429	$ 4,988	(51) %
Diluted earnings per share (EPS)*	$ 0.85	$ 1.69	(50) %

*Includes a $3.0 billion legal expense accrued in the first quarter of 2019 related to the ongoing U.S. Federal Trade Commission (FTC) matter as discussed below. As this expense is not expected to be tax-deductible, it had no effect on our provision for income taxes. Excluding this expense, our operating margin would have been 20 percentage points higher, our effective tax rate would have been 14 percentage points lower and our diluted EPS would have been $1.04 higher.

Source: https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-First-Quarter-2019-Results/default.aspx