UNIVERSIDADE
FEDERAL RURAL
DE PERNAMBUCO

Maria Eduarda Rebelo Di Carlli

Power and Privacy in Software Ecosystems — A Study on Data Breach Impact on Tech Giants

Recife

2020

Maria Eduarda Rebelo Di Carlli

Power and Privacy in Software Ecosystems — A Study on Data Breach Impact on Tech Giants

Bachelor Thesis presented to the members of B.Sc in Computer Science from Universidade Federal de Pernambuco as partial requirement to achieve title of B.Sc in Computer Science.

Universidade Federal Rural de Pernambuco – UFRPE

Departament of Computing

B.Sc in Computer Science

Supervisor: Prof. George Augusto Valença Santos, PhD

Recife

2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

D536p Di Carlli, Maria Eduarda Rebelo
Power and Privacy in Software Ecosystems — A Study on Data Breach Impact on Tech Giants / Maria Eduarda Rebelo Di Carlli. - 2020.
60 f. : il.

Orientador: George Augusto Valenca Santos.
Inclui referências e apêndice(s).

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal Rural de Pernambuco, Bacharelado em Ciência da Computação, Recife, 2020.

1. Software ecosystems. 2. Privacy engineering. 3. Power. I. Santos, George Augusto Valenca, orient. II. Título

CDD 004

MINISTÉRIO DA EDUCAÇÃO E DO DESPORTO
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

http://www.bcc.ufrpe.br

Ficha de Aprovação do Trabalho de Conclusão de Curso

Trabalho defendido por Maria Eduarda Rebelo Di Carlli às 15 horas do dia 27 de outubro de 2020, no link https://meet.google.com/bkp-gkbd-gee, como requisito para conclusão do curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco, intitulado **Power and Privacy in Software Ecosystems — A Study on Data Breach Impact on Tech Giants**, orientado por George Augusto Valença Santos e aprovado pela seguinte banca examinadora:

George Augusto Valença Santos
DC/UFRPE

Fernando Antônio Aires Lins
DC/UFRPE

“To free us from the expectations of others, to give us back to ourselves–there lies the great, singular power of self-respect.”

(Joan Didion)

Acknowledgements

To my dear parents Giovanni and Patricia, and brother Pedro, for the undying support and understanding throughout my entire academic journey. Despite being privy to the challenges and occasional struggles, I have always felt encouraged to keep on going. Thank you for everything.

To my supervisor George Valença, Ph.D., for guiding me through every single second of this challenging work and providing assistance whenever requested. Thank you for understanding, for supporting, and reassuring faith in the work I was doing. Here's to many more research projects to come in the future.

To my friend Ariany Ferreira, my partner in crime for years in this so-called life — academic or otherwise. Thank you for being there through the good and the bad, the hardships and celebrations, and everything else in between. To many more years of sharing so many other accomplishments together.

To my friend Tássia Barros, for all these years of looking after one another, countless academic projects and many accomplishments together. Thank you for the support, for the late nights and the mutual assistance to get through this journey. To many more to come.

To my friend Nikoo Saber, Ph.D., for being the voice of reason and the utmost supporter, on top of all the dedicated hours invested in this work. This journey would certainly be a lot bumpier had it not been for the lending of a hand and a listening ear on your end, and having faith in me. Forever grateful.

To my friend Katherine Daniel, for holding me up and keeping me motivated even during trying, suffocating times. You have been with me throughout the entire course of this journey, cheering me on, keeping me grounded and looking out for me. Grateful beyond words.

To all the friends I have made during the course of my undergrad, thank you for sharing so many great moments and joining forces to get through the last five years.

To all the professors and staff members of Department of Computing at Universidade Federal Rural de Pernambuco, for the ongoing support provided to students throughout the years. It certainly gives the students the courage and strength to keep on going.

To everyone who, directly or indirectly, contributed to this work and my academic journey: you have my heartfelt gratitude.

Abstract

Concerns about data privacy and protection in companies from various fields and sizes are not only a reality, but a requirement at this day and age. The need to comply with governmental laws and other rules became a driving force in handling personal data. For major IT companies, especially those in charge of a software ecosystem, such concerns grow tenfold and extend over to their platforms, software solutions (internal or external products/services - i.e. from third parties) and respective partnerships. When a case of privacy breach is identified, the relationship between the company and users becomes another concerning factor, with consequences abound — financial, technical, business or social aspects. This research investigates privacy and data breach cases in GAFA (Google, Amazon, Facebook, Apple) ecosystems using the perspective of power relationships. By considering the five main forms of power (coercive, expert, legitimate, referent and reward power), we aim to describe how actors in a software ecosystem exercise power in the occurrence of a data protection issue. Moreover, we analyse the impact of the manifested power in the overall health of the ecosystem. The results of our research show that these companies are able to exercise types of power that are enabled by elements such as reputation and technical orchestration, evoking a sense of trust and convenience. Additionally, we discuss the role of media outlets and data protection rules as threats against the exercise of power from these ecosystems.

Keywords: Software Ecosystems, Power, Privacy Engineering

Contents

List of Figures

List of Tables

1 Introduction

The consolidation of software ecosystems in the last decade represents a paradigm shift in the IT industry, in terms of both business models and software development. In this setting, varied companies join forces to co-create value by acting as a unit in a shared market for software and services (MESSERSCHMITT; SZYPERSKI et al., 2005; JANSEN; FINKELSTEIN; BRINKKEMPER, 2009). Through a platformisation approach (PARKER; ALSTYNE; CHOUDARY, 2016), which consists of a company offering its environment as a service, a keystone structures, releases, and controls a central technology to pave the way for open innovation. This company starts to rely on partners to complement (e.g. creating a specific feature or module in a system), extend (e.g. adapting a feature to a specific customer segment), or simply promote a software product (e.g. including it in an app store or suggesting its use during innovation-centred events such as hackathons). This is the case of successful networks created around Apple's iOS, Amazon's Alexa or Google's Android.

Ecosystems require software development to be oriented towards an architecture model that promotes secure software sourcing, integration, deployment, and evolution throughout a supply chain of different producers (SCACCHI; ALSPAUGH, 2018). Otherwise, we may perceive events such as data breaches, which reveal the fragility of a software platform and related solutions. In 2017, a security researcher identified a data protection incident in the iOS ecosystem. The popular third-party solution AccuWeather from Apple's marketplace continued sending private location data to a backend monetisation service called RevealMobile, even with the location sharing turned off by the user[1]. Two years later, the Guardian newspaper reported on Apple passing on Siri recordings to contractors working for the company around the world. Amazon was accused of a similar practice: it analysed snippets of conversations from Alexa-powered devices, which are secretly recorded and uploaded to the cloud without the user's consent[2]. In the Facebook ecosystem, a loose app review process combined with configuration errors allowed Instagram advertising partners to misappropriate a vast set of sensitive user data, including physical location, personal bios, and photos[3].

The previous examples highlight the need to ensure the privacy of user data, which is essential for software solutions to properly operate in the ecosystem. Furthermore, the success or failure of these solutions may affect the platform owner, innumerous complementors and, more

[1] "AccuWeather caught sending user location data, even when location sharing is off" - <https://www.zdnet.com/article/accuweather-caught-sending-geo-location-ata-evenwhen-denied-access/>

[2] "Confirmed: Apple Caught In Siri Privacy Scandal, Let Contractors Listen To Private Voice Recordings" - <https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-aple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recodings/>

[3] "Instagram's lax privacy practices let a trusted partner track millions of users' physical locations, secretly save their stories, and flout its rules - <https://www.businessinsider.com/startup-hyp3r-saving-instagram-users-stories-tracking-locations-2019-8>

importantly, the pool of users. Such impact is not perceived in isolation but rather in a systemic form, as the evolution of the ecosystems depends on the coopetition[4] of these players (MOORE, 1993). Their active collaboration resembles biological interactions among species in natural environments,given the business—technical as well as social—assets that are shared among partners, e.g. the expertise of a developer community; the image of a respectable reseller; the resources that a big company provides to the network (e.g. profits, technological support); or the role assignment strategy, together with rights and penalties, defined by a keystone (VALENçA; ALVES, 2017). These assets are sources of power, since they enable one party to increase another party's dependence by controlling what it values in the ecosystem (EMERSON, 1962). As a network of interdependent parties is established, power distribution becomes a useful lens of analysis in this scenario of multiple interfirm relationships.

This research is motivated by the question of how data protection issues potentially affect power relationships within a software ecosystem, as well as the dynamic among its elements. The study adopts the concept of power relationships (VALENÇA; ALVES, 2017) as a tool to analyse the aforementioned issues. The perspective of power exercise is utilise to conduct a reinterpretation of privacy breach scenarios for better comprehension of how relationships among entities are affected once the scandal occurs. To investigate this phenomenon, a descriptive case study of GAFA (Google, Amazon, Facebook, Apple) ecosystems is performed, considering their power in the software industry in addition to their ubiquity in our daily routine. Evidence of recent privacy breaches, representing four critical privacy cases from the perspective of power types and sources are collected and examined, followed by the analysis of power-changing operations (VALENçA; ALVES, 2017) and the impact of these privacy breaches on the health of the studied ecosystems.

[4] *Coopetition*: cooperation + competition

2 Literature Review

2.1 Software Ecosystems

Software ecosystems can be described as a set of businesses functioning collectively as a unit and interacting with a shared market for software and services, forging relationships among themselves, as well as with companies investing in innovative business models to co-create value for the ecosystem to promote knowledge sharing among the community of participants. In a platform business model, companies open their platforms for third parties/potential partners to integrate their specific solutions and/or develop new ones (VALENCA et al., 2019).

In order to comprehend how software ecosystems operate, an understanding through three different dimensions is considered: **social**, **technical** and **business** (VALENçA; ALVES, 2017). The **social** dimension encompasses the actors participating in the ecosystem with their respective roles, relationships, skills and motivations, among other factors that regulate the interactions within the network. The **technical** dimension is primarily concerned with the software platform itself and its software-based system that provides core features shared by a portfolio of products or services that interoperate with each other, with extended solutions via boundary resources, such as application programming interfaces (APIs) and software development *toolkits* (SDKs) (NAMBISAN; SIEGEL; KENNEY, 2018). Within this dimension, product management and development processes that shape how solutions are collaboratively planned, evolved and released to customers can also be found. Lastly, the **business** dimension deals with the strategies to obtain value and generate revenue for all ecosystem participants by involving the platform business model and its definitions about entry barriers and intellectual property rights, as well as overall innovation directions (VALENCA et al., 2019).

By delving into its elements, a partitioning of the ecosystem is executed into **two** main groups of **actors**: those imposing all controlling actions and those submitted to the established rules. A company called **keystone** (MANIKAS; HANSEN, 2013) governs the ecosystem's evolution by defining rules of access to the platform and orchestrating the creation of new solutions (e.g. apps). At the same time, a group of **complementors** are able to co-create value on top of such platform by concatenating solutions from all parties to supply market needs when it comes to additional services or features.

Forging partnerships occurs whenever firms join efforts to achieve goals that could not necessarily be attain so easily by each company individually, often orchestrated as an intentional strategic relationship between companies that share compatible goals, strive for common benefits, and maintain a high level of mutual interdependence (VALENçA; ALVES, 2017). Such partnerships between software companies have been consistently established throughout recent

years in order to increase the diversity of technologies, co-create innovations, and enter new markets. The aim for these companies has been to eliminate any traditional software development paradigm archetype known for consisting of a single company responsible for designing, implementing and selling the product. Software companies have welcomed external developers to their interfaces, aiming to integrate solutions that are specifically curated and developed as new applications within their platforms. A mutual agreement between these firms grants interactions with external actors, resulting in complementing functionalities for existing products, in addition to offering a variety of technical services such as systems integration and maintenance (VALENçA; ALVES, 2017); this phenomenon is what characterises a **software ecosystem**. Lastly, the keystone firm is thoroughly responsible for governing the activities of all actors within an ecosystem, orchestrating players and coordinating their development efforts accordingly. In order to succeed in a software ecosystem, companies must identify core power capabilities to achieve their goals (e.g. a company that develops innovative apps can either strengthen its position or alter its role in the ecosystem, eventually elevating its status among partners if they recognize this ability) (Alves; Valença; Franch, 2019).

Regarding the aspect of governance, each individual software ecosystem relies on a set of specifically designed procedures responsible for controlling, maintaining or even modifying elements within the ecosystem, also encompassing all businesses and technical aspects such as the integration technology, sustainable business models and developer partnerships. In relation to the effectiveness in governance strategy, it is important to provide competitive success of partners and leverage the overall **health** of the ecosystem itself by taking the adoption of a life cycle that nurtures its well-being from birth to expansion (and whatever comes later on) in consideration. Additionally, by analysing the birth phase as critical, it is possible to highlight the process of transforming opportunities into fruitful and legitimate organizational form, taking a group of complementors co-creating value by combining their solutions to address market needs for additional features or services. The firms gradually share their customers and gain access to new segments (VALENçA; ALVES, 2017). Software ecosystems can, too, be considered a particular type of business ecosystem with a technological platform serving as intermediate variable between the interaction of players involved in it.

The software platform and customer base grow as the ecosystem naturally expands, describing a particular phase which involves internal and external battles for conquering customers, aiming to reach new segments and increasing market share. Competitions among key rival ecosystems also take place throughout the expansion. The subsequent phase, called *leadership*, is also known as *maturity* and involves internal disputes among players to inherit more power within the network once the ecosystem proves to be large and profitable (VALENçA; ALVES, 2017) The structure of central processes to the ecosystem (e.g. governance and development processes) becomes more stable, favouring the contribution of participants. Central firms reinforce their roles by making innovative contributions and further extending their pool of customers, serving as a means to gain power over partners and shape future directions of the

ecosystem. This type of innovation flow is crucial to starting a new evolutionary cycle throughout the self-renewal stage. It will increase the capacity of the ecosystem to adapt to changes and external interference, preventing its premature death. Mergers and acquisitions among ecosystem participants or even among ecosystems can happen at this stage (VALENçA; ALVES, 2017).

Finally, the overall health of a software ecosystem is intrinsically linked to the actions and decisions taken by each participant. This can be assessed it via three key measures. *Productivity* is the ability of the ecosystem to transform inputs into products and services, which may occur by increasing the number of applications in an app store. *Robustness* means the capacity of the ecosystem to deal with interference and pressure from competitors. It comprises the number of participants in the ecosystem, as well as their active contribution and survival rate. Lastly, *niche creation* involves the business opportunities that the ecosystem can provide to its participants. It relies on increasing the number of players that use the platform, producing valuable resources and creating new market niches. Therefore, by assessing these aspects, it enables the establishment of potentially useful strategies that should enable all ecosystem participants to evolve collectively (VALENCA et al., 2019).

2.2 Privacy Engineering

Privacy research in computer science has produced a rich array of privacy solutions, however, the actual implementation of these findings into practical engineering has been significantly hindered. Recently, countless reports of privacy violations and technology companies' failure to comply with basic data protection requirements have become commonplace, suggesting that we are far from applying privacy design know-how in practice (Gürses; del Alamo, 2016). Nevertheless, when it comes to privacy, a data breach is only one concern among many. Subtle engineering decisions that ignore users' privacy needs may have far-reaching consequences. Recent highlights include *Snapchat* violating user expectations and privacy by not deleting users' messages, *Firefox* extension NoScript's defaults leading to deanonymization attacks on Tor users, and Facebook apps allowing the sharing of users' friend networks with advertisers (Gürses; del Alamo, 2016).

