LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Privacy by Design

A qualitative study to explore privacy by design adaptation in reducing privacy breaches

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Esther Nampiina
Mandukhai Lkhagvasuren
Arman Madjidian

Supervisor: Miranda Kajtazi

Correcting Teachers: Bo Andersson
Blerim Emruli

Privacy by Design: A qualitative study to explore privacy by design adaptation in reducing privacy breaches

AUTHORS: Esther Nampiina, Mandukhai Lkhagvasuren & Arman Madjidian

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June, 2020

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Christina Keller, Professor

NUMBER OF PAGES: 170

KEY WORDS: Privacy by Design, Data Privacy, GDPR

ABSTRACT (MAX. 200 WORDS):

Privacy by Design is a methodology that enables privacy to be built into the design and architecture of information systems and business processes. Rather than bolting on protection at the end of a design process, care for privacy needs to be one of the foundational concerns of any implementation. Traditionally, privacy policies have been largely approached reactively, and only triggered once a breach occurs. However, to comply with new privacy data protection laws, companies are now obliged to implement the principles of *PbD* and take data privacy into the account during the design stage of all projects. Therefore, this study aims to explore the practices that have been adopted by companies to implement *PbD*. To achieve this aim, empirical data from semi-structured interviews conducted with UI/UX designers worldwide were analysed and insightful findings were found. Overall, the concept of *PbD* is a relatively unknown concept among most respondents. Several companies have adopted practices in accordance with the principle of data minimization, and the principle of visibility and transparency.

Content

Figures

Tables

Acknowledgement

First, we would like to thank our supervisor Miranda Kajtazi for her continuous guidance and invaluable feedback.

We wish to thank all the respondents who were engaged in our study without whose generous support, we would not have been able to complete this report.

We would also like to thank our families for all their love and support.

Arman Madjidian Esther Nampiina Mandukhai Lkhagvasuren

1 Introduction

1.1 Background

Recently, there has been an observable paradigm shift regarding privacy protection as the introduction of new privacy laws such as the *General Data Protection Regulation* (GDPR) and the *California Consumer Privacy Act* (CCPA) are changing the way data is handled (Cusick, 2018). These privacy laws demand more proactive board oversight to protect categories of previously unregulated information that organizations routinely collect and store (Cusick, 2018). Privacy by Design (*PbD*) calls for privacy to be taken into account in the early stages of product development (Cavoukian & Dixon, 2013). A noteworthy definition of the phenomenon *Privacy by Design* is given by Campisi who states that: "The principle of '*Privacy by Design'* means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use, and ultimate disposal" (2013, p.364). Product development is broadly described as stages involved in bringing a product to retirement through phases: requirements definition, design implementation, production maintenance, and retirement (Li & Unger, 2012). For this study, the term disposal is used to refer to retirement.

The idea of *PbD* is hereby that privacy-protecting compliance becomes an integral component of an organization's processes and technologies, rather than something that is imposed and reviewed for compliance afterward (Campisi, 2013; Cavoukian, Taylor & Abrams, 2010, p. 408). Thereby, *PbD* offers an opportunity to prevent privacy breaches from occurring, rather than just providing remedies for resolving them (Campisi, 2013). As shown in *Verizon's 2019 Data Breach Investigations Report*, more than 2,013 data breaches were reported in 2019, averaging a data breach in every four hours. Seemingly, no organization is too large or too small to fall victim to a data breach, and regardless of what measures are put in place by security professionals, attackers can circumvent them (Verizon, 2019). A global survey found that more than 88 percent of people are concerned about who has access to their data and how it is being used; over 80 percent expect government authorities to regulate privacy and impose penalties on organizations that fail to use data responsibly (Spiekermann, 2012). Therefore, providers of technological solutions need to estimate customers' value for protecting their personal data and suggest "privacy-enhancing" initiatives as a competitive advantage to shield their business strategy (Alessandro, Leslie & George, 2013, p.249; Redman & Waitman, 2020).

Spiekermann (2012) describes the unpredictable nature of data and compares it to water, as it flows and ripples in ways that are hard to predict. In addition to the unpredictableness of data, technology is constantly changing (Spiekermann, 2012). The countless marks of science pervade our world and they are constantly altering the fabric of our society (Cavoukian, 2006; Spiekermann, 2012). The rapid pace at which technologies such as artificial intelligence (AI) and automation are developing, is continuously transforming the systems that we take for granted today, generating new profound challenges for information privacy in the process (Cavoukian, 2006). As a result, even a well-conceived privacy regulation such as the General Data Protection Regulation (GDPR) struggles to ensure its effectiveness (Eagan, 2019). Designed to give power back to consumers, the GDPR has been championed as the one weapon that can restore our human right to privacy (Cusick, 2018). Yet, companies continue to regularly test the boundaries of such regulations, and many even risk sanctions for privacy breaches only to avoid constraining their business (Rubens, 2019). Against this background,

regulatory bodies are in search of a more effective balance between the privacy rights of citizens and the data needs of companies and governments (Cusick, 2018; Hustinx, 2010; Spiekermann, 2012). According to Spiekermann (2012), the apparent solution proposed by regulators is the concept of *PbD*. Privacy from a design perspective was first introduced in a joint article between the Dutch Data Protection Authority and the Ontario Information Commissioner in 1995 (Hustinx, 2010). The article demonstrates the technologies and components that could improve privacy in product development (Hustinx, 2010). Two deputy commissioners — Dr. John Borking and Dr. Ann Cavoukian—played a key role in this project (Hustinx, 2010). However, believing that companies would try to solve their privacy issues simply by adding these components to existing systems, Ann Cavoukian further developed the concept by introducing *PbD* and its seven foundational principles (Danezis et al., 2015).