A direct consequence of poor privacy design decisions — or lack thereof — is the inevitable impact on global infrastructures, such as cloud services and mobile networks. Past reports of Apple, Google and Microsoft indicate malicious collection of location information gathered by their respective mobile devices from Wi-Fi hotspots—even when users turn off location tracking (Gürses; del Alamo, 2016).

The concept of privacy engineering addresses an overall lack of generalization in existing approaches; shortage in efforts to integrate different subdisciplines' techniques and tools; the need to evaluate proposed approaches in different social, organizational, technical, and legal contexts; and concrete challenges emerging from the evolution of engineering practices, techni-

cal architectures, legal frameworks and social expectations (Gürses; del Alamo, 2016).

Throughout several decades, privacy-friendly systems have been a considered a research challenge for computer scientists. Most efforts have followed three prominent approaches. The first is identified as **privacy by architecture**, an approach that aims to minimize the collection or inference of sensitive information by unintended parties, typically service providers (Gürses; del Alamo, 2016). Researchers develop technologies that enhance privacy by applying techniques that establish constraints on data collection and processing, as well as ensures that no entity can single-handedly undo these constraints.

A second approach is referred to as **privacy by policy**, one that aims at *"protecting consumer data from accidental disclosure or misuses and facilitating informed choice options"* (Gürses; del Alamo, 2016), which translates to reinforcing measures to ensure compliance with principles of data protection laws regarding information systems. These requirements may include *"specifying and notifying users of the purpose of collection; limiting collection and use to this purpose; being transparent about additional recipients of the data; and providing users access to their data for verification, correction, and deletion"* (Gürses; del Alamo, 2016). Proposed technologies include policy specification languages, policy negotiation and enforcement mechanisms, and design techniques to improve the readability of privacy policies.

A third approach is called **privacy by interaction**, which focuses on socio-technical designs[1] that would improve users' agency with respect to privacy in social settings; the approach captures privacy matters that arise between peers or in a workplace due to the introduction of information systems (Gürses; del Alamo, 2016). These privacy concerns are related to, but often differ from, concerns regarding organizations collecting and processing data, which privacy by policy approaches address, and unintended inferences, which privacy by architecture tackles. The social computing perspective, in which information systems facilitate social interactions, informs the methods and techniques the approach uses (Gürses; del Alamo, 2016).

Lastly, the fourth approach is known as **privacy by design**, one that is rooted in providing organizations with a means to successfully achieve both privacy and functionality requirements from the very beginning stage of software development's life-cycle (Cavoukian; Kursawe, 2012). Privacy by design (PbD) can be described through seven core principles that serve a framework to coordinate along with other controls for particular domains and use case scenarios. These principles suggest that the design process of systems require *"minimal data collection processes and proper notice and consent interactions"* (HADAR et al., 2018). PbD has taken centre stage in the recent years in light of data protection regulations demand that software engineers inherit PbD principles throughout the development and apply data protection solutions throughout their projects, as well as the technological developments to provide these solutions (Martin; Kung,

[1] *Describes the application of social and ethical requirements to human-computer interaction, software and hardware systems.*

2018). It illustrates the core of regulations such as the General Data Protection Regulation[2] (GDPR) in the European Union.

Low privacy standards can provoke media backlash and lead to costly legal trials around privacy breaches, and distrust caused by these breaches is possibly the one real blemish on the image of technology companies such as Google or Facebook (SPIEKERMANN, 2012). A company's branding stands as one of its most valuable asset, as well as the most difficult to build and likely the most costly to maintain. Hence, brand managers should be keen to avoid privacy risks.

Despite improvements and developments regarding privacy matters in the corporate field, a core challenge for designing privacy requirements is to get organizations' management involved in the privacy strategy. Management's active involvement in the corporate privacy strategy is fundamental, as personal data is the asset at the heart of many companies' business models nowadays (SPIEKERMANN, 2012). High privacy standards often cause further restriction of data collection for multipurpose analysis and limit strategic options.

Managing personal data means optimizing its strategic use, quality, and long-term availability. Unfortunately, quite a few managers still fail to grasp the need for sustainable strategy for one of their company's core assets—personal data—requires in order to actively manage this asset. An even smaller number of today's managers are actually interested in taking on this new challenge (SPIEKERMANN, 2012). Instead, they derive what they can from segments of information at their disposal and leave the privacy issue as a nuisance that is better left to be fixed by lawyers. However, even if managers took up the privacy challenge and incorporated the active governance of personal data into their companies' strategic asset management, they would not be able to determine the right strategy without their IT departments: designing privacy standards requires the expertise of those . As the term implies, the design of systems needs to be altered or focused to technically embrace the protection of peoples' data. Consequently, privacy must be on engineers' requirements radar from the start of a new IT project. (SPIEKERMANN, 2012)

2.3 Power

The notion of Power in interpersonal relationships has been the subject of extensive study by social scientists for decades. Recently, power has also be subject of study in managerial research, more specifically on firms' alliances and strategies (VALENçA; ALVES; JANSEN, 2018). The power of an entity A can be described as the ability that A has to exert some level of influence in its relationship with an entity B. This power generally stems from B's dependence on A, meaning that A has fertile ground to exercise power over B if the player somehow depends on A (Alves; Valença; Franch, 2019). A well-known taxonomy proposed by French and Raven (FRENCH; RAVEN, 1959) illustrates the five types of **power** that a company can hold in a

[2]General Data Protection Regulation (GDPR) - Official Legal Text - <https://gdpr-info.eu>

given relationship, a theory widely adopted across several disciplines due to its loose conceptual framework. The understanding of power as a set of forms is suitable to analyse this construct in several domains (VALENçA; ALVES; JANSEN, 2018). These works aim to classify power in a precise manner. The proposed power taxonomy comprises five power types, which we describe in light of a relationship between two given companies X and Y (Alves; Valença; Franch, 2019):

- **Coercive** power is Y's perception that X has the ability to punish it (e.g. a company disqualifies partners whose products do not live up to quality standards).
- **Reward** power is Y's perception that X has the ability to offer rewards (e.g. a company provides financial benefits to partners in the ecosystem).
- **Expert** power is Y's perception that X has special knowledge or expertise (e.g. a company has strategic market knowledge or masters innovative technologies).
- **Legitimate** power is Y's perception that X has the right to impose behavior for it (e.g. a company can set ecosystem goals due to its superior position).
- **Referent** power is Y's feeling of respect or admiration toward X (e.g. players value a company because they recognize its status, which creates a feeling of identification and attracts them).

Power capability (PC) is defined as a given asset that denotes a company's power, such as developing functionalities for a specific market segment, providing partners with key information about customers, or defining the roles of partners in a joint initiative for system integration (VALENçA; ALVES, 2017). Each one of these capabilities derives from power sources, with tangible or intangible resources that an actor can use to affect the behavior of others. Therefore, by cultivating such sources, a company is able to exercise some level of power. In particular, any change in the availability or demand for power sources may influence the power distribution in a partnership, considering it impacts on an actor's ability to obtain or lose power.

Considering the seminal and highly influential work proposed French and Raven (FRENCH; RAVEN, 1959) in the literature of power, combined with the work of Valença et. al (VALENçA; ALVES, 2017) and Alves et. al (Alves; Valença; Franch, 2019), the results secure the motivation for this study by comprehending the nature of these power bases. This in turn allows the identification of different effects that an actor could potentially generate in another actor once a relationship has been forged and maintained.

Wrong (WRONG, 1980) describes each power form as having a built-in tendency to metamorphose over time into a different form, meaning that transitions may occur among power forms. One can perceive this evolution when the power relationships recur frequently. Williams and Moore (ZACHARY; ROBERT, 2007) are also aligned with this view as it argues about one power form having an ability to generate other forms of power, acting as a precursor. They

also cite works from supply chain research (e.g. (GASKI, 1986)) that examine the effects that *reward* power or *coercive* power may have on expert power, *referent* power and *legitimate* power. Within business relationships, possible power sources are **strong reputation**, **large customer base** or **intellectual property**. It is important to highlight that one shall only consider the two sides of the relationship to identify the power types and respective sources utilised. Although companies operate in a software ecosystem, each specific partnership between two parties must be explored in order to identify such elements (VALENçA; ALVES, 2017).

In a power relationship, actors may have different levels of dependence, illustrating different levels of power. Since the exercise of power is circumstantial and relative, these levels may vary between parties. Emerson (EMERSON, 1962) introduced **four operations** to promote structural changes in power relationships by altering the power advantage between two actors. These power-changing operations revolve around the idea of dependence, e.g. increase the degree of dependence of the partner on the company, or decrease the degree of dependence of the company on the partner. Such operations enable a company to deal with the power of a partner by exploring its power capabilities. As illustrated by Valença et. al (VALENçA; ALVES; JANSEN, 2018), the power-changing operations occur in different levels with different impacts for each of the actors involved, as presented in Fig. 1.

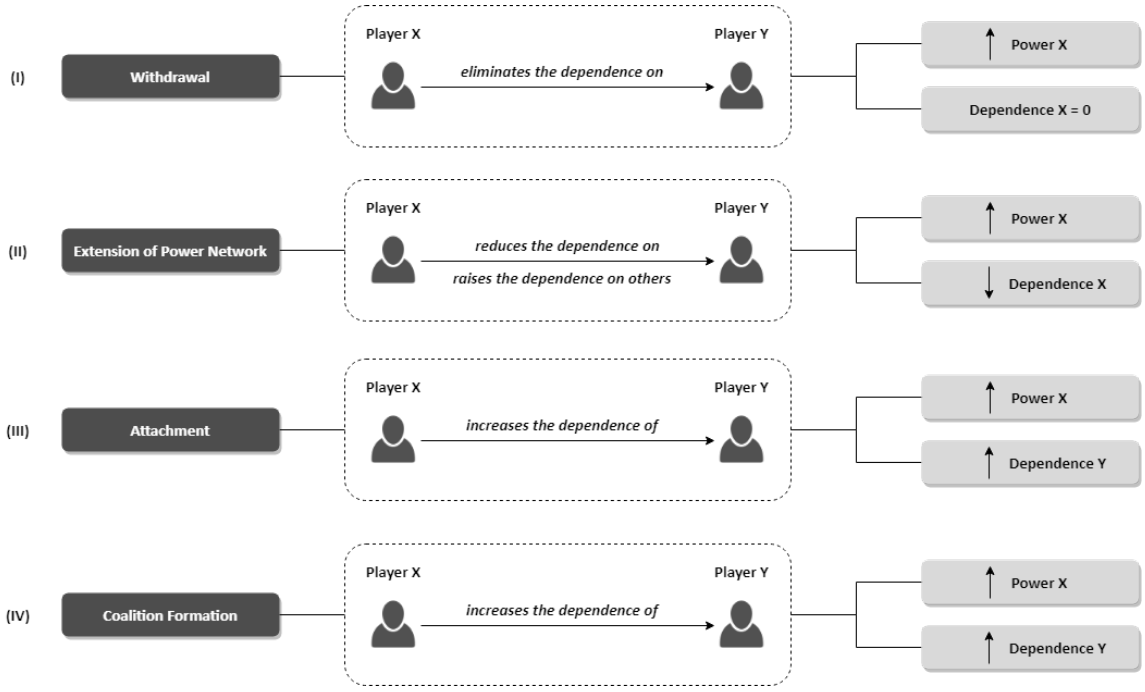

Figure 1 – *Effects of power-changing operations between two software ecosystem elements* (VALENçA; ALVES, 2017).

- *Withdrawal* occurs when X reduces motivational investment in goals mediated by Y. Hence, X gains power by absorbing the dependence on Y. For instance, X neglects the complementation from Y by internally building the product feature previously supplied by Y.

- *Extension of power network* occurs when X cultivates alternative sources for gratification of the goals mediated by Y. Hence, X gains power by reducing its total dependence on Y and relying on other players. For instance, X obtains the technical complementation previously offered by Y from one or more partners, which provides X with relationships that are more flexible.

- *Attachment* occurs when X mediates goals that increase the motivational investment of Y in the relationship. Hence, X gains power by increasing the dependence that Y has on their relationship, given new benefits provided by X. For instance, X provides Y with new commercial benefits such as new customers or a wider profit margin in a joint project.

- *Coalition formation* occurs when X establishes coalitions that prevent Y from accessing alternative sources of resources to achieve its goals. Hence, X gains power by making Y more dependent on their relationship, given a reduction in the options for alternative partnerships. For instance, X forms coalitions with other companies (including competitors) to deny Y to define substitute partners, who could offer similar commercial benefits to Y.

In order to describe the application of power-changing operations in action, consider the same partner companies *X* and *Y*. In their relationship, *X* uses the large dependence of *Y* on its pool of customers to control the relationship. For instance, *X* can specify the roles and duties of suppliers in a joint project, select the strategic requirements that it will implement or establish the percentage of profits that partners will receive (VALENçA et al., 2014). In this scenario, *Y* can alter the power relationship by considering one or more power-changing operations. For instance, *Y* can apply *withdrawal* operation and neglect the existing dependence on *Y* by strengthening its relationship with customers or prospecting new customers in a new market niche. *Y* could also adopt the *attachment* operation by implementing a new cutting-edge technology in an integrated product, causing *X* to depend on this innovation. In these situations, *Y* can (i) *exercise power capabilities that were not used in the relationship with X or that can be used in a different manner*, or (ii) *develop new power capabilities derived from other elements of the software ecosystem used as power sources*. Once adopting one or more power-changing operations, *Y* ultimately undermines or changes actions in the relationship. For instance, in light of a new benefit offered to *X* (*attachment* operation), *Y* gradually changes its role in the ecosystem or increases its participation in overall decisions (VALENçA; ALVES, 2017).

3 Research Method

The study was conducted as a descriptive case study to understand the impact of privacy security breaches in influential software ecosystems from a power perspective. Choosing such an approach aims to neither generalise nor conduct a theory test of any kind. Instead, the case study took a descriptive form, which is often used to provide researchers with a rich description of the actual phenomenon being studied (YIN, 2013). By combining grey literature research and literature review, we were able to conduct an analytical study on how privacy breach scandals can affect influential companies from a perspective of power. All the actors and keystones involved in a scandal hold a certain level of power capability, which reflects upon countless business and technical decisions on the companies' end in an attempt to repair the damage caused to the users. Fig 2 outlines all phases encompassed in this research. In Phase 1, we investigated known privacy breach cases. Phase 2 involved the execution of the case study. Phase 3 illustrates the validation process of impact analysis on these ecosystems from the perspective of power. Phase 4 describes the final analysis of ecosystem health and power-changing operations within the final selected cases after the prior validation.

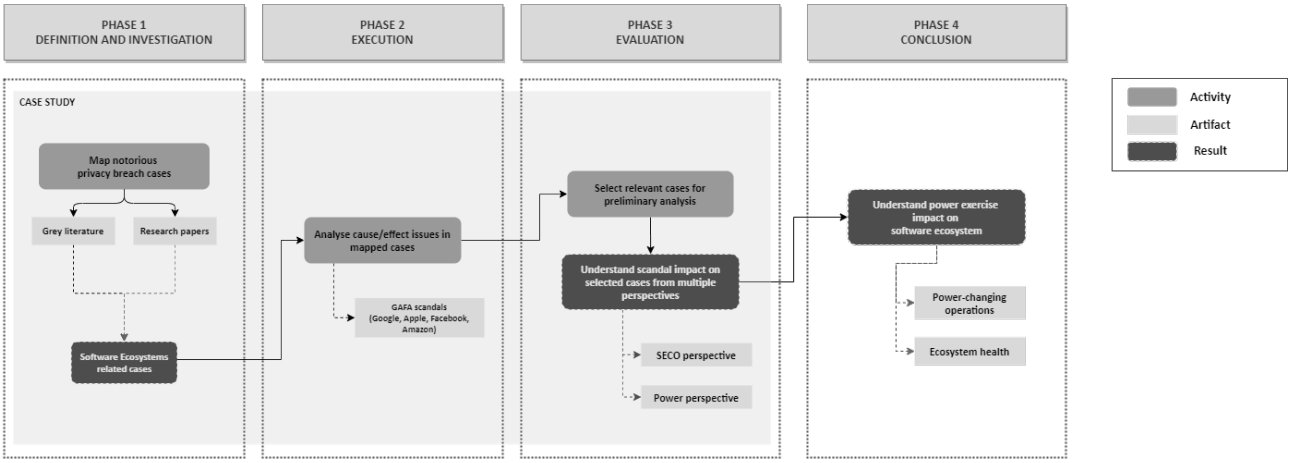

Figure 2 – *Research Phases*

3.1 Research Phases

3.1.1 Phase 1 - *Definition and Investigation*

3.1.1.1 Data Collection

This first phase commenced by actively seeking out information online concerning privacy leak and security breach scandals. Within the various results, we focused on selecting those involving well-established companies that operate in a software ecosystem format, such as Google and Apple. The conducted literature review reinforced fundamental concepts to conduct

a thorough analysis of all selected cases by drawing required elements that would emphasise our main research goal: understanding how power is exercised in the context of security breach among all entities involved. The process of data collection branched into two separate stages.

The first stage described the process of collecting data from websites reporting data leak and privacy breach cases. Initially, the focus remained on gathering as many relevant cases as possible within a range of recent years (between 2016 and 2020) using search queries with structure illustrated below. The investigation in its entirety focused on extracting information mostly from grey literature (due to the nature of this research) through Google's search engine, as well as examples potentially included in research papers. A total of **20 articles**, encompassing results relating to the proposed ecosystems across a variety of articles and publications, were collected and selected for further analysis. Detailed queries can be found in Appendix A.

> **privacy** AND (**scandal** OR **breach** OR **data leak**) AND (**Google** OR **Amazon** OR **Facebook** OR **Facebook**

As expected, there were a multitude of results involving several hundreds of different companies worldwide from multiple sources. While that would be promising to our studies overall, the main focus of the research was to investigate this particular situation within the context of software ecosystems. The second stage focused on refining the search queries to find assertive results, focusing on four specific companies that are knowingly meet the previously established requirements.

3.1.2 **Phase 2** - *Execution*

3.1.2.1 Data Analysis

For this next phase, the collection of 20 articles went through a final process of categorization considering a few important aspects, such as the company involved in the scandal *(e.g. Google, Amazon)*, the relevance of product or platform from the ecosystem with the security breach *(e.g. Google Chrome, Alexa)*, and reliability of the source reporting the case *(e.g. Financial Times, Forbes, New York Times)*. To determine the reputation factor of these sources, a media bias rating[1] scale was taken in consideration as a form of guidance, additionally to a manual verification of each source for factual reporting via the Media Bias/Fact Check[2] website. Altogether, a total of **14 different sources** were identified within the number of articles, and 5 cases per ecosystem, as illustrated in Fig. 3

[1] Media Bias Ratings - AllSides - <https://www.allsides.com/media-bias/media-bias-ratings>
[2] Media Bias/Fact Check - <https://mediabiasfactcheck.com>

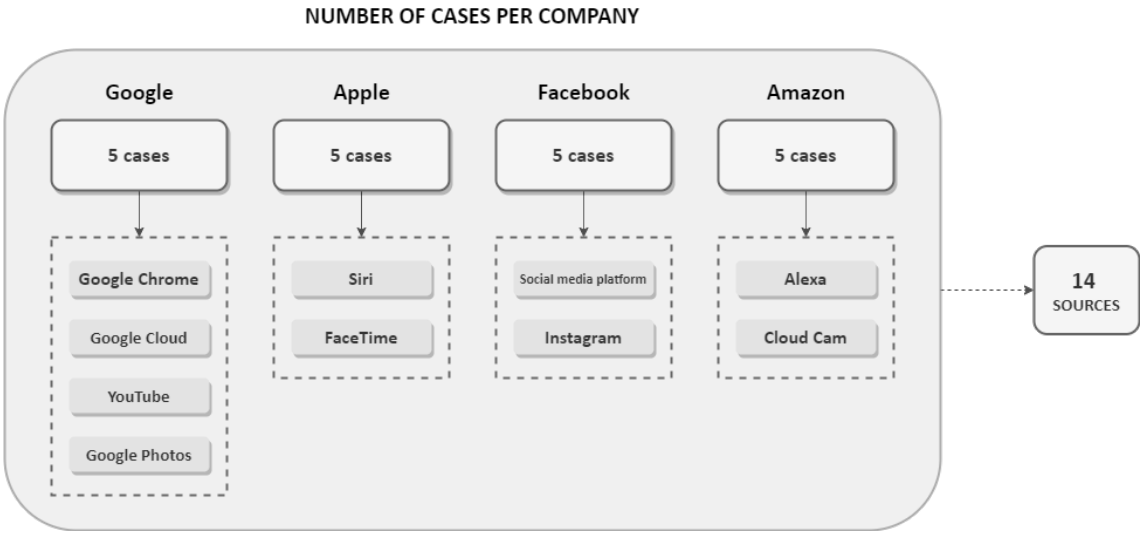

Figure 3 – *Data Collection*

Initially, the main focus was to review each individual case in order to identify relevant information on the matter, when and how it happened, how many people were affected by it, and what kind of consequence it entailed (i.e. financial, technical, business-related). Elements such as the company involved, the nature of the leaked data, and the number of users affected by the issue were fundamental to understanding the gravity of the situation and allowed a better comprehension of how further detailed analysis would take place in the upcoming phases. Once all the required data was extracted from the cases, a spreadsheet with an overview of each one was created with the goal of outlining the most poignant aspects of each case that correlates to the established criteria, serving as a form of breakdown sheet for further analysis. The complete spreadsheet can be found here.

3.1.3 **Phase 3** - *Evaluation*

In this phase, each case was thoroughly analysed and dissected considering the notion of ecosystems and power capability (VALENçA; ALVES, 2017), aiming to understand the elements at play and their interactions with each other (VALENçA; ALVES, 2017), in addition to interpreting what kind of repercussions a privacy breach entails and its impact across the relationships among ecosystem elements (Alves; Valença; Franch, 2019). Firstly, the key elements from each case were translated considering the software ecosystem nomenclature (VALENçA; ALVES, 2017) for a better understanding of the chosen scenario. The goal was to correctly identify a **keystone**, the **actors**, and the affected **software product or platform**. To categorise the data, this next step encompassed selecting one case from each company illustrated in the studies, specifically those with a great level of detail regarding the scandal happenings that would permit a proper analysis considering the elements involved. In order to decide which case would be prioritized among all, the decisive factors were defined considering (i) the amount of information regarding post-scandal actions taken by the company; (ii) direct quotations of responses from

the keystone's representatives; and (iii) evidences that alluded to the breach having negative implications on the keystone at play. Fig. 4 outlines the final structure of this step.

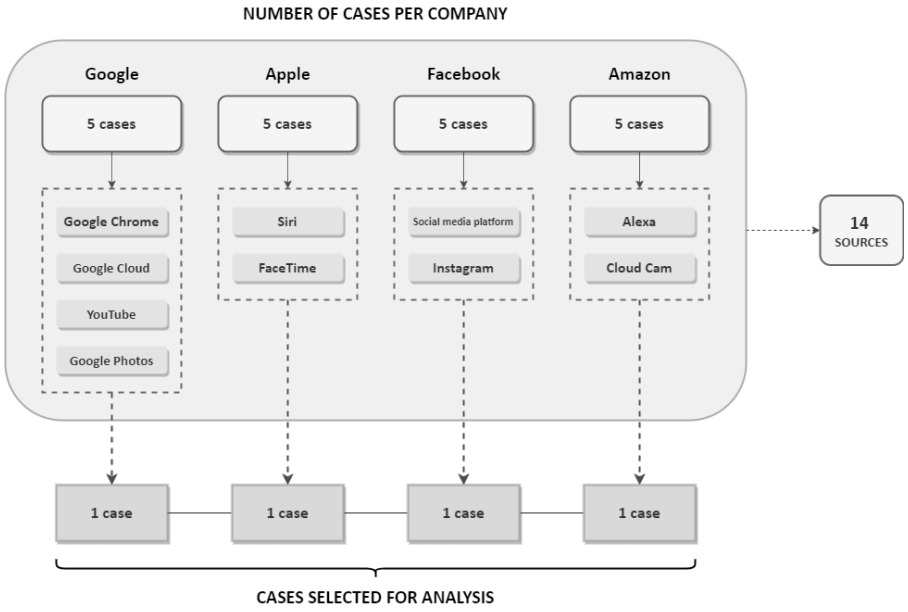

Figure 4 – *Data Categorisation*

Lastly, the analysis consisted in understanding how power was exercised and what kind of power capability was intrinsic to each element, a follow-up investigation on how different types of power were exercised among these elements was conducted, aiming to diagnose how that could potentially influence all parties involved in different ways. The process is detailed in Fig. 5.

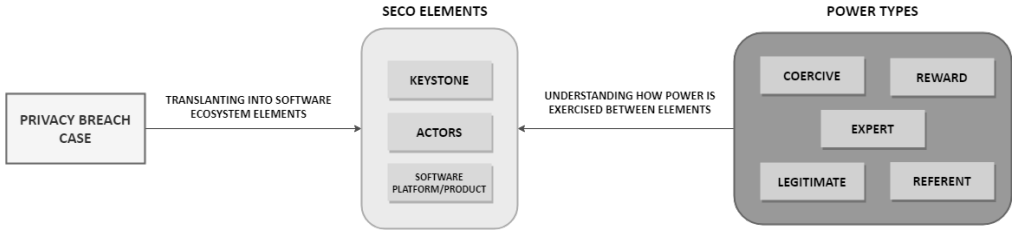

Figure 5 – *Data Analysis*

The four selected cases were used to further investigate on the relationship between actors and the keystone, as well as what kind of action it warranted once the breach was identified and exposed. Considering there is an innate interfirm dependency in these relationships, and the need for each to maintain a relationship with another to acquire resources and accomplish their goals (VALENçA; ALVES, 2017), it was also relevant to investigate points such as privacy policy changes, redefinition of multiple products' requirements, financially prohibitive measures, and most importantly, restructuring to avoid closure of partnerships. Keystones are responsible for ensuring a strategic position in the market, which translates to being able to create a prosperous ecosystem in which value is distributed among all participants (Alves; Valença; Franch,

2019), and that extends to handling potential privacy scandals with effective approaches to benefit all ends.

3.1.4 **Phase 4** - *Conclusion*

In this final phase, the results generated in the previous phase (described in section 3.1.3) were analysed to understand how power-changing operations (as detailed in Chapter 2) can be applied within each one of the cases once the power exercising was properly identified and categorised. These operations describe a degree of dependence among the elements involved in an ecosystem, and each one of them most likely possess a different level of dependence, which entails different levels of power (VALENçA; ALVES; JANSEN, 2018). The four power-changing operations utilised in this analysis are the ones proposed by Emerson (EMERSON, 1962).

Additionally, a discussion regarding the impacts on the health of an ecosystem in the privacy breach scandals considering these power dynamics followed suit. The goal is to understand determining factors that indicate how the ecosystem is evolving, the managerial strategies aiming the sustainability of individual players as well as the whole ecosystem are affected. The impact can be identified by analysing the dependency on actions and decisions taken by all the elements involved in software ecosystem (VALENçA; ALVES; JANSEN, 2018).

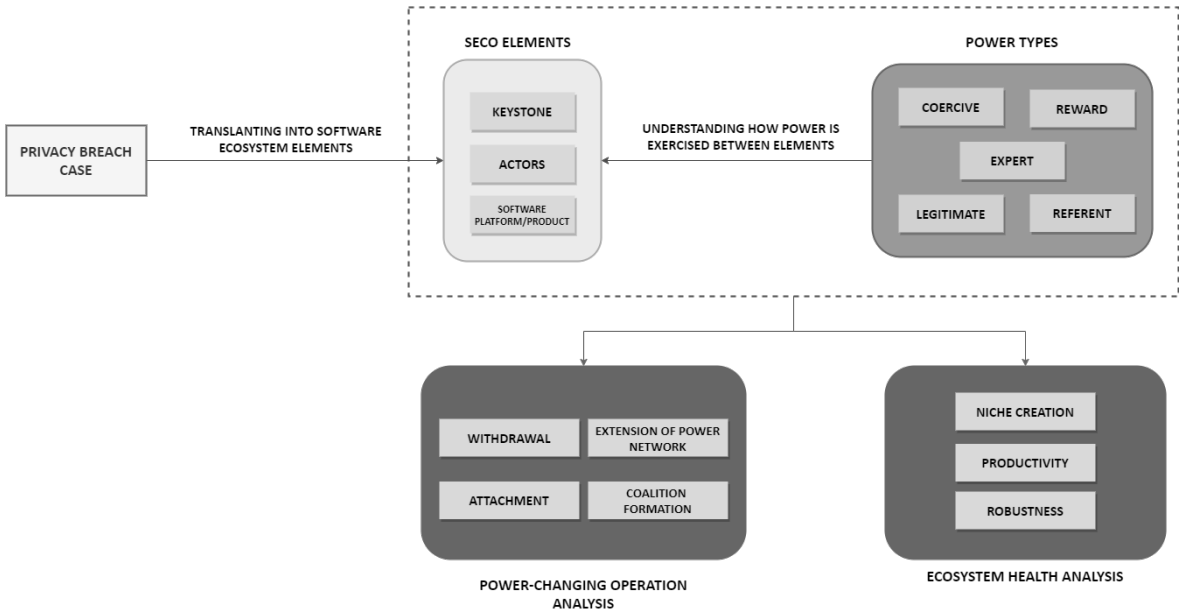

Figure 6 – *Final analysis*

4 Results

This chapter discloses a further detailed description of the results obtained by the studies conducted following the steps encompassed in Phases 2 and 3 as illustrated in Section 3.1 of chapter 4. The following sections are structured aiming to (i) **describe the privacy breach cases used for the extraction of results**; and lastly, (ii) **analyse power exercising in each one of the four cases**. The achieved results are discussed in the subsequent chapter based on the structure in which they were constructed throughout each analysis process.