The rules of the game are changing; cybercriminals are breaking into government agencies and companies daily and unless something fundamentally changes, such incidents are going to continue (Oetzel & Spiekermann, 2012). Regulations such as the GDPR and the CCPA have placed the subject of privacy and *PbD* at top of the agenda (Cusick, 2018). The approach of *PbD* indicates that privacy should be a proactively paramount consideration at the design stage of system development (Cavoukian & Dixon, 2013). However, the interpretation of privacy and the measures required to prevent privacy breaches is still very much up to the organizations themselves (van Rest, Boonstra, Everts, van Rijn & van Paassen, 2012). In order to be able to prevent further privacy breaches, what is needed now are more innovative methods that assure that personal information is in fact being managed responsibility by data holders (Cavoukian, Taylor & Abrams, 2010, p.406). Typically, the paths to enhanced assurance and accountability involve a combination of law and regulation, and technologies, practices, and policies. Therefore, a comprehensive and proactive *PbD* approach is more important than ever, one which assures responsibility right from the very start (Cavoukian et al., 2010).

1.2 Problem

In modern times, organizations typically audit data access and use rather than enforcing protection policies (Cavoukian, 2011; Cavoukian & Dixon, 2013). As a result, security teams end up spending most of their energy identifying data breaches and cleaning up after incidents (Cavoukian & Dixon, 2013). In September 2017, personally identifying data of hundreds of millions of people were stolen from Equifax, one of three major credit reporting agencies that assess the financial health of nearly everyone in the United States (Smith & Mulrain, 2017). The audit report concluded, among other things, that Equifax had adopted a reactive approach towards privacy (Portman & Carper, 2017). As history has shown many times before, reacting in a responsive way towards privacy-invasive events not only damages the reputation of an organization, but ruins live as well (Cavoukian & Dixon, 2013; Smith & Mulrain, 2017). Traditionally, privacy policies have been largely approached reactively, and only triggered once a privacy breach occurs (Cavoukian & Dixon, 2013). In this age of massive social media and data collection, we are no longer able to protect privacy with a reactive model alone (Cavoukian & Dixon, 2013). As stated earlier, *PbD* consists of seven principles that can be applied from the onset of system development to mitigate privacy concerns and achieve data protection compliance (Gürses, Troncoso & Diaz, 2011).

Although several researchers are suggesting proactive privacy measures concerning system development, the proactive practices which entail *PbD* are not discussed (Lee, Cho & Lim, 2018; Xu, Dinev, Smith & Hart, 2011). Furthermore, in an extensive literature review

conducted by Kurtz, Semmann & Böhmann (2018), the authors found that no further conceptual development has taken place since the initial publication of the *PbD* framework in 1995 and the establishment of its principles in 2009. In view of this, the principles of *PbD* are often criticized for being vague, therefore, its application in system development is left unclear (van Rest et al., 2012). According to van Rest et al. (2012) the specific meaning in a particular application domain of the principles of *PbD* is unknown, and what citizens and consumers actually need to know about *PbD* for it to "work" has remained an open question (van Rest et al., 2012). It is also not known what the consequences of adopting *PbD* are, what relevant best practices are, or which methodologies are available (van Rest et al., 2012).

Legislation such as the GDPR makes extensive reference to "*PbD*", without necessarily specifying exactly what it means (Kurtz, Semmann & Böhmann, 2018; van Rest et al., 2012). Furthermore, as stated by van Rest et al. (2012), there is no market mechanism favouring *PbD* as citizens tend not to flock to services that better protect their privacy. With these arguments at hand, it may be argued that *PbD* still lags in becoming a priority even for regulations such as the GDPR and the CCPA, which have partly adopted the principles of the framework (Blix, Elshekeil & Laoyookhong, 2018). However, in accordance with the GDPR, organizations are required to adopt the principles of *PbD* and implement the correct security measures to stay compliant with these regulations (GDPR, 2020). However, because of the vagueness of the framework, *PbD* has been left open to interpretation and it is up to each organization to implement its principles as effectively as possible (Blix et al., 2018; van Rest et al., 2012). This paper aims to study the theoretical foundations of *PbD* and compare it with how the system and product designers work with privacy in practice.

1.3 Purpose

The main purpose of this paper is to use our empirical data, based on several qualitative interviews to study design practitioners' and developer's awareness and understanding of *PbD*, as well as their ability to realize its principles in agreement with new laws and regulations.

Design practitioners are among those who are responsible for embedding user privacy when developing a system. Therefore, User Experience (UX) designers and User Interface (UI) designers are targeted as the main source of our study. The contribution of knowledge in this study is to increase the awareness of *PbD* in the information systems discipline, as its principles should be implemented under the requirements of new regulatory frameworks

1.4 Research Question

In regard to the identified and delimited problem area, the following research question was generated:

RQ: *What practices do companies adopt to implement Privacy by Design?*

1.5 Delimitations

The focus of our research is to explore the various design practices adopted by UX/UI designers. The foundational principles of *PbD* are used as guidelines during the empirical study. This study will not involve privacy breaches related to the invasion of personal space, for instance by using surveillance cameras.

Designers approach problems from a different, often opposing perspective than what lawmakers or engineers do. A designer's vision is often based on user research, data intuition, and design process. The intended audience is quite narrow: UX designers and UI designers. In our research, interviews with policymakers, legal, engineers, and sociological scientist were not concluded. Although they are very much part of product development, we had to delimit ourselves to the most relevant parts of our research question in order to go deep into each topic.