4.1 Privacy Breach Cases

4.1.1 Google

In a case reported by New York Times, YouTube (which is owned by Google) illegally gathered children's data — including identification codes used to track web browsing over time — without their parents' consent (SINGER; CONGER, 2019). The accusations include marketing itself to advertisers as a top destination for young children, despite informing advertising firms that they did not have to comply with the children's privacy law because YouTube did not have viewers under the age of thirteen, only then proceeding to make millions of dollars by using the information harvested from these children to redirect specific ads their way.

As a result of this investigation, Google agreed to repair the damage by paying a record $170 million fine and to make needed changes to secure children's privacy on their YouTube platform in a move resulting from enforcement action taken by regulators in the United States against technology companies for violating users' privacy. Claims suggested that the video site had knowingly and illegally harvested personal information from children and used it to profit by targeting them with ads. In addition, as part of the settlement, YouTube also agreed to create a system that asks video channel owners to identify the children's content they post so that targeted ads are not placed in such videos. The regulators stipulated that YouTube must also obtain consent from parents before collecting or sharing personal details like a child's name or photos.

Despite reaching a significant settlement, regulators and other legal entities were extremely critical of how the case was conducted, including a U.S. Senator named Edward J. Markey, Democrat of Massachusetts, who described the $170 million penalty as merely *"a slap on the wrist for one of the world's richest companies"* (SINGER; CONGER, 2019).

> *"Merely requiring Google to follow the law, that's a meaningless sanction," said Jeffrey Chester, the executive director of the Center for Digital Democracy, a non-*

> *profit group whose efforts in the 1990s helped lead to the passage of the children's privacy law. "It's the equivalent of a cop pulling somebody over for speeding at 110 miles an hour, and they get off with a warning."* (SINGER; CONGER, 2019)

The article also reports that, under the agreement, required changes could limit how much video makers earn on the platform because, while they still make money on certain types of ads on children's videos, they will no longer be able to profit from ads targeted at children.

Consequently, YouTube said that not only had it agreed to stop placing targeted ads on children's videos, it would also stop gathering personal data about anyone who watched such videos, regardless of the company believing that the viewer was actually an adult. YouTube also claimed it would eliminate features on children's videos, like comments and notifications, that involved the use of personal data.

> *"Nothing is more important than protecting kids and their privacy. (...) From its earliest days, YouTube has been a site for people over 13, but with a boom in family content and the rise of shared devices, the likelihood of children watching without supervision has increased."* — YouTube's chief executive, Susan Wojcicki, regarding the settlement[1].

In addition to relying on reports from video creators, Ms. Wojcicki said that YouTube planned to use artificial intelligence in an attempt to identify content that targeted young audiences, like videos featuring children's toys, games,or characters.

With this report, the fact that Google has dealt with privacy violations repeatedly in recent years has been reinforced. The company is subject to a 20-year federal consent order signed in 2011 for deceptive data-mining related to Buzz, a now-defunct social network. The order required Google to establish a comprehensive privacy program and prohibited it from misrepresenting how it handles personal data (SINGER; CONGER, 2019).

4.1.2 Amazon

To illustrate this particular case, three different reports regarding the same subject matter were concatenated for further investigation. The core of the these privacy breach cases from Amazon concern the company's Alexa service, the popular and well-established voice assistant built in certain Amazon devices, such as the Echo speakers. Both Amazon Echo and the Alexa voice assistant have had widely publicised issues with privacy (BENJAMIN, 2020) and it branches into many problematic topics that have been exposed by the media on multiple occasions. An article published by The Guardian (LYNSKEY, 2019) in 2019 reported a series of mishaps involving Alexa such as:

[1] "The Most Measured Person in Tech Is Running the Most Chaotic Place on the Internet" - <https://www.nytimes.com/2019/04/17/business/youtube-ceo-susan-wojcici.html>

- An Amazon customer in Germany was mistakenly sent about 1,700 audio files from someone else's Echo, providing enough information to name and locate the unfortunate user and his girlfriend.
- In San Francisco, Shawn Kinnear claimed that his Echo activated itself and said cheerfully: "Every time I close my eyes, all I see is people dying.".
- In Portland, Oregon, a woman discovered that her Echo had taken it upon itself to send recordings of private conversations to one of her husband's employees.

In a subsequent statement, Amazon attributed the error to Echo mishearing the wake word, which lead to a request to send a message, mishearing then a name in its contacts list and then misheard a confirmation to send the message. Another publication, Bloomberg, analysed transcripts from Alexa and identified that, in more than one out of 10 transcripts analysed, Alexa did wake up accidentally. These dangerous slips on Amazon's end raised major concerns regarding the way Alexa devices interact with other services, directly "risking a dystopian spiral of increasing surveillance and control" (BENJAMIN, 2020).

An article published by Washington Post highlighted problems related to Alexa's data capture with a report on users being unable to take any actions to prevent Amazon from collecting data other than muting the device's microphone altogether (FOWLER, 2019). This issue is also linked to another practice implemented by the company where recordings are listened and reviewed by human contractors under the argument of "[listening] to recordings to train its artificial intelligence" and admittedly reported that "some of those employees also have access to location information for the devices that made the recordings" (FOWLER, 2019). The handling of personal customer data by Amazon raised concerns on all fronts, reinforcing that the service acquired is also aware of what the user are searching for, listening to or sending in their messages.

> *"Many smart-speaker owners don't realize it, but Amazon keeps a copy of everything Alexa records after it hears its name. Apple's Siri, and until recently Google's Assistant, by default also keep recordings to help train their artificial intelligences."* (FOWLER, 2019)

The most concerning factor, reported by one of the articles, is that Amazon is disturbingly quiet, evasive, and reluctant to act when it comes to tackling the privacy implications of their practices, many of which are buried deep within their terms and conditions or hard-to-find settings (BENJAMIN, 2020). Whether it is the amount of data they collect or the fact that they reportedly pay employees and, at times, external contractors globally to listen to recordings to improve accuracy, the potential exists for sensitive personal information to be leaked through

these devices. Criticism towards the way Amazon chooses to handle personal data and its practices is also questioned, accompanied by actions that should be required in order to respect these boundaries.

> *"It should be on the box. (...) I doubt they thought no one would care. I think they were trying to keep it quiet because if users knew what was going on they might stop buying the devices. It was a calculated business decision."* — Dr Jeremy Gillula, project director at the Electronic Frontier Foundation (LYNSKEY, 2019).

Amazon's response, on the other hand, suggests different approaches as it reassures they do not disclose customer information unless required to do so to comply with a legally valid and binding order (BENJAMIN, 2020). It also recurrently reassures that, in order to improve their services, "[it] is only possible by training her [Alexa] with voice recordings to better understand requests, provide more accurate responses, and personalize the customer experience," (FOWLER, 2019) according to Beatrice Geoffrin, director of Alexa privacy.

> *"Customer trust is at the centre of everything we do and we take customer privacy very seriously. We continuously review our practices and procedures to ensure we're providing customers with the best experiences and privacy choices. We provide customers with several privacy controls, including the ability to review and delete their voice recordings. To help improve Alexa, we manually review an extremely small sample of Alexa requests to confirm Alexa understood and responded correctly. Customers can opt out of having their voice recordings included in that review process."* — Amazon's spokeswoman (LYNSKEY, 2019)

4.1.3 Facebook

In August 2019, Business Insider reported on a combination of configuration errors and lax oversight by Instagram that allowed Hyp3r, a vetted advertising partner from the social network, to misappropriate vast amounts of public user data. The San Francisco-based marketing firm created detailed records of users' physical whereabouts, personal bios, and photos that were intended to vanish after 24 hours (PRICE, 2019). This partner developed a tool that could successfully "geofence" specific locations and then harvest every public post tagged with that location on Instagram.

Hyp3r scraped and stitched users' profiles together, which constituted a clear violation of Instagram's rules. However, it all occurred on Instagram's watch throughout 2019. In particular, Hyp3r was considered by Instagram as one of its preferred "Facebook Marketing Partners" (PRICE, 2019). Stories from ordinary users of Instagram have never been available through Instagram's API. In particular, these posts were supposed to disappear after 24 hours. Hyp3r orchestrated a way to collect this type of data as well, which then allowed this partner to save the

temporary images indefinitely, along with the associated metadata. One of the key issues relates to the uncertainty regarding the total volume of Instagram data that Hyp3r obtained, even though the firm had publicly affirmed it withheld ”a unique dataset of hundreds of millions of the highest value consumers in the world,” and more than of 90% of such data came from Instagram” (PRICE, 2019).

In order to provide the capabilities of service, the unauthorised use of Instagram data by Hyp3r was done in three crucial ways (PRICE, 2019):

- *”It took advantage of an Instagram security lapse, allowing it to zero in on specific locations, like hotels and gyms, and vacuum up all the public posts made from the locations;*
- *At these locations, it systematically saved users’ public Instagram stories — a type of content designed to vanish after 24 hours — including the individual photos that users shared in the stories, in a clear violation of Instagram’s terms of service;*
- *It scraped public user profiles on a broad basis, collecting information like user bios and followers, which it then combined with the other location information and data from other sources.”*

As pinpointed by the article, Hyp3r distinctly appeared to violate Instagram’s rules on multiple points with their scraping techniques. Despite Instagram’s requirement to store or cache content only ”for the period necessary to provide your app’s service”, Hyp3r stored user data indefinitely, according to multiple sources. Another example: the prohibition on ”reverse engineer[ing] the Instagram’s APIs” was neglected by Hyp3r, which deliberately rebuilt its own version of an API that Instagram shuttered after Cambridge Analytica (PRICE, 2019). The result included a database of thousands of locations, including ”hotels, casinos, cruise ships, airports, fitness clubs, stadiums and shopping destinations across the globe,” as well as hospitals, bars, and restaurants (PRICE, 2019).

Additional information also revealed a publicly available JSON package that bundles up various bits of data in an easy-to-access format, when users access Instagram through their web browsers. This JSON is available by simply appending a short string of characters to any Instagram URL. No logging in is required to gain approval or to authenticate one’s identity in any way to access it (PRICE, 2019), which can be clearly categorised as an unexpected breach on Instagram’s end.

The issue regarding Instagram and Hyp3r demonstrates one of Facebook’s biggest struggles when it comes to restricting users’ personal information and the way it extends beyond the core of their main Facebook app. Instagram is certainly the only service to have been affected over the years, but Hyp3r is probably not the only business scraping its data (PRICE, 2019). Hence, Hyp3r’s activity raises questions regarding the extent of the due diligence that Insta-

gram and its parent company Facebook conduct on partners using their platform, as well as on their own procedures to safeguard user data.

> *"Like many big platforms, Instagram has an API, or application programming interface, that allows developers to build services that can interact with its platform. Publicly, Hyp3r welcomed Instagram's API changes, writing a worthy blog post in which it said it ""understand[s] and welcome[s] the changes that Facebook is making to protect the privacy of all of us,"" and promising its data would never be used for political purposes. But behind the scenes, the company got to work building a system that could disregard Instagram's decision and keep on harvesting data anyway, sources told Business Insider."* (PRICE, 2019)

Despite these facts, Hyp3r denied breaking Instagram's rules. This partner argued that it accesses public data on Instagram, which is legitimate and justifiable. Besides, it claimed to be confident that any issues with Instagram would be resolved shortly. The result of the public information it gleaned was a sophisticated database about Instagram users, their interests, and their movements. Hyp3r openly touted such database to customers as one of its key selling points, despite the fact that Instagram's policies were structured so that such a thing would not be possible.

As a response to the scandal, Instagram sent Hyp3r a cease-and-desist letter after being presented with Business Insider's findings, which confirmed that the startup broke the rules of the social network (PRICE, 2019). As a result, Hyp3r promptly armed its defense: it claimed to process public data, whose harvest does not require consent from Instagram users. It also added that companies have legitimate business needs that justify knowing what is being shared from their properties (PRICE, 2019).

> *"HYP3R's actions were not sanctioned and violate our policies. As a result, we've removed them from our platform. We've also made a product change that should help prevent other companies from scraping public location pages in this way," a Facebook spokesperson said in a statement.* (PRICE, 2019)

An Instagram spokesperson also reassured that the company periodically reviews Facebook Marketing Partners to ensure compliance (PRICE, 2019), which led to inevitable actions on Facebook's end. Instagram also bans data from being transferred "to any ad network,". However, the Instagram data could be plugged into Facebook's own ads manager to target people with advertisements. It means Facebook indirectly profited from Hyp3r's data collection.

In response to Hyp3r's actions, Instagram has made a change to prevent public location pages from being available to logged-out users. It has also completely revoked Hyp3r's access to its APIs and removed it from the list of Facebook Marketing Partners (PRICE, 2019).

4.1.4 Apple

For this case, two complementary articles published by Forbes illustrate the scandal scenario concerning Siri, Apple's groundbreaking and popular voice assistant service built in a variety of Apple products. These reports shine a light on a sensitive and concerning topic regarding Apple's practices when it comes to handling private data from customers: "a small proportion of Siri recordings are passed on to contractors working for the company around the world" (SU, 2019b). According to one of the articles, these audio recordings have been sent to Apple "to improve Siri after an accidental activation of Siri, either through [Apple's] smartwatch, the HomePod wireless speaker or one of the other Apple mobile devices including the iPhone, the iPad, or the iPod touch" (SU, 2019b). This situation was labeled as a concerning privacy gaffe and raised questions regarding the severity level of Apple concerning its own privacy matters. Moreover, customers may doubt whether or not Apple is, in fact, practicing what it has been preaching: there is "a false sense of privacy that Apple has communicated through its marketing strategy to help distinguish itself from Amazon and Google" (SU, 2019b).

> *"There have been countless instances of recordings featuring private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on. These recordings are accompanied by user data showing location, contact details, and app data."* (SU, 2019b)

A report, published in late July 2019 by the Guardian, revealed that Apple contractors were regularly hearing confidential details on customers' Siri recordings[2], which led the company to promptly review the process it uses to handle the recordings of Siri queries, and the subsequent announcement that it would turn off recordings by default and bring the human evaluation process in-house (SU, 2019a).

> *"We know that customers have been concerned by recent reports of people listening to audio Siri recordings as part of our Siri quality evaluation process—which we call grading,"* an Apple spokesperson commented. *"We heard their concerns, immediately suspended human grading of Siri requests and began a thorough review of our practices and policies. We've decided to make some changes to Siri as a result."* (SU, 2019a)

In addition, unlike Alexa and Google Assistant, there is no way to opt out of having users' audio recordings sent to any of the Apple's servers. However, the company clearly stipulates in its privacy policy that it does send to its servers information such as *"your name, contacts, music you listen to, and searches to help Siri recognize your pronunciation and provide better responses"* (SU, 2019b).

[2] "Apple contractors 'regularly hear confidential details' on Siri recordings" - <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings>

> *"We at Apple believe that privacy is a fundamental human right. But we also recognize that not everyone sees things as we do. In a way, the desire to put profits over privacy is nothing new. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded, and sold. Taken to its extreme, this process creates an enduring digital profile and lets companies know you better than you may know yourself."* — Tim Cook, Apple CEO, at the '40th International Conference of Data Protection and Privacy Commissioners' in October 2018. (SU, 2019b)

Regardless of the evident controversies illustrated in both reports, Apple still claimed it would eventually resume the Siri grading program later the same year. Hence, it would present a Siri software update with the promise of three major changes (SU, 2019a):

- *"First, by default, Apple will no longer retain audio recordings of Siri interactions and requests but will continue to use computer-generated transcripts in machine learning training to improve Siri, determine common usage patterns, and update language and understanding models. The transcripts may also be used to resolve critical problems that affect Siri reliability. According to Apple, these transcriptions are associated with a random identifier, not your Apple ID, for up to six months.*
- *Second, users will be able to opt-in to help Siri improve by learning from the audio samples of their requests and those who choose to participate will be able to opt-out at any time.*
- *Third, when customers opt-in, only Apple employees—not contractors anymore—will be allowed to listen to audio samples of the Siri interactions and delete any recording which is determined to be an inadvertent trigger of Siri."*

4.2 Power Relationships

4.2.1 *Power exercising analysis*

4.2.1.1 Google

It is understood that YouTube (owned by the Alphabet Inc.[3] group) is seductive to users across the board. For the past few years, the company has redirected its efforts to accommodate underage users on its platform and service. The exercise of **expert power** can be identified in how YouTube has orchestrated its marketing strategies to make advertisers recognise its platform as a top destination for young children, despite telling them it would not require any com-

[3] American multinational conglomerate headquartered in Mountain View, CA. It was created through a restructuring of Google and became the parent company of Google and several former Google subsidiaries. - <https://abc.xyz>

pliance with children's privacy laws as YouTube "did not have users under 13" [PC_EXYT01] (SINGER; CONGER, 2019).

Expert power of YouTube to orchestrate marketing strategies towards specific customer base [PC_EXYT01]	
EXERCISE OF POWER	*YouTube redefines its marketing strategies to target a specific customer base through strategic advertisers.*
SOURCES OF POWER	*Relevant partnerships and reliable marketing information.*

Table 1 – *Description of YouTube's power capability to exercise **expert** power [PC_EXYT01]*

The expert power exercised by YouTube is such that users are not necessarily suspicious of any malicious activity, with factors such as reputation and trust coming to play in the relationship between the keystone and customer base. This comfort zone granted YouTube a silent permission to illegally gather, monitor, and track children's data without their parents' consent, as well as to serve targeted ads to young children (SINGER; CONGER, 2019), putting itself in a tough spot. This situation paved the way for the exercise of **coercive power** by legal entities, when legal clauses became part of the overall equation of the scandal by threatening Google's revenue models.

New York's Attorney General Letitia James, responsible for enforcing the federal children's privacy law in the state, notified the trade commission of apparent violations of the law on the site (SINGER; CONGER, 2019). This situation resulted in the penalty and changes encompassed in the settlement along with the Federal Trade Commission [PC_COYT01]. The accusations against YouTube pointed to a direct violation of the federal Children's Online Privacy Protection Act (COPPA).

> *"The move is the latest enforcement action taken by regulators in the United States against technology companies for violating users' privacy (..) It follows a $5 billion privacy settlement between the trade commission and Facebook in July over how the company collected and handled user data.* (SINGER; CONGER, 2019)

Coercive power of legal entities to notify legal authorities about YouTube's law violations on software product [PC_COYT01]	
EXERCISE OF POWER	*Attorneys and trade commission officers penalise keystone financially and demand privacy changes under legal settlement.*
SOURCES OF POWER	*Legal permissions to investigate disobedience through knowledge of established laws.*

Table 2 – *Description of legal entities' power capability to exercise **coercive** power [PC_COYT01]*

Like other companies caught in a similar scandal, Google sought to make amends for requirements they should have been complying with in the first place. The company began by offering financial compensation to repair damage under the legal settlement, reinforcing its ability to exercise **reward power** [PC_RWYT01]. Consequently, other changes were agreed upon YouTube's end, such as *"create a system that asks video channel owners to identify the children's content they post so that targeted ads are not placed in such videos"* (SINGER; CONGER, 2019).

> *"To settle the charges, YouTube agreed to the $170 million penalty, with $136 million going to the trade commission and $34 million to New York State. It is the largest civil penalty ever obtained by the commission in a children's privacy case, dwarfing the previous record fine of $5.7 million against the owner of the social video-sharing app TikTok."* (SINGER; CONGER, 2019).

Reward power of YouTube to offer monetary compensation to repair damages [PC_RWYT01]	
EXERCISE OF POWER	*Keystone compensates authorities for breach incident after legal demand.*
SOURCES OF POWER	*Financial resources originated from keystone's significant revenue model.*

Table 3 – *Description of YouTube's power capability to exercise **reward** power [PC_RWYT01]*

Regardless, the case still cornered YouTube into taking firmer and visible actions that reach beyond the users alone, proving its ability to exercise **coercive power** upon users and third-party entities involved. It agreed to not only stop placing targeted ads on children's videos, but also cease gathering personal data about anyone who watched such videos, even if the company believed that the viewer was an adult (SINGER; CONGER, 2019). The agreement also included eliminating features on children's videos, like comments and notifications, that involved the use of personal data [PC_COYT02].

> *"The changes required under the agreement could limit how much video makers earn on the platform because while they still make money on some kinds of ads on children's videos, they will no longer be able to profit from ads targeted at children."* (SINGER; CONGER, 2019)

Coercive power of YouTube to redefine its targeted ad and data collection practices to avoid reaching unsuitable users [PC_COYT02]	
EXERCISE OF POWER	*Keystone reshapes strategies for targeting ads on its software product and limits the collection of personal data from addressed customer base.*
SOURCES OF POWER	*Technical orchestration of its software products/services, combined with a strong knowledge of market information.*

Table 4 – *Description of YouTube's power capability to exercise **coercive** power [PC_COYT02]*

Another action on YouTube's end can be understood as **referent power** upon users and third-party entities involved. These actions involved funneling $100 million to creators of children's content over the next three years after 2019. (SINGER; CONGER, 2019) [PC_RFYT01]. Additionally, YouTube claimed it would *"heavily promote YouTube Kids, its child-focused app, to shift parents away from using the main YouTube app when allowing their children to watch videos"* (SINGER; CONGER, 2019).

Referent power of YouTube to funnel financial resources towards content creators for its customer base [PC_RFYT01]	
EXERCISE OF POWER	*Keystone redefines investments and financial compensation for content creators using its software product to generate content, aiming to preserve its reputation.*
SOURCES OF POWER	*Technical orchestration of its software products/services and strong reliability on its revenue model.*

Table 5 – *Description of YouTube's power capability to exercise **referent** power [PC_RFYT01]*

The exercise of power for this case can be illustrated in the form of a power relationship model, considering the power types that were outline throughout this section, along with the its respective power capabilities related to each power type, as illustrated in Fig.7.

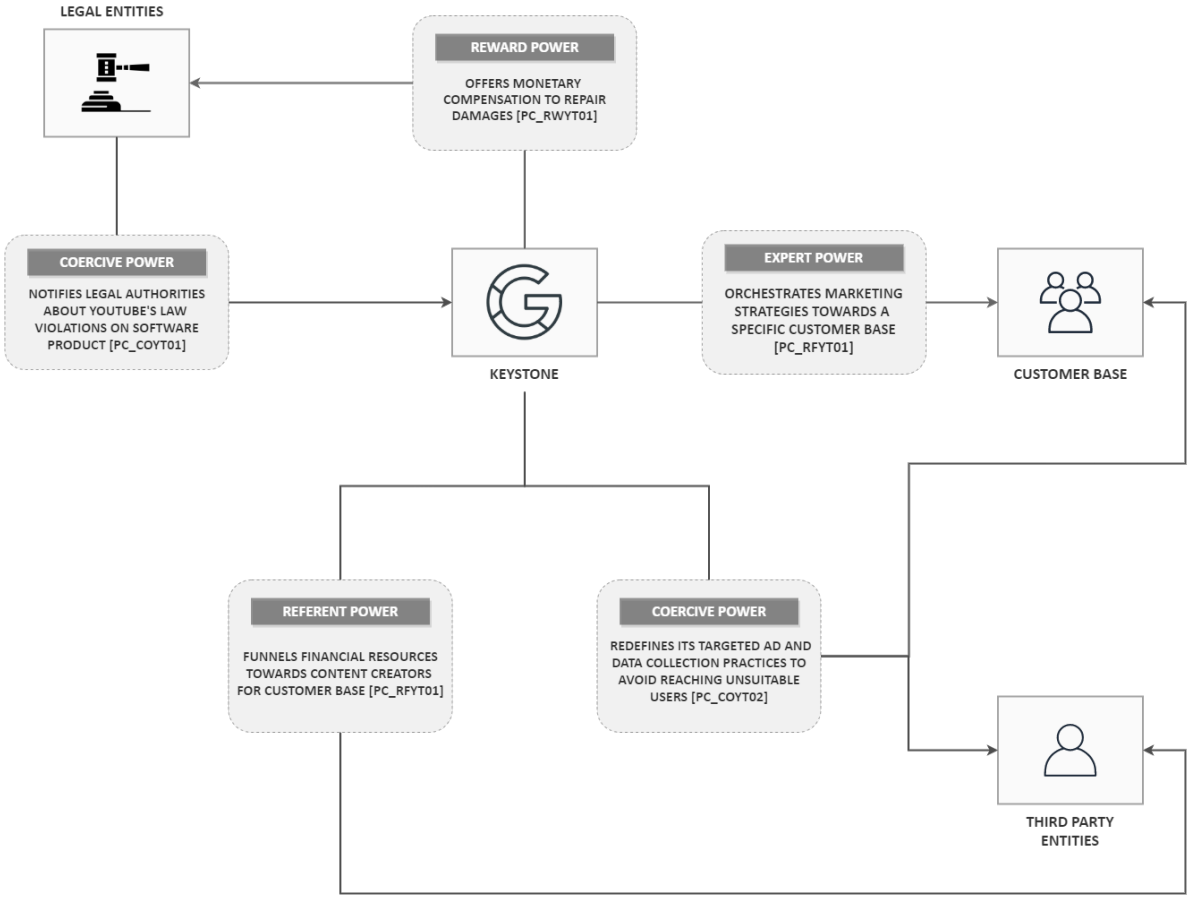

Figure 7 – *Power relationship model for Google case*

4.2.1.2 Amazon

Concerning voice assistants, there is no doubt that Amazon is a well-known and influential entity among them. The Alexa service is well-established and broadly used, which yields data and privacy issues in this ecosystem more critical. Both the service and Amazon's Echo product are part of a series of privacy scandals due to the broad adoption of both service and product. The main issue lies in customers being unable to stop Amazon from making recordings of their conversations with Alexa unless Echo's microphone is completely muted. Amazon's systems appear not just designed to collect as much data as they can, but also to create ways of sharing it (FOWLER, 2019), raising concerns when compared to its biggest competitors.

> *"While Apple and Google – who face their own privacy issues – have similar voice assistants, they have at least made progress running the software directly on their devices so they won't need to transfer recordings of your voice commands to their servers."* (BENJAMIN, 2020)

Amazon's biggest advantage lies in the exercise of **expert power** over its customers. By *"accurately interpreting voice commands by taking account of different languages, accents,*

tones, contexts and degrees of ambient clutter" (LYNSKEY, 2019), Amazon improves their services. As these solutions become practical, they bring a sense of trust and convenience that often retain users in the ecosystem [PC_RFAZ01]. Such performance *"requires far more computational power than a single device can contain; therefore, most of the work is performed in the cloud, which is how human monitors are able to collect and analyse voice recordings"* (LYNSKEY, 2019). Nevertheless, these arguments denote Amazon's invasive practices, with users facing a questionable data analysis process that tech companies routinely make obscure in terms of extent and nature of the data harvesting.

> *"Google and Amazon have shown us that they're inclined to take as much as they can until someone catches them with their hand in the cookie jar. I hate to be dramatic, but I don't think we're ever going to feel safe from their data-collection practices"*. — Adam Clark Estes, Gizmodo[4] editor (LYNSKEY, 2019)

Referent power of Amazon to exude sense of trust and convenience capable of retaining users due to practicality [PC_RFAZ01]	
EXERCISE OF POWER	*Keystone continuously attracts new customers and retains its existing customers regardless of any potential mishandling of data.*
SOURCES OF POWER	*Established reputation, along with innovative software solutions (products, services) that offer significant value.*

Table 6 – *Description of Amazon's power capability to exercise **referent** power [PC_RFAZ01]*

Amazon exercises **legitimate power** of analysing user data in order to provide services that are painstakingly designed for the customers. This power is enabled by the knowledge of what users are searching for, listening to, or sending in personal messages [PC_LGAZ01], giving the company a large degree of control over the customer base's data (BENJAMIN, 2020). However, there are concerns about such power capability based on users' information. Amazon signed a deal with UK's National Health Service (NHS) for medical advice provided via the Echo assistant, which could lead to users' health data getting linked to online shopping suggestions, third-party ads for costly therapies, and even ads that are potentially traumatic and often lead to some sort of oversharing with the company (BENJAMIN, 2020), regardless of users' willingly deciding to cut ties with what the service can actually access.

> *"You can tell Amazon to delete everything it has learned about your home, but you can't look at it or stop Amazon from continuing to collect it."* (FOWLER, 2019)

[4] Gizmodo World - <https://gizmodo.com/>

Legitimate power of Amazon to access and control users' data to customise its services/products [PC_LGAZ01]	
EXERCISE OF POWER	*Keystone utilises personal data from users to customise its services/products.*
SOURCES OF POWER	*Valuable personal data from users (market information).*

Table 7 – *Description of Amazon's power capability to exercise **legitimate** power [PC_LGAZ01]*

It is also possible to identify **legitimate power** being exercised as it is known that third-party services can serve as a pool of data from which Amazon services and products can collect information [PC_LGAZ02], raising concerns regarding how Alexa devices interact with other services (BENJAMIN, 2020). Nonetheless, Amazon acknowledges it collects data about third-party devices even when users do not utilise Alexa to operate them. It also mentions Alexa needs to know the "state" of users' devices "to enable a great smart home experience" (FOWLER, 2019), while it is fairly unlikely that customers are [often] aware of this practice among other powerful ecosystems as a whole.

Legitimate power of Amazon to collect data through third-party devices via integration with its services/products [PC_LGAZ02]	
EXERCISE OF POWER	*Keystone builds database of users' personal data from third-party applications through its services/products.*
SOURCES OF POWER	*Well-performed integrations with other services and products (technical orchestration) due to a solid technical background (intellectual property), used to collect valuable data for improvement (market information).*

Table 8 – *Description of Amazon's power capability to exercise **legitimate** power [PC_LGAZ02]*

The exercise of power for this case can be illustrated in the form of a power relationship model, considering the power types that were outline throughout this section, along with the its respective power capabilities related to each power type, as illustrated in Fig.8.