UX design dictates the relationship and the experience that a user has as they interact with every aspect of a company's product or service (Schrage, 2016). UI design is a series of screens, pages, and visual elements that help users utilize the product or service (Galitz, 2007). Furthermore, the value of user experience among companies (Schrage, 2016) and the design of a user interface system has a profound impact on behaviour and decision making (Benartzi & Bhargava, 2020; Bhargava, Conell-Price, Mason & Benartzi, 2018; Galitz, 2007).

2 Theoretical Background

This chapter will act as a frame of reference for this thesis. First, relevant concepts and prior research are presented. Second, a thorough analysis and a critical review of Privacy by Design (PbD), which is the theoretical framework guiding this thesis.

2.1 Data Privacy

The term data privacy is used to refer to "*an expanding subfield of data management whose goal is to answer queries over sensitive datasets without compromising the privacy of individuals whose records are contained in these databases"* (Kifer & Machanavajjhala, 2011, p.193).

Although data privacy and data security are closely interconnected, they are not the same (Culnan, 2019). The distinctions between the two are fundamental to understand how they complement each other. Essentially, data security entails keeping personal data safe whereas privacy involves ensuring that data is accessed only when one has access rights to the data (Culnan, 2019).

Privacy can be described as a broad and subjective concept (Wunderlich, Veit & Sarker, 2019), and its meaning often depends on context scope (van Rest et al., 2012). Privacy of personal data and certifying that the collected data is invulnerable to a privacy breach is among the main concerns related to data collection (Fuller, 2019). This is due to the interactions between humans and robots which require constant collection and processing of personal data jeopardizing the personal data privacy of users (Bednar, Spiekermann & Langheinrich, 2019). Subsequently, guaranteeing data privacy regarding new complex technologies, data analytics, advertising based on behavioural patterns and cumulative use of IoT devices is not self-evident (Cavoukian & Chibba, 2018; Chanson, Bogner, Bilgeri, Fleisch & Wortmann, 2019; Culnan, 2019). Meanwhile, encrypted data content based on an accessed address sequence can be affected by malicious servers (Yang, Zheng, Zhou, Jin & Wang, 2019). Through this, data subjects are commonly unaware of which part of their data is being mined and yet techniques used to collect data to obtain business insights are vulnerable to a privacy breach (Abbasi, Sarker & Chiang, 2016; Acquisti, Brandimarte & Loewenstein, 2015; Schaar, 2010). Therefore, with less knowledge about the quantity of information to share (Acquisti et al., 2015). A study conducted by Wunderlich et al. (2019) showed that privacy is among the factors that affect the embracement of sustainable technologies. Similarly, the use of retail store cards, smartphones recording geographical location, online purchases, social media, and other activities that involve the use of the internet can lead to profiling an individual without their consent (Fuller, 2019). Since the relationship between companies and customers is not transparent, impacting negatively on privacy, organizations can easily face privacy disasters in case they use customer data in publicly unacceptable ways (Culnan, 2019). Furthermore, the incapability to safeguard data procession protection is entirely held accountable to a company (GDPR, 2020).

According to research conducted by Li and Unger (2012), it is assumed that quality and privacy are inversely proportional to each other. Nevertheless, consumers who demand highly personalized quality have concerns about the privacy of their personal data since an acceptable

quality of service requires them to provide a certain amount of information about themselves (Culnan, 2019). Moreover, it is very unlikely for consumers to completely comprehend how their data is utilized and shared with third parties by various organizations extending the role to protect their data to the organizations (Culnan, 2019). In a parallel argument, organizations can avoid privacy catastrophes using formal policies that encourage notifying data subjects about how their data is used (Culnan, 2019)**.** Whereby the skills needed to address data privacy invasion include privacy engineering for system development (Culnan, 2019). Deploying a privacy program that clearly defines formal processes and principles to aid strategic data governance is therefore important (Culnan, 2019).

2.2 Privacy by Design

According to Spiekermann (2012), the idea of data protection by design has been around for decades and a great deal of work has been conducted in this area under the term PbD. Furthermore, as a result of recent discoveries of inappropriate use of personal data, the public debate on data protection has been driven to an unprecedented level. Campisi (2013) argues that privacy ought to be addressed from a design thinking perspective, where privacy is embedded in networked data systems and products by default. The author further points out that the main purpose of *PbD* is to optimize privacy and data protection by embedding safeguards across the design and developments of products by taking privacy considerations into account throughout the whole engineering process, rather than as a remedial afterthought. This inspired her to develop the universal framework known as *PbD.* According to Gürses et al. (2011), the principles of *PbD* serve as a guideline for adjusting design and implementing privacy requirements with complex social, legal, and ethical concerns.

PbD was broadly acknowledged by international data protection commissioners in 2010 during an annual conference as fundamental in privacy protection and to aid in the prevention of privacy-invasive events (Cavoukian, 2012). The adoption of *PbD* does not only augment trust between a company and its customers but postulates a competitive advantage as well (Cavoukian, 2009; Cavoukian, 2020). Mainly because trust deficiency affects the adoption of certain technologies, such as digital technologies and IoT (Chanson et al., 2019; Spiekermann, 2012; Wunderlich et al., 2019). Against this background, the certainty that various new technologies improve the quality of our lives (Bednar et al., 2019), motivates the aim of *PbD* to address privacy throughout the whole product development process (Cavoukian, 2009; Cavoukian & Chibba, 2018). Moreover, "*PbD* is adjuvant for all kinds of IT systems designated or used for the processing of personal data (Schaar, 2010). In other words, the *PbD* principle advocates embracing the cumulative benefits conveyed through novel technologies such as data analytics and dealing with privacy before any privacy breaches occur (Cavoukian & Chibba, 2018).