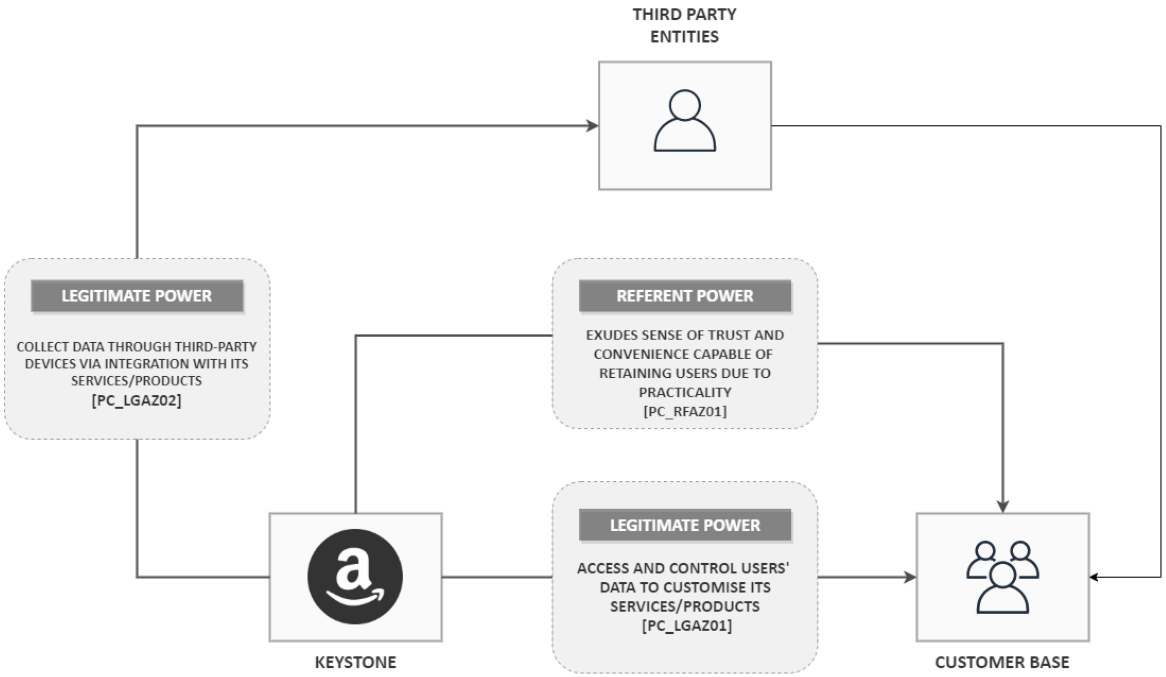

Figure 8 – *Power relationship model for Amazon case*

4.2.1.3 Facebook

Facebook has established a rather controversial reputation for itself regarding data handling and privacy, one that extends to its other products such as Instagram. The scandal broke after it was discovered that Hyp3r, one of its now former advertising partners, misappropriated vast amounts of public user data and created detailed records of users' physical whereabouts, personal bios, and photos that were intended to vanish after 24 hours through the API provided by Instagram, all with the intent of utilising data in more ways than one.

> *"By harvesting them systematically from popular locations, Hyp3r became able to build up detailed profiles of huge numbers of people's movements, their habits, and the businesses they frequent over time."* (PRICE, 2019)

Naturally, an exercise of **expert power** is immediately identified from Instagram over Hyp3r, since the keystone is a source of crucial information for the advertiser solution to become what it is [PC_EXFB01], with *"the result of the public information it gleaned was a sophisticated database about Instagram users, their interests, and their movements"* (PRICE, 2019) ultimately becoming not only what Hyp3r utilised to orchestrate its marketing strategies to attract customers, but also their key selling point (PRICE, 2019).

Despite the controversy surrounding Hyp3r's practices to successfully collect data from Instagram, the former company reinforced such database was accessed through legit means. Hence, Hyp3r was exercising **legitimate power** over Instagram with a retort that argues how

"accessing public data on Instagram in this way is legitimate and justifiable" (PRICE, 2019), with confidence that any issues with Instagram would be resolved accordingly [PC_LGFB01].

Expert power of Instagram to provide key user data to third-party services [PC_EXFB01]	
EXERCISE OF POWER	*Keystone withholds valuable database from which partners can benefit from.*
SOURCES OF POWER	*High-end technical solutions to collect personal data from customer base (technical orchestration) for product improvement know-how (market information).*

Table 9 – *Description of Instagram's power capability to exercise **expert** power [PC_EXFB01]*

Legitimate power of Hyp3r to access information from Instagram's services for its own service/product [PC_LGFB01]	
EXERCISE OF POWER	*Partner accesses and collects data from keystone's primary database for its own service.*
SOURCES OF POWER	*An official partnership that grants third-party to access keystone's information (interfirm relationship) through intricate software solutions (technical orchestration).*

Table 10 – *Description of Hyp3r's power capability to exercise **expert** power [PC_LGFB01]*

Hyp3r's relationship with Facebook also illustrates the exercising of **reward power** coming to play, considering its groundbreaking services rely heavily on utilising third-party elements with a powerful reputation to boot, packaging that marketing strategy and selling to customers in a particularly seductive way [PC_RWFB01]. Naturally, their initial response suggested quite clearly it would welcome Instagram's API changes and other changes Facebook implemented *"to protect the privacy of all of us post the Cambridge Analytica scandal"* (PRICE, 2019).

Behind the scenes, however, Hyp3r focused on building a system that could disregard Instagram's decision in order to continue harvesting data regardless, exercising **legitimate power** as it willingly continued to go out of its way to dig further into, and beyond, what the world of what Instagram provided. To succeed in their data collection practices, Hyp3r *"[created] a tool that could "geofence" specific locations and then harvest every public post tagged with that location on Instagram"* (PRICE, 2019), taking advantage of an Instagram security lapse which allowed access to a vast amount of personal data from Instagram users.

> *"The result is a database of thousands of locations, including "hotels, casinos, cruise ships, airports, fitness clubs, stadiums and shopping destinations across the globe, as well as hospitals, bars, and restaurants."* (PRICE, 2019)

Reward power of Hyp3r to collect data from Instagram's database to design its services [PC_RWFB01]	
EXERCISE OF POWER	*Partner accesses and collects data offered from keystone to benefit its services and marketing strategy.*
SOURCES OF POWER	*Technical orchestration, interfirm relationship, market information.*

Table 11 – *Description of Hyp3r's power capability to exercise **reward** power [PC_RWFB01]*

However, despite Hyp3r's fervent claims of following the rules within the confines of its partnership with Instagram, the scraping appeared to violate Instagram's rules on multiple points, including a requirement to store or cache content only for as long as necessary to provide a required service (PRICE, 2019). Hence, the company stored user data indefinitely. By prohibiting the practice of the so-called "reverse engineer[ing]" of Instagram's APIs, Facebook's exercise of **coercive power** over its partner — a power it maintains over its partners in general — came to play when the company stepped in and *"completely revoked Hyp3r's access to its APIs, removed it from the list of Facebook Marketing Partners" (PRICE, 2019) despite initially including Hyp3r on exclusive list of partners* [PC_COFB01], [PC_COFB02].

The fallout with Hyp3r nicely illustrates the overall ability of coercion a company such as Facebook is capable of exercising over its partners, going to lengths to establish boundaries. In this case, changes included *"[making] a change to prevent public location pages from being available to logged-out users"* in response to this scandal, a direct consequence of what they claim to be *"[periodic] reviews [of] Facebook Marketing Partners to ensure compliance"* (PRICE, 2019). Additionally, an exercise of **coercive power** of media outlets over Facebook is identified through the published report of this scandal, which eventually led to Instagram sending Hyp3r *"a cease-and-desist letter after being presented with Business Insider's findings and confirmed that the startup broke its rules"* (PRICE, 2019), illustrating a chain reaction of power exercising [PC_COFB03].

Coercive power of Instagram to revoke Hyp3r's access to its services [PC_COFB01]	
EXERCISE OF POWER	*Keystone makes technical changes to prevent partners from accessing its database and potential misuse.*
SOURCES OF POWER	*Tweaking its service (technical orchestration) to prevent unauthorised third-parties to gain access to keystone's pool of data.*

Table 12 – *Description of Instagram's power capability to exercise **coercive** power [PC_COFB01]*

Coercive power of Instagram to terminate partnership through cease-and-desist letter [PC_COFB02]	
EXERCISE OF POWER	*Keystone effectively terminates partnership after fact-checking controversial practices on partner's end.*
SOURCES OF POWER	*Legal team to handle required measures (human resources) regarding any partnerships established by the keystone (interfirm relationship).*

Table 13 – *Description of Instagram's power capability to exercise **coercive** power [PC_COFB02]*

Coercive power of press and media outlets to expose Instagram x Hyp3r scandal [PC_COFB03]	
EXERCISE OF POWER	*Media outlets report on the breach scandal involving keystone and its partner's malpractices.*
SOURCES OF POWER	*Public prestige and means of investigation.*

Table 14 – *Description of press and media outlets' power capability to exercise **coercive** power [PC_COFB03]*

The exercise of power for this case can be illustrated in the form of a power relationship model, considering the power types that were outline throughout this section, along with the its respective power capabilities related to each power type, as illustrated in Fig.9.

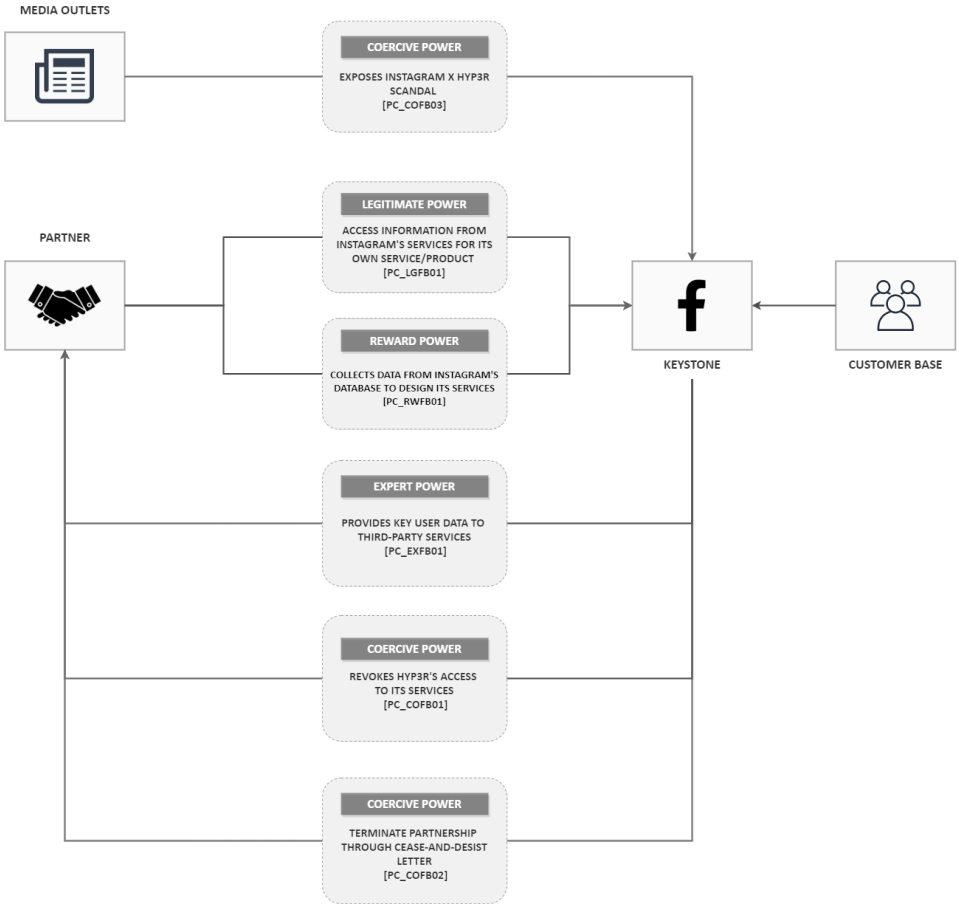

Figure 9 – *Power relationship model for Facebook case*

4.2.1.4 Apple

Much like Amazon, Apple has cemented its reputation when it comes to offering cutting-edge technology for voice assistant services with the launch of Siri in 2011, built in its many products. Notably, that alone happens to be not the only element the two companies have in common. Apple also keeps copies of conversations with Siri, claiming the voice data is assigned as a random identifier and is not linked to individuals (FOWLER, 2019). In a similar fashion, Apple was also questioned about its data handling practices. In particular, a report from The Guardian remarked that Apple failed to explicitly disclose to its customers that a large volume of incredibly sensitive and personal data was passing through human verification[2].

> *"There have been countless instances of recordings featuring private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on. These recordings are accompanied by user data showing location, contact details, and app data."* (SU, 2019b)

Apple is known for the kind of experience it offers and the convenience of using its integrated services. This reinforces its **referent power** over its customers. However, such power

capability causes the mishandling of data to be rarely considered until a critical data breach, for instance, comes to light [PC_RFAP01]. Apple seems to not only collect an overwhelming amount of data, but also transfer these scraps of data, which are *"carefully assembled, synthesized, traded, and sold"* (SU, 2019b) to its partners and third-party applications in the process. Unlike other major players such as Amazon (Alexa) and Google (Google Assistant), the company does not provide means to *"opt-out having your audio recordings sent to servers"* (SU, 2019b). In fact, none of the current leading digital voice assistants (Alexa, Google, and Siri) *"provide enough guarantees to help protect a user's privacy to recommend any of them"* (SU, 2019b).

Referent power of Apple to exude sense of trust and convenience capable of retaining users due to practicality [PC_RFAP01]	
EXERCISE OF POWER	*Keystone continuously attracts new customers and retains its existent customers regardless of any potential mishandling of data.*
SOURCES OF POWER	*Established reputation, intrinsically linked to its high-end products and services with significant attached value.*

Table 15 – *Description of Apple's power capability to exercise **referent** power [PC_RFAP01]*

However, it is possible to identify **coercive power** being exercised by media outlets and the press (and, consequently, users once they get to read these articles) as entities capable of exposing these negative practices. Once the case was exposed by these publications, Apple then takes some sort of action with the decision to take time to thoroughly review the process that it uses to handle the recordings of Siri queries (SU, 2019a) [PC_COAP01]. This situation caused Apple to announce that it would turn off recordings by default, as well as *"bring the human evaluation process in-house"* (SU, 2019a).

> *"We know that customers have been concerned by recent reports of people listening to audio Siri recordings as part of our Siri quality evaluation process—which we call grading. We heard their concerns, immediately suspended human grading of Siri requests and began a thorough review of our practices and policies. We've decided to make some changes to Siri as a result."* — Apple's statement (SU, 2019a)

Coercive power of press and media outlets to expose Apple's negative practices [PC_COAP01]	
EXERCISE OF POWER	*Media outlets report on keystone's privacy breach scandals and potential mishandling of customer base's data.*
SOURCES OF POWER	*Public prestige and means of investigation.*

Table 16 – *Description of press and media outlets' power capability to exercise **coercive** power [PC_COAP01]*

The core of the problem is the fact that Apple's privacy policy stipulates that certain personal information is sent to its servers (e.g. users' names, contacts, music they listen to, and searches to help improve Siri and provide better responses), which creates *"a false sense of privacy with their marketing messaging"* (SU, 2019b). As a result, it is possible to identify that the company exercises a type of **reward power** on its customers: as they overshare their data, Apple offers better curated personal service. The tech giant argues such data is needed because *"[the] goal with Siri, the pioneering intelligent assistant, is to provide the best experience for our customers while vigilantly protecting their privacy"* (SU, 2019a) [PC_RWAP01].