Making privacy the default mode of design and operation addresses the privacy risk management expectations that data subjects believe are to be handled by the data collectors (Cavoukian & Chibba, 2018). One of the adopters of *PbD*, TELUS Communications Inc. in Canada decided to address the risks of privacy by implementing *PbD* which required them to customize the foundational principles to fit their business processes (Cavoukian, 2020). Likewise, Intel and General Electric (GE) successfully implemented *PbD* in healthcare technologies by applying the foundational principle of positive-sum (Cavoukian, 2020). These companies first identified the privacy considerations that needed to be addressed and designed

them directly into the system (Cavoukian, 2020). Furthermore, *PbD* is not only focused on IT, organizational practices, and processes but also in principles that can be used to guide the design of privacy (Cavoukian, 2012).

2.2.1 Foundational Principles of Privacy by Design

The seven foundational principles that were formulated to aid the prevention of privacy-invasive events are presented below (Cavoukian, 2009):

Proactive, **not Reactive**. *PbD* aims at addressing privacy before the occurrence of any privacy-invasive events (Cavoukian, 2009). This principle encourages the use of proactive measures to prevent privacy breaches from occurring not abusing opportunities but seeking consent (Cavoukian, 2009). *PbD* applies to information technologies solutions of any context of organizations therefore it requires commitment from all stakeholders of the company ecosystem. Having a well-trained privacy practitioner is also part of it. Moreover, a *PbD* approach requires a systematic, innovative, and preventive nature from the practice execution to mitigate the risk of a disqualified attempt (Cavoukian, 2009).

Privacy as the Default. This principle aims at ensuring that privacy is inbuilt in a system without the data subject initiating the privacy request (Cavoukian, 2009). In other words, privacy should be built into products before adding features that enable data sharing (Cavoukian, 2009). Through this, companies should start by ensuring data minimization. Essentially, it means the maximum privacy protection should be provided to consumers as a baseline. More specifically, it is informed by the following factors.

- Purpose Specification - Before collecting data, the purposes for which they are processed must be communicated to the data subject (Cavoukian, 2009).
- Collection Limitation - Collection limitations refer to limiting data collection to only what is required to fulfil a specific purpose and for reasons that were clearly stated in advance (Cavoukian, 2009).
- Data Minimization - Data minimization is a principle that refers to measures performed by an organization to limit the collection of personal data (Cavoukian, 2009). Additionally, the data must be limited to what is essential concerning the purposes for which they are processed. It also involves minimizing the identifiability and linkability of personal information (Cavoukian, 2009).
- Use, retention, and disclosure limitation - An organization should limit the ways it uses, discloses, and retain personal information (Cavoukian, 2009). Personal information should not be used for purposes beyond what was communicated before the collection of data and received consent (Cavoukian, 2009).

Privacy Embedded in the Design. This principle translates to the incorporation of privacy into the design, the architecture of IT systems, and business processes (Cavoukian, 2009). Privacy considerations should be holistically embedded in the design, and not bolted on as an add on (Cavoukian, 2009). Cavoukian (2009) presents three key elements to successfully embed privacy in the design. First, privacy should be addressed systematically following accepted standards and frameworks, which are amenable to external audits. Secondly, whenever possible, detailed risk assessments should be performed, documenting, and publishing identified risks as well as the measures taken to mitigate them. Finally, technology or system should have a minimized impact on privacy, and not degraded through use or errors.

Full functionality - Positive-Sum, not Zero-Sum. The full functionality principle aims at encouraging a balance between privacy and other fundamental requirements of a product without any trade-off (Cavoukian, 2009). The concept of *PbD* challenges the fact that privacy should compete with other legitimate interests such as design or technical opportunities. Instead, *PbD* advocates creativity and innovation as tools to achieve full functionality along with the highest level of privacy.

End to End Security. Privacy protection follows data, wherever it goes (Cavoukian, 2020). This foundational principle serves as a guide to protect personal data throughout its lifecycle and taking full responsibility for the data even when third parties are involved (Cavoukian, 2009). Entities must assume responsibility for data throughout its entire lifecycle under certain accepted standards. Furthermore, to achieve an end to end security, Cavoukian (2009) promotes the use of secure data destruction, appropriate encryption, and strong access control and logging.

Visibility and Transparency. This principle means ensuring transparency by clarifying to all involved stakeholders that regardless of all business practices and technology involved, an operation is based on the mentioned objectives which involve privacy verification (Cavoukian, 2009). This principle employs openness, accountability, and compliance with Fair Information Practices as elaborated below (Cavoukian, 2009).

- Accountability – The process of collecting personal information is followed by a duty to protect the information.
- Openness - The management of personal information and its related practices shall be made available to individuals
- Compliance - Mechanism that ensures that these policies are evaluated and followed should be established. Complain and redress mechanisms should be established as well.

Respect for User Privacy. *PbD* looks at designing human-machine interfaces that are user-centric, human-centred, and user-friendly so that it is easy for the user to reliably make privacy decisions (Cavoukian, 2009). This principle refers to the fact that the user should always be in focus and all decisions should be made with the users' best interest in mind. Cavoukian (2009) suggests practices below to meet the respect for user privacy principle:

- Consent – Before collecting or processing any data, the individuals' consent is required. Furthermore, the individual has a right to withdraw their consent at any time.
- Accuracy – Data holders must ensure that all personal information is accurate, up to date, and not misleading.
- Access - An individual shall be given access to their personal information and informed of its uses. An individual may also request the correction of that information
- Compliance – Compliant and redress mechanisms should be established.

The diagram below (Figure 1) is developed by a critical analysis of the foundational principles of *PbD*. Based on the discussion above highlighting the need for business practice, commitment, leadership protection, and user-centricity, *PbD* can visually be described as seen below.

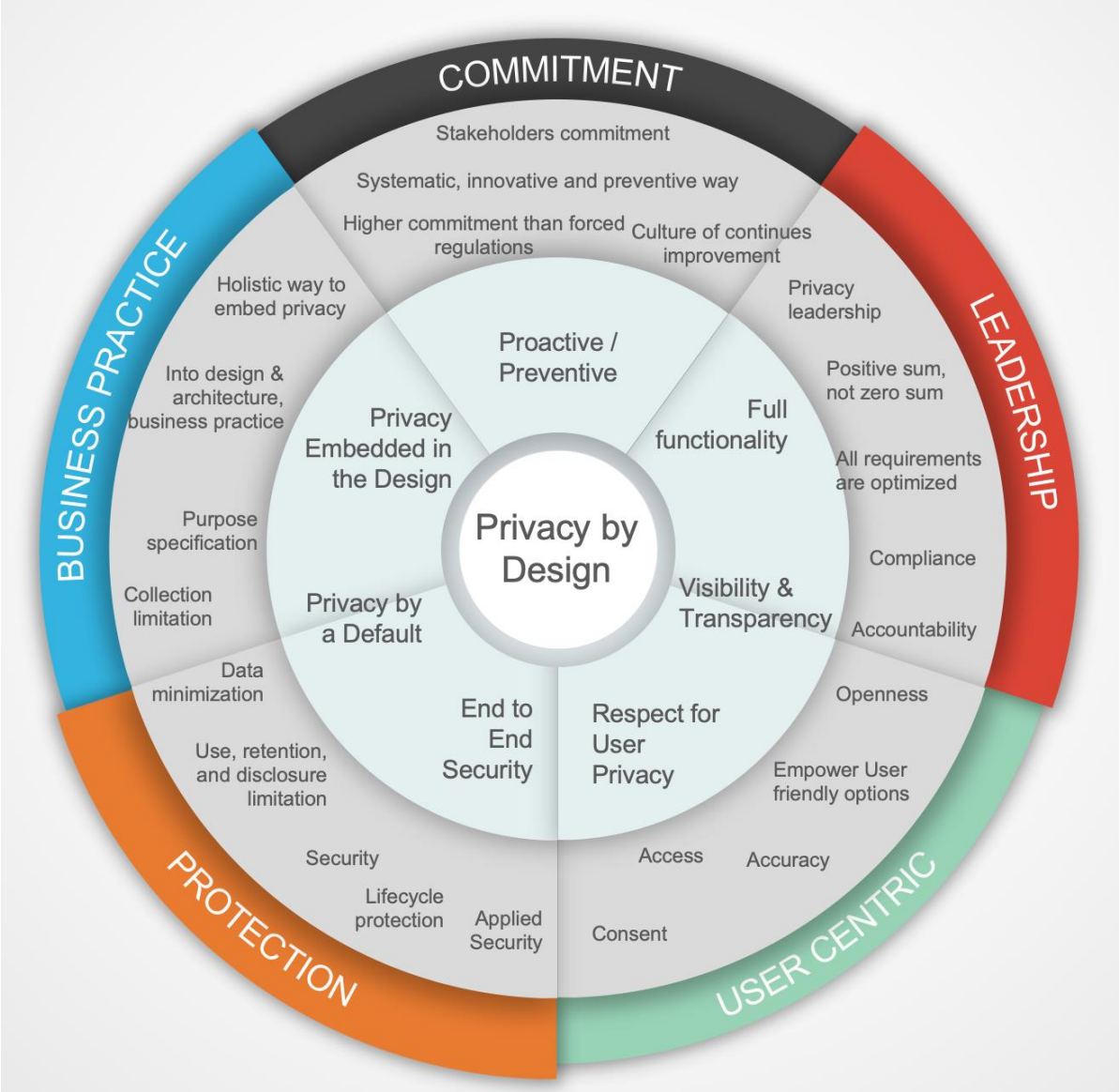

Figure 1: Full reflection of Privacy by Design developed by Authors

The above concept of privacy principles is widely favoured by policymakers and applied to the trilogy of accountable business practices, IT systems as well as physical design and networked infrastructure (Gürses et al., 2011). From a broader perspective, the *PbD* principles should guide data controllers and system designers to consider data privacy as an obligation at the beginning of the system development phase (Schaar, 2010). However, from the perspective of a system developer, it is not clear how to translate *PbD* into system development (Gürses et al., 2011). Although widely accepted as a game-changer to privacy protection, *PbD* has developed a reputation for being difficult to implement for businesses (Cavoukian, 2020). To successfully implement *PbD*, Cavoukian (2020) advises conducting training proactively, contextualizing its principles for them to be able to suit the needs of an organization, and to work collaboratively in teams on challenging data projects. Furthermore, Spiekermann argues that "*PbD* requires the guts and ingenuity of engineers" (2012, p.39). This might be a solid argument as to why *PbD* is still not popular in engineering design practices.