Even with the scandal hitting the general public and Apple suspending the 'grading process' that involved human intervention, Apple still planned to resume the grading program later in 2018, following a Siri software update to boot (SU, 2019a). However, it aimed to offer it with further restrictions to give users more control of their shared data through the option of them being able to opt-in on helping Siri improve by learning from their shared audio samples, with the possibility of participants opting out at any time.

Reward power of Apple to curate services to its customer base through collected personal data [PC_RWAP01]	
EXERCISE OF POWER	*Keystone is capable of curating personal service for its customer base by withholding a significant amount of users' data.*
SOURCES OF POWER	*Technical orchestration of its products that allow significant data collection.*

Table 17 – *Description of Apple's power capability to exercise **reward** power [PC_RWAP01]*

The exercise of power for this case can be illustrated in the form of a power relationship model, considering the power types that were outline throughout this section, along with the its respective power capabilities related to each power type, as illustrated in Fig.10.

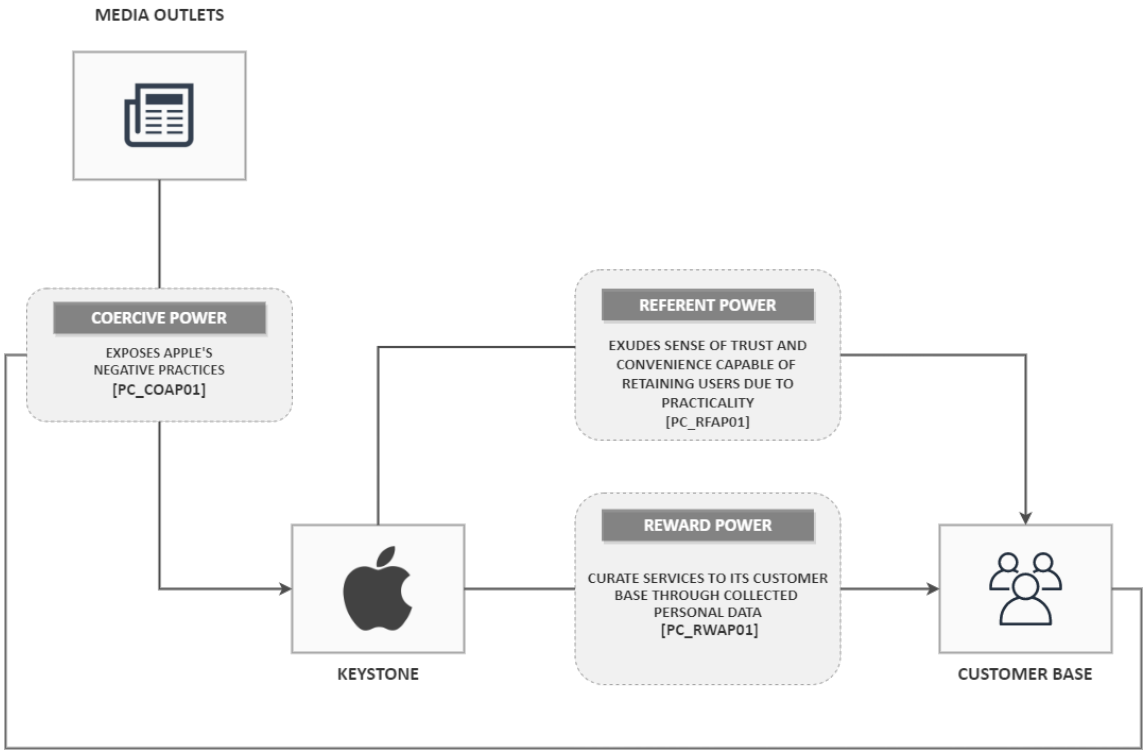

Figure 10 – *Power relationship model for Apple case*

5 Discussion

5.1 Understanding power-changing operations and ecosystem health in privacy breach cases

This chapter discusses the application of power-changing operations among entities involved in all four privacy breach cases based on the findings reported in section 4.2, exploring the potential outcome of these interactions (as illustrated in Fig. 1) and their subsequent impact on the health of these ecosystems.

5.1.1 Google

As presented in Fig. 7, the power model for the YouTube case outlines the instances of power exercise and YouTube's respective power capabilities. These power relationships involve the keystone company (Google), its complementors and users, setting the tone for the outcome of this particular case in more ways than one.

An initial observation showcases how YouTube's *reward power* results from the *coercive power* of regulators who cornered the company with legal demands of monetary compensation for the authorities reporting the case. By agreeing with the settlement, the move presents itself as a way for YouTube to preserve its reputation and thereby maintain its referent power. However, the move appeared to be poorly constructed and merely a temporary solution to a much bigger and more complex issue as the company continues to profit from these missteps, while failing to get to the core of privacy concerns. Such action is able to hold Google accountable for the consequences of its own errors, retaining its users within its customer base. Hence, it inevitably maintains the ecosystem's **robustness**.

By applying **withdrawal** operation upon YouTube, the platform's customer base could potentially reaffirm their discontentment by migrating to other ecosystems with similar solutions. Once aware that its power to compensate users would not suffice, the company could eventually redirect its attention to avoiding future privacy breaches by implementing approaches such as privacy by design, and guiding its services towards compliance with data regulations. . Within compliance, chances of getting caught in this type of scandal decreases quite drastically, avoiding any implementation of **extension of power network** from YouTube's customer base.

> *"The F.T.C. let Google off the hook with a drop-in-the-bucket fine and a set of new requirements that fall well short of what is needed to turn YouTube into a safe and healthy place for kids."* — Senator Edward J. Markey, Democrat of Massachusetts (SINGER; CONGER, 2019).

These consequences extend beyond YouTube itself due to demands established on the legal settlement. The company's *coercive power* comes to play over content creators by *"[limiting] how much video makers earn on the platform because while they still make money on some kinds of ads on children's videos, they no longer be able to profit from ads targeted at children."* (SINGER; CONGER, 2019). These creators implementing **withdrawal** operation by removing their content from YouTube, and consequently, **extension of power network** redirecting their content generating efforts elsewhere, as well as their aim at different children-focused platforms such as SuperAwesome[1]. This platform aims to *"[fill] the gap left by YouTube's move (...) to stop running targeted ads on videos designed for children* (O'REILLY, 2020). These moves would impact YouTube's **robustness** directly.

However, YouTube enhances its *referent power* by investing in creators for content directed at children with a total of $100 million, as well as *"heavily promote YouTube Kids, its child-focused app, to shift parents away from using the main YouTube app when allowing their children to watch videos"* (SINGER; CONGER, 2019). Therefore, Google ceases the negative consequences on its revenue model.This is a clear application of **attachment** operation, when Google retains the creators within the platform under reformed requirements and with additional benefits (injection of financial resources). Moreover, it keeps the customer base as it is. Such strategy generates a positive impact on the ecosystem's **productivity**.

5.1.2 Amazon

As presented in Fig. 8, the power model for this Amazon case outlines the instances of power exercise and the respective power capabilities. For this case, the intricacies of power exercise are rooted in Amazon's relationships with its customer base and complementors.

Amazon's *referent power* is the most relevant factor within the dynamics of this case. Due to its undeniably well-established reputation, the company has been able to engross its customer base significantly throughout the years, and that extends beyond the marketplace services it is known for. The company actively utilises users' data to curate their services/products, which allows it to continuously increase its customer base. By relying on the reputation factor, the company is able to implement certain practices that are either completely undisclosed or incredibly hard to detect within their privacy policy.

> *"Amazon is disturbingly quiet, evasive and reluctant to act when it comes to tackling the privacy implications of their practices, many of which are buried deep within their terms and conditions or hard-to-find settings. Even tech-savvy users don't necessarily know the full extent of the privacy risks, and when privacy features are added, they often only make users aware after researchers or the press raise the issue."* (BENJAMIN, 2020)

[1] "SuperAwesome - Making the Internet safer for kids" - <https://www.superawesome.com>

In light of the addressed scandal, despite the personalised service offered by Amazon, users could implement **withdrawal** operation over the company by taking a step back from its services once aware of its data handling practices. Additionally, these users could even adopt an **extension of power network** by opting to utilise other services provided by different companies. With this, they could potentially counteract Amazon actively adopting a **attachment** operation to maintain the bond between keystone and customer base, one that directly improves both the ecosystem's **robustness** and **productivity**.

Amazon's *referent power* originates from its strong reputation, and the implications of that power are translated into the company actively attracting new customers. Such significant customer base enables Amazon to gain access and control over this pool of data, legitimating its role as a controller and processor of said database. It strengthens the legitimate power of Amazon over both its customer base and third-party complementors within the ecosystem: the company can access customers' personal data through services/products and use it as a relevant asset. The company can customise, improve, and expand its solutions, which once again impacts ecosystem productivity positively on the **productivity** of the ecosystem. In the same fashion, Amazon is able to access users' information through third-party integrations with other services, which is a good indicator of its ability to further improve its **niche creation** through these collaborations for technical orchestration to develop new services/products.

Much like the Google case, users could also potentially retaliate against Amazon's practices and mishandles by adopting **withdrawal** operation. The movement from users to revoke to revoke the usage of its services/products could be a threat to the profits of the company. These users could also adopt **extension of power network** by utilising other services/products provided by different companies, inevitably impact negatively on Amazon's **robustness**. Considering the fact that *"CEOs are less likely to trivialise privacy concerns"* (LYNSKEY, 2019), a stance such as this one would certainly nudge an ecosystem like Amazon into revisiting its internal concerns to prevent future breaches by guiding the ecosystem towards compliance with regulations.

5.1.3 Facebook

As presented in Fig. 9, the power model for the Facebook case outlines the instances of power exercise with respective power capabilities. This scandal illustrates the coercive power of media outlets over big ecosystems in light of any signs of missteps, especially if that branches out to its partners and third-party complementors.

Another important aspect of the relationships of this case is how Instagram's *expert power* is so intrinsically linked to the enabling of Hyp3r's *reward* and *legitimate power*. Instagram serves as a pool of data for its own services and those from third-party solutions as this platform holds an immeasurable amount of crucial information from users. Instagram is a provider of a vast amount of crucial data to integrated services through its APIs. By permitting this kind

of access, the ecosystem's **niche creation** abilities are significantly enabled since these partners are able to access Instagram's databases through its provided APIs for their own services. Facebook could potentially increase **robustness** through these forged partnerships, similar to how it granted Hyp3r a slot in *"its exclusive list of Facebook Marketing Partners — a directory of vetted companies that "can give you superior insights and data for better marketing decisions"* (PRICE, 2019). The move could also avoid any adoption of **coalition formation** from these partners with other companies once given a privileged pass within Instagram/Facebook ecosystem.

Hyp3r was well aware of how relevant the data accessed through Instagram would be, and despite limitations determined by Facebook post Cambridge Analytica[2] scandal, the company reinforced its *legitimate power* over Instagram by orchestrating ways to access users' personal information by creating *"a tool that could "geofence" specific locations and then harvest every public post tagged with that location on Instagram"* (PRICE, 2019) and *"got to work building a system that could disregard Instagram's decision and keep on harvesting data anyway"* (PRICE, 2019). This could lead Hyp3r to adopt a **attachment** operation by offering their own customers a privileged service, reinforcing its *reward power* by curating and selling its own advertising services based on malicious data scraping while publicly offering *"features that far exceed what is available through Instagram's API, saying it "surfaces all public social activity from a location (...) so you never miss an opportunity to dazzle your customers"* (PRICE, 2019). It could also prevent any **extension of power network** from Hyp3r's customers to look for different advertising companies.

> *"Hyp3r's scraping [violates] Instagram's rules on multiple points, including a requirement to store or cache content only "for the period necessary to provide your app's service" (Hyp3r stored user data indefinitely, according to multiple sources), and a prohibition on "reverse engineer[ing] the Instagram's APIs" (Hyp3r deliberately rebuilt its own version of an API that Instagram shuttered after Cambridge Analytica)."* (PRICE, 2019)

> *"Before the scandal broke, Instagram's API allowed developers to search for public posts for a given location. But in the aftermath of it, Instagram began to deprecate (i.e. switch off) a bunch of its API's functionality, including location tools — causing chaos for companies, like Hyp3r, that had been relying on it."* (PRICE, 2019)

The consequences of Hyp3r's actions eventually leads to the exercise of *coercive power* from Business Insider[3], the publication that exposed its malicious practices to Facebook by presenting evidence after speaking with *"multiple former employees of Hyp3r to learn about its*

[2] "The Cambridge Analytica Files" - <https://www.theguardian.com/news/series/cambridge-analytica-files>
[3] "Business Insider" - <https://www.businessinsider.com>

practices and reviewed public documents and marketing materials that outline its capabilities." (PRICE, 2019). It led to the ecosystem exercising its own *coercive power* in different ways. Per an Instagram's spokesperson, it was known that *"the company periodically reviews Facebook Marketing Partners to ensure compliance"* (PRICE, 2019), paving the way for a potential adoption of **withdrawal** operation on misconducting partners in order to preserve the company's reputation. This move could also maintain its **niche creation** capabilities thriving to perhaps increase **productivity** in the form of new services/products.

> *"Before the scandal broke, Instagram's API allowed developers to search for public posts for a given location. But in the aftermath of it, Instagram began to deprecate (i.e. switch off) a bunch of its API's functionality, including location tools — causing chaos for companies, like Hyp3r, that had been relying on it."* (PRICE, 2019)

By taking advantage of the publication's exposure of the scandal, Facebook sent Hyp3r a *"cease-and-desist letter after being presented with Business Insider's findings and confirmed that the startup broke its rules"* (PRICE, 2019), along with completely revoking Hyp3r's access to its APIs and removing it from the list of Facebook Marketing Partners (PRICE, 2019). With the adoption of **withdrawal** from Hyp3r, Facebook could preserve its reputation by removing a misconducting partner from its network.

5.1.4 Apple

As presented in Fig. 10, the power model for this Apple case outlines the instances of power exercise and the respective power capabilities. The scandal surrounding Apple, much like Facebook's case (presented in section 5.1.3), describes the impact of media outlets and publications exercising coercive power over companies to demand clarification of their practices.

This case also illustrates the manifestations of the keystone's *referent power* over its customer base, reinforcing a reputation Apple has strongly cemented while continuously leveraging the company's thriving profits. Over the years, it has attracted users all across the board by offering one-of-a-kind services/products. This strong reputation grants it the ability to dig for further information from users without necessarily having to be transparent about it. Apple's *reward power* serves as a repackaging of their invasive practices to curate services based on personal information collected through their services/products, leading to the creation of*"a false sense of privacy with their marketing messaging"* (SU, 2019b). In light of these practices getting exposed, Apple's customer base could adopt a **withdrawal** operation by opting out of their services/products. They could also enable **extension of power network** by moving to other products from different companies. This migration could directly impact Apple's **robustness**, which then takes a toll on its revenue model. Additionally, their **productivity** could be also affected if its pool of data from users decreases in volume.