2.2.2 Impact of technologies on privacy

Internet of Things is a concept used to describe the connection of different devices through the use of the internet (Anscombe et al., 2017; Jandl et al., 2019). According to Wang et al. (2019) users lose control of the privacy of their data when there is a need to transfer data between devices and remote datacenter servers. This leads to Anscombe et al. (2017) suggestion that there should be a privacy policy that governs the development of such technologies, policies that require transparency between the data holder and the data subject. Due to the privacy issues associated with IoT, Jandl et al. (2019) suggest the use of *PbD* as an effective approach to address privacy in IoT.

Advertising based on behavioral patterns is another concept that has led to several discussions within the subject of privacy. Mandal, Mitchell, Montgomery and Roy (2017) point out that targeted online advertising is characterized by massive collection and transfer of data which leads to privacy concerns. Predicting behavior based on online activity is a powerful tool used by companies to market products based on a built behavior profile (Kagan & Bekkerman, 2018). However, privacy concerns arise due to the sensitive nature of the collected data. According to Mandal et al. (2017), although personal data is often anonymized, due to large volumes of collected data it could lead to privacy breaches.

Data analytics
In this section, data analytics will be explained concerning personal data used in a corporate context with analytics addressing future outcomes based on historical data (Davenport, Harris & Morison, 2010). Moreover, given its sensitive nature, personal data itself is vulnerable to being collected, analysed, and abused through privacy breaches (Abbasi et al., 2016; Acquisti et al., 2015; Schaar, 2010). Companies consider data analytics a tool for success; therefore, they implement an "all you can collect" strategy (Davenport et al., 2010). However, this approach generates new challenges for companies as it becomes harder to implement the correct security measures to protect an abundance of data against potential privacy breaches (Davenport et al., 2010; Sun, Song, Jara & Bie, 2016).

2.3 Data Security

Data security refers to the protective measures of securing data from accidental or intentional but unauthorized disclosure or modification throughout the data lifecycle (Buckbee, 2020).

Information is widely considered as the lifeblood of modern business (Calder & Watkins, 2008). However, data security has consistently been a major issue in IT as a loss of data can have a severe impact on the business, brand, and trust of an organization (Rao & Selvamani, 2015). To such intellectual capital, organizations are facing a flood of threats from sophisticated hackers and viruses (Calder & Watkins, 2008). Additionally, as people have become more aware of their privacy rights, organizations are required to meet customers increasingly complex demands regarding data protection and privacy regulations as well (Calder & Watkins, 2008).

The core elements of data security are confidentiality, integrity, and availability (Buckbee, 2020). Also known as the *CIA triad*, this is a security model designed to guide policies for information security within an organization (Buckbee, 2020). Samonas and Coss (2014) suggest that *confidentiality* implies the notion that data must be protected; in such a way that

its use is confined to authorized people only. The *integrity* of information involves maintaining and assuring the accuracy and completeness of data over its entire lifecycle. Moreover, data should not be changed in transit, and measures need to be taken to ensure that data cannot be altered by unauthorized people (Samonas & Coss, 2014). The *availability* of information ensures that authorized parties can access the data when needed (Samonas & Coss, 2014). Together, known as the holy trinity of data security, they form the most popular reference model for information security and information assurance needed (Samonas & Coss, 2014). While the CIA triad must be rigorously implemented to provide for the information assurance needs of a network, depending upon the context or the environment, one of these principles might be more important than the others (Samonas & Coss, 2014). However, as all vulnerabilities and risks are measured for their potential capability to compromise one or all of the principles, the triad as a whole is the basis for creating a holistic security plan to protect the assets of your organization needed (Samonas & Coss, 2014).

According to Calder and Watkins (2008), unless organizations adopt a comprehensive systematic approach to protecting these elements, they will be vulnerable to a wide range of possible threats. However, although many information security practitioners consider the CIA triad as the foundation of information security, its relevance is frequently questioned by scholars (Samonas & Coss, 2014). Moreover, academic research suggests several extensions to the original CIA triad as they question its capacity to address the extent of socio-technical issues that have emerged in security in recent times, such as big data and IoT (Samonas & Coss, 2014). Nevertheless, Samonas and Coss (2014) advocate the view that the CIA triad will continue to assume a key role in information security, not because practitioners have rejected the improvements proposed by security scholars, but because these improvements can be accommodated by a more extensive re-conceptualization of the original CIA triad. Having said that, there are of course other security models in the world of information security as well, such as the Parkerian Hexad which is often seen as an extension of the CIA triad, or Stride, a model of threats used in the Microsoft Security Development Lifecycle (SDL) (Pender-Bey, 2016; Potter, 2009).

2.3.1 Regulatory Frameworks

On September 22, 2016, Yahoo! Inc. announced it had been victim to a state-sponsored data breach in 2014 which had stolen personal information from at least 500 million user accounts (Wang & Park, 2017). At the time it was announced, the theft represented the biggest known intrusion of one company's network (Wang & Park, 2017). However, the record would only later be surpassed by another Yahoo breach, in an incident that exposed over three billion accounts — every Yahoo account that existed at the time (Wang & Park, 2017).

The highly profitable aspect of processing personal information combined with the low penalties for privacy violations has led to circumstances where protection of privacy is not often considered a priority (Rubens, 2019). To successfully address the many challenges of data security, organizations should prioritize the security of the personal information that it holds and implement reasonable security measures to protect that information (Rubens, 2019). The new millennia brought a tsunami of personal data breaches, and Yahoo is only one among many organizations that have had to succumb to the increased number of malware threats (Verizon, 2019). Along with an influx of massive amounts of personal data, these threats have fuelled the need for new privacy laws.

General Data Protection Regulation

In response to these issues, the European Union drafted the GDPR, a new set of comprehensive regulations designed to strengthen data protection and to give power back to consumers (Cusick, 2018). As the successor of the *Data Protection Act* (DPA), GDPR was enforced in May 2018 and permanently changed the way you, as an organization collects and uses customer data (Cusick, 2018).

The European privacy rules have changed significantly as the GDPR empowers consumers with control over their personal data (Gjermundrød, Dionysiou & Costa, 2016). The GDPR introduces new responsibilities that require organizations to integrate data protection into every aspect of their processing activities (Gjermundrød et al., 2016). For organizations operating in EU state members, compliance with GDPR is mandatory and requires significant restructuring of data processing routines conducted by enterprises to cope with the novel legal requirements (Gjermundrød et al., 2016; Kurtz, Semmann & Böhmann, 2018). Furthermore, without necessarily detailing how it can or should be applied, the GDPR embraces *PbD* as a way for organizations to operationalize these legal requirements (Cusick, 2018; Koops & Leenes, 2014; Kurtz & Semmann, 2018).

The Privacy by Design Provision in the GDPR

Article 25 of the GDPR is entitled "*Data protection by design and by default*" and communicates requirements for data privacy by design and data privacy by default. According to article 25, companies that process personal data are required to implement appropriate technical measures and safeguards that adhere to privacy principles such as purpose limitation and data minimization (GDPR, 2020). These need to be built into data processing systems by default. Although "*PbD*" is well described throughout the GDPR, it is not clear what the obligation to ensure *PbD* would entail in practice. There is no specific technical implementation and data protection by design is not elaborated in any detail. Unfortunately, the regulation merely scratches the surface of *PbD* (GDPR, 2020).

California Consumer Privacy Act

The US has long been notable for not having adopted an extensive privacy law (Camhi & Lyon, 2018). However, in 2020, America's most complete data privacy legislation was implemented to give consumers rights to control how businesses monetize their personal information (Camhi & Lyon, 2018). The privacy act is known as the CCPA and applies to virtually any business that stores a reasonable amount of data and which does business in California (Camhi & Lyon, 2018; de la Torre, 2018). The CCPA and its comprehensive approach to privacy protection are in many ways similar to the GDPR that the EU adopted in 2018 (Camhi & Lyon, 2018).

A company does not have to be located in California but is subject to the law if it collects personal data on that threshold of residents there (de la Torre, 2018). Moreover, although just a state law, given California prominent position in the global and digital economy, it has broad global ramifications. According to de la Torre (2018), businesses are subject to the CCPA if they meet the following requirements:

- Annual revenues of at least $25,000,000
- Possess the personal data of more than 50000 consumers or devices in California.
- Derives more than 50 percent of annual revenues from selling consumer's personal information

In an article published in 2017, Saraiva (2017) acknowledges the geographical limitations of the GDPR as it was implemented to protect citizens of the EU. The article further states that CCPA is a result of the reaching influence and the extended impact of the GDPR, which ultimately forced governments to shift priorities and make them more inclined to protect individual privacy. Similar to Article 25 of the GDPR, the CCPA also regulates what kind of data businesses may collect from their consumers (Camhi & Lyon, 2018; Saraiva, 2017). Section 1798. 100(b) of the CCPA states the following:

"business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used" (CCPA, 2020, n.p.).

2.3.2 Proactive versus Reactive Cybersecurity

Privacy breaches continue to make headlines around the world. Over the last few years, the number of malware threats has increased, and the idea of a sophisticated hacker is forcing security teams to stay ahead of the curve to protect their organizations (Oetzel & Spiekermann, 2012). In this era of data breaches, every organization should look at how security procedures can protect its assets and customer data. Organizations can choose to take a proactive approach to cybersecurity, which includes pre-emptively identifying security weaknesses and adding processes to identify threats before they occur, or a reactive approach, in which they respond to a security breach after they occur (Cavoukian & Dixon, 2013).

According to Cavoukian and Dixon (2013), cybersecurity evolved as a reactive endeavour. Historically, security approaches have centred around the detection of and reaction to threats that penetrate a system or a network (Cavoukian & Dixon, 2013). To this day, many businesses often fail to understand the value of their data and choose to approach data security in a very reactive way (Cavoukian & Dixon, 2013). The author further points out that many businesses make the mistake of relying on a reactive approach towards data security worrying that trying to anticipate attacks will be too expensive in the long run. This statement is further amplified by Cavoukian (2018) who not emphasizes the economic costs of a reactive approach, but the cost of losing trust as well. The author also acknowledges the costs associated with a proactive approach towards data security but refers to them only as a fraction of the cost that you incur when you have privacy infractions. Additionally, adopting a proactive strategy does not necessarily have to be a prohibitively expensive approach — it simply means allocating resources to prepare your business to prevent attacks earlier (Cavoukian, 2018). It may be argued, that only by adopting a proactive approach and by ensuring privacy and security throughout every phase of the data lifecycle are businesses able to protect themselves against the ever-evolving threat of a cyber-attack (Cavoukian, 2018).

2.4 Literature review: An IS perspective

In response to our review of data privacy and data security as two interplaying parts of what it entails to conduct privacy by design, the study focused on understanding how *PbD* has been particularly researched in the IS discipline.