> *"This latest privacy scandal highlights the false sense of privacy that Apple has communicated through its marketing strategy to help distinguish itself from Amazon and Google." (SU, 2019b)*

However, the *coercive power* of media outlets stand out in the equation since it is known that Apple was cornered into responding to such questionable practices *"following a report published in late July by the Guardian which revealed that Apple contractors were regularly hearing confidential details on customers' Siri recordings"* (SU, 2019a). The negative repercussions could directly impact the company's **robustness** by driving users and complementors away from the ecosystem. The **productivity** could also be affected considering the migration of these actors from the ecosystem, ceasing their direct or indirect contribution to Apple's services/products. Potentially, its **niche creation** abilities could be impacted by the negative repercussions. As a way to prevent any of the outcomes previously described, Apple took action and was forced to reevaluate human intervention practices, eventually *"[deciding] to temporarily stop contractors from "grading" Siri voice recordings"* (SU, 2019a). With this, the company adopts an **attachment** operation to preventing users from taking a step back from their services/products, and consequently reinforcing Apple's *referent power* as it holds itself accountable for remedying its own errors.

5.1.5 Final remarks

Concerns with data and privacy protection are ever growing in the software industry, and more so regarding big influential tech companies such as the ones described throughout this research. With the implementation of data protection regulations, these legal requirements exercise an innate form of *coercive power* over companies who fail to comply with them. Privacy by design is a demanded requirement within the GDPR[4] compliance, which implies that any company utilising personal data to shape and operate their services must further concern themselves with data protection practices.

As previously illustrated, the dynamics of power-changing operations between Apple and Amazon (described in section 5.1.2) are very similar, considering their issues branch out from a nearly identical background. Trust and reputation play a huge role on the health of these ecosystems. It also raises questions regarding their adopted practices for service/product improvement involving a multitude of invasive practices.

Relying on reputation to exercise *reward power* with **attachment** operations could eventually result in external sources exercising *coercive power*. This would lead to an intense adoption of **withdrawal**, **extension of power network**, and perhaps even **coalition formation** from the customer base, complementors, and potentially partners.

[4]"Art. 25 GDPR - Data protection by design and by default" - <https://gdpr-info.eu/art-25-gdpr/>

6 Conclusion

6.1 Contributions

There is no denying that privacy breach scandals are capable of wreaking severe havoc within companies across the board, and it is certainly much more complicated when an influential ecosystem turns into the subject of study. Dealing with security and privacy architecture has become a major concern in the technology world and yet there are still gaps that allow these mishaps to happen more often than not. Through the interpretation of power exercising, it was possible to understand the dynamics between elements involved in a data breach scandal, the elements that grant them privileges or lack thereof, and consequences which reverberated either positively or negatively towards them.

This study aimed to showcase the intricacies of these dynamics and offer potential normalising operations for an equilibrium of power between entities that are crucial to the relationships at hand. The health of an ecosystem is tightly linked to what it offers to its customer base, leading to a reputation that could be terribly damaged if these customers, third-parties, or partners retaliate. Despite the outlining of potential withdrawal, the fact remains that it is challenging to actually step out of these powerful ecosystems and their services/products due to a lack of other competitors that can match the level of value and quality offered by the GAFA.

From a research perspective, the contribution lies in understanding how these relationships take place through an initial analysis of power exercise, eventually translated in power-changing operations to balance out power between entities. Additionally, an interpretation of potential impact on the overall health of each one of the ecosystems in question was presented. The understanding outlines the consequences of privacy breaches on the elements involved in it, either positively or negatively, as well as potential strategies that could protect crucial factors within the ecosystem and its many elements.

From a practical perspective, the contribution lies in offering a non-technical, non-trivial understanding of privacy breach cases having implications beyond the mere exposure of personal data. These relationships have an underlying impact on one another, and could potentially carve havoc throughout the ecosystems from a financial, technical, or even social perspective. By projecting these consequences beyond the context of software development, the need to protect users' data and privacy can be comprehended from the sociological perspective of power.

6.2 Threats to Validity

1. *Internal validity*

Despite the investigative process required to conduct this research, it is known that any information regarding these privacy breaches are primarily collected through the articles reported by selected publications along with their presented evidence. These reports are susceptible to the publication author's personal impressions and opinions. Therefore, regardless of how informative these journalistic pieces are, additional undisclosed factors could also influence the analysis.

2. *Conclusion validity*

The results of this research were concluded through subjective analysis, which could inevitably sway the interpretation of different researchers. Perceptions of how power is exercised derived from researchers' interpretation based on their understanding of the subject matter and their theoretical background. Additionally, the selection of a restricted number of cases for this study (only four, as presented in chapter 4) describes the power exercise models in very specific scenarios, whereas other cases could potentially lead to different types of power being exercised among various entities and actors, and the outcome of these cases could also differ.

6.3 Future Work

As a continuation of this research, the following topics are proposed for future studies:

1. *Explore different sources*

As reinforced earlier in the chapter (section 6.1), the information used to conduct the analysis of these cases were primarily extracted from the articles that made through the final selection, meaning the argumentative foundation relied on what was reported by the authors of each of those publications. To enrich the discussion, and subsequently, the arguments to justify the analysis, complementary (and trustworthy) information can be added, such as:

- Interviews with relevant people from each one of these ecosystems (CEOs, COOs, CFOs) to clarify and enhance the veracity of the facts, as well as to potentially question them directly;
- Interviews with other members involved within the ecosystem to understand the situation from a multitude of perspectives;
- Other media outlets (e.g. *videos*) reporting information on the case and overall situation surrounding the scandal;
- Research papers possibly addressing these cases.

2. ***Additional privacy breach investigations***

Another branch of this research could encompass studies exploring different cases, across different ecosystems with various configurations and operations. The goal lies in aiming to identify similar situations of privacy breach or lack of regulation compliance to try and detect patterns regarding lack of security/privacy concerns within these ecosystems.

3. ***GDPR and Requirements***

Lastly, another relevant study encompasses the translation of data protection regulations such as General Data Protection Regulation[1] into legal requirements to be applied across these ecosystems. The aim of guiding these ecosystems towards compliance with these regulations in light of the current demands regarding privacy engineering is a fundamental part of the software development process, and aims to prevent potential breach scandals in the future.

[1] "General Data Protection Regulation (GDPR) - Official Legal Text" - <https://gdpr-info.eu>

A Appendix

A.1 Data search queries

This appendix lists the queries used to collect the required data for this research as described in section 3.1.1 of chapter 3. Queries are grouped based on the respective companies in the search.

Google

- *privacy* + *scandal* + *Google* OR
- *privacy* + *breach* + *scandal* + *Google* OR
- *data* + *leak* + *scandal* + *Google* OR
- *data* + *leak* + *cases* + *Google*

Amazon

- *privacy* + *scandal* + *Amazon* OR
- *privacy* + *breach* + *scandal* + *Amazon* OR
- *data* + *leak* + *scandal* + *Amazon* OR
- *data* + *leak* + *cases* + *Amazon*

Facebook

- *privacy* + *scandal* + *Facebook* OR
- *privacy* + *breach* + *scandal* + *Facebook* OR
- *data* + *leak* + *scandal* + *Facebook* OR

- *data* + *leak* + *cases* + *Facebook* OR

Apple

- *privacy* + *scandal* + *Apple* OR
- *privacy* + *breach* + *scandal* + *Apple* OR
- *data* + *leak* + *scandal* + *Apple* OR
- *data* + *leak* + *cases* + *Apple*

Bibliography

Alves, C.; Valença, G.; Franch, X. Exercising power in software ecosystems. IEEE Software, v. 36, n. 3, p. 50–54, 2019. Cited 5 times on pages 12, 15, 16, 21, and 23.

BENJAMIN, G. Amazon Echo's privacy issues go way beyond voice recordings. The Conversation, 2020. Access date: July 29, 2020. Disponível em: <https://theconversation.com/amazon-echos-privacy-issues-go-way-beyond-voice-recordings-130016>. Cited 7 times on pages 25, 26, 27, 35, 36, 37, and 47.

Cavoukian, A.; Kursawe, K. Implementing privacy by design: The smart meter case. In: 2012 International Conference on Smart Grid (SGE). [S.l.: s.n.], 2012. p. 1–8. Cited on page 14.

EMERSON, R. M. Power-dependence relations. American Sociological Review, [American Sociological Association, Sage Publications, Inc.], v. 27, n. 1, p. 31–41, 1962. ISSN 00031224. Disponível em: <http://www.jstor.org/stable/2089716>. Cited 3 times on pages 10, 17, and 23.

FOWLER, G. Perspective | Alexa has been eavesdropping on you this whole time. WP Company, 2019. Access date: August 02, 2020. Disponível em: <https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/>. Cited 6 times on pages 26, 27, 35, 36, 37, and 42.

FRENCH, J.; RAVEN, B. The bases of social power. [S.l.: s.n.], 1959. v. 6. Cited 2 times on pages 15 and 16.

GASKI, J. F. Interrelations among a channel entity's power sources: Impact of the exercise of reward and coercion on expert, referent, and legitimate power sources. Journal of Marketing Research, v. 23, n. 1, p. 62–77, 1986. Disponível em: <https://doi.org/10.1177/002224378602300107>. Cited on page 17.

Gürses, S.; del Alamo, J. M. Privacy engineering: Shaping an emerging field of research and practice. IEEE Security Privacy, v. 14, n. 2, p. 40–46, 2016. Cited 2 times on pages 13 and 14.

HADAR, I. et al. Privacy by designers: Software developers' privacy mindset. In: Proceedings of the 40th International Conference on Software Engineering. New York, NY, USA: Association for Computing Machinery, 2018. (ICSE '18), p. 396. ISBN 9781450356381. Disponível em: <https://doi.org/10.1145/3180155.3182531>. Cited on page 14.

JANSEN, S.; FINKELSTEIN, A.; BRINKKEMPER, S. A sense of community: A research agenda for software ecosystems. In: IEEE. 2009 31st International Conference on Software Engineering-Companion Volume. [S.l.], 2009. p. 187–190. Cited on page 9.

LYNSKEY, D. 'Alexa, are you invading my privacy?' – the dark side of our voice assistants. Guardian News and Media, 2019. Access date: July 29, 2020. Disponível em: <https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants>. Cited 4 times on pages 25, 27, 36, and 48.

MANIKAS, K.; HANSEN, K. M. Software ecosystems – a systematic literature review. Journal of Systems and Software, v. 86, n. 5, p. 1294 – 1306, 2013. ISSN 0164-1212. Disponível em: <http://www.sciencedirect.com/science/article/pii/S016412121200338X>. Cited on page 11.

Martin, Y.; Kung, A. Methods and tools for gdpr compliance through privacy and data protection engineering. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). [S.l.: s.n.], 2018. p. 108–111. Cited on page 15.

MESSERSCHMITT, D. G.; SZYPERSKI, C. et al. Software ecosystem: understanding an indispensable technology and industry. MIT Press Books, The MIT press, v. 1, 2005. Cited on page 9.

MOORE, J. F. Predators and prey: a new ecology of competition. Harvard business review, SUBSCRIBER SERVICE, PO BOX 52623, BOULDER, CO 80322-2623, v. 71, n. 3, p. 75–86, 1993. Cited on page 10.

NAMBISAN, S.; SIEGEL, D.; KENNEY, M. On open innovation, platforms, and entrepreneurship. Strategic Entrepreneurship Journal, v. 12, n. 3, p. 354–368, 2018. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sej.1300>. Cited on page 11.

O'REILLY, L. Ad tech isn't dying: children-focused ad platform SuperAwesome raises $17m. 2020. Disponível em: <https://digiday.com/media/ad-tech-isnt-dying-children-focused-ad-platform-superawesome-raises-17m/>. Cited on page 47.

PARKER, G. G.; ALSTYNE, M. W. V.; CHOUDARY, S. P. Platform revolution: How networked markets are transforming the economy and how to make them work for you. [S.l.]: WW Norton & Company, 2016. Cited on page 9.

PRICE, R. Instagram's lax privacy practices let a trusted partner track millions of users' physical locations, secretly save their stories, and flout its rules. Business Insider, 2019. Access date: July 29, 2020. Disponível em: <https://www.businessinsider.com/startup-hyp3r-saving-instagram-users-stories-tracking-locations-2019-8>. Cited 8 times on pages 27, 28, 29, 38, 39, 40, 49, and 50.

SCACCHI, W.; ALSPAUGH, T. A. Securing software ecosystem architectures: Challenges and opportunities. IEEE Software, IEEE, v. 36, n. 3, p. 33–38, 2018. Cited on page 9.

SINGER, N.; CONGER, K. Google Is Fined $170 Million for Violating Children's Privacy on YouTube. The New York Times, 2019. Access date: August 10, 2020. Disponível em: <https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html>. Cited 7 times on pages 24, 25, 32, 33, 34, 46, and 47.

SPIEKERMANN, S. The challenges of privacy by design. Communications of The ACM - CACM, v. 55, p. 38–40, 07 2012. Cited on page 15.

SU, J. Apple Apologizes For Eavesdropping On Customers, Keeping Siri Recordings Without Permission. Forbes Magazine, 2019. Access date: August 05, 2020. Disponível em: <https://www.forbes.com/sites/jeanbaptiste/2019/08/28/apple-apologizes-for-eavesdropping-on-customers-keeping-siri-recordings-without-permission/>. Cited 5 times on pages 30, 31, 43, 44, and 51.

SU, J. Confirmed: Apple Caught In Siri Privacy Scandal, Let Contractors Listen To Private Voice Recordings. Forbes Magazine, 2019. Access date: July 25, 2020. Disponível em: <https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/>. Cited 7 times on pages 30, 31, 42, 43, 44, 50, and 51.

VALENÇA, G.; ALVES, C. A theory of power in emerging software ecosystems formed by small-to-medium enterprises. Journal of Systems and Software, Elsevier, v. 134, p. 76–104, 2017. Cited on page 10.

VALENCA, G. et al. On the benefits of corporate hackathons for software ecosystems – a systematic mapping study. In: . [S.l.: s.n.], 2019. p. 367–382. ISBN 978-3-030-35332-2. Cited 2 times on pages 11 and 13.

VALENçA, G.; ALVES, C. A theory of power in emerging software ecosystems formed by small-to-medium enterprises. Journal of Systems and Software, v. 134, p. 76 – 104, 2017. ISSN 0164-1212. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0164121217301863>. Cited 10 times on pages 7, 10, 11, 12, 13, 16, 17, 18, 21, and 22.

VALENçA, G. et al. Competition and collaboration in requirements engineering: A case study of an emerging software ecosystem. In: . [S.l.: s.n.], 2014. p. 384–393. Cited on page 18.

VALENçA, G.; ALVES, C.; JANSEN, S. Strategies for managing power relationships in software ecosystems. Journal of Systems and Software, v. 144, p. 478 – 500, 2018. ISSN 0164-1212. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0164121218301468>. Cited 4 times on pages 15, 16, 17, and 23.

WRONG, D. Power: Its forms, bases and uses. [S.l.]: Transaction, 1980. Cited on page 16.

YIN, R. Case Study Research: Design and Methods. SAGE Publications, 2013. ISBN 9781483322247. Disponível em: <https://books.google.com.br/books?id=OgyqBAAAQBAJ>. Cited on page 19.

ZACHARY, W.; ROBERT, M. Supply chain relationships and information capabilities: The creation and use of information power. International Journal of Physical Distribution & Logistics Management, Emerald Group Publishing Limited, v. 37, n. 6, p. 469–483, Jan 2007. ISSN 0960-0035. Disponível em: <https://doi.org/10.1108/09600030710763387>. Cited on page 16.