Below, Table 1 presents the key references extracted from a basket of ten IS journals. Showing the key literature that has tackled *PbD* from various forms of theories such as

privacy paradox and privacy calculus (Pavlou, 2011), Communication Privacy Management (CPM) theory (Xu et al., 2011), personalization-privacy paradox, gratifications theory, and information boundary theory (Sutanto, Palma, Chuan-Hoo & Chee Wei, 2013), prevention motivation theory and analogical social norm theory (Lee, Cho & Lim, 2018) and information boundary theory (Karwatzki, Dytynko, Trenz & Veit, 2017). With important key elements identified, for instance, information systems research has mainly focused on describing and predicting theoretical contributions with minimal studies about design and action (Bélanger & Crossler, 2011). Additionally, highlighting that most organizations' privacy practices are reactive thereby reacting to external pressure (Xu et al., 2011). Meanwhile, key outputs that strengthen the position of *PbD* suggested by Xu et al. (2011); Karwatzki et al. (2017); Lee, Cho and Lim (2018).

To show the details of each of these references, Table 1 illustrates that in terms of the following columns: journal, author and year, used theories, explanation, key elements, and useful information.

Table 1: Literature Review with identified theories

Journal	Author, Year	Used theories/ terms	Explanation	Key elements	Useful information
MISQ	(Pavlou, 2011)	Privacy Paradox & Privacy Calculus Descriptive Versus Prescriptive (Design) Studies; Information privacy	The privacy paradox was described as the phenomenon where an individual expresses strong privacy concerns but behaves in a contradictory way to these concerns. Privacy calculus (e.g., Ackerman 2004), namely, that consumers will seek to reveal certain information about themselves to obtain certain benefits. The role of context shapes the meaning and conceptualization of information privacy.	IS research should focus more on design and action with an emphasis on building actual implementable tools to protect information privacy. Call for design and action research that focuses on the design of IT artifacts for the protection and control of information privacy.	Confusion surrounding the conceptualization of information privacy is because the concept has different meanings across disciplines, such as a right or entitlement (in the law literature), a state of limited access or isolation (in the social psychology literature), and control over information (in the information systems literature).
MISQ	(Bélanger & Crossler, 2011)	Information Privacy Concern Multilevel Framework	Information privacy is a multilevel concept. Multilevel framework for information privacy concerns.	As design science becomes an increasingly important area of research, IS researchers should consider the development of more (and easier to use) privacy protection practices for individuals, groups, organizations, and society	Information privacy research focuses on explaining and predicting theoretical contributions, with few studies in journal articles focusing on design and action contributions.
JAIS	(Heng, Dinev, Smith & Hart, 2011)	Communication Privacy Management (CPM) theory	CPM is a rule-based theory that proposes that individuals develop rules to form cognitive information spaces with clearly defined boundaries around themselves. Therefore, privacy is complex, multifaceted, and context-specific.	Organizational privacy practices (such as privacy policies) are linked to individuals' perceptions of these practices, which, in turn, can contribute to reducing individual privacy concerns.	Organizations' privacy behaviours have been largely reactive and driven by external pressures. That is, executives rarely take a proactive stance, but rather react to an external event (a threat, security breach, or legislative action)

					that pressures them to act.
MISQ	(Sutanto et al., 2013b)	Personalization-Privacy paradox; Gratifications theory and Information boundary theory	People may be willing to forgo privacy in return for the advantages they enjoy from personalization. IT solution, which delivers a personalized service but avoids transmitting users' personal information to third parties, reduces users' perceptions that their information boundaries are being intruded upon, thus mitigating the personalization–privacy paradox and increasing both process and content gratification.	Need for a better theoretical understanding of the personalization–privacy paradox, and the establishment of alternative measures to alleviate users' information privacy concerns effectively, while still allowing them to enjoy the benefits of personalization.	Users of personalized, privacy-safe application not only engaged in higher application usage behaviour (process gratification) but also saved adverts more frequently (content gratification) than those whose applications lacked this privacy- safe feature.
JMIS	(Karwatzki et al., 2017)	Information boundary theory	the theory acknowledges the important role of individuals' personalities in managing their information boundaries and the resulting information disclosure	Relative to the personalization–privacy paradox, individuals' privacy valuation is a strong inhibitor of information provision in general, not only for personalized services.	Personalization benefits only convince consumers who exhibit little focus on privacy. Thus, service providers need to align their service designs with consumers' privacy preferences.
JAIS	(Jae Kyu, Daegon & Gyoo Gun, 2018)	Prevention motivation (PM) theory & analogical social norm theory, Bright internet	In a social context, people take protective actions about their fear of a severe threat and the high probability of its occurrence. Also, PM theory considers the possibility of self-protection failure. To justify the validity of design principles that have not yet been physically implemented, it is reasonable to infer implicit social norms about the principles from similar existing conventions. The	Bright Internet adopts a preventive security paradigm in contrast to the current self-centric defensive protective security paradigm and requires the design of technologies and protocols, policies and legislation, and international collaboration and global governance	Principles of the Bright Internet using prevention motivation theory and analogical social norm theory, and demonstrates the need for a holistic and prescriptive design for a global scale information infrastructure

			justification approach based on analogical references called as the analogical social norm theory.		
MISQ	(Wunderlich et al., 2019)	The privacy calculus	Where consumers do a cost/benefit analysis of relinquishing privacy in the interest of enjoying new benefits.	Privacy calculus has a strong role in the adoption context of digital and environmentally friendly technologies.	Privacy is one of the importance of motivational factors of the adoption of household IoT technologies. Consumers' concerns about privacy violations will negatively affect their adoption of smart technologies.
JAIS	(Shuaifu & Armstrong, 2019)	Altman's privacy theory (1975); Communication Privacy Management theory (CPM)	Privacy is an input process and an output process. To achieve the desired level of privacy, individuals regulate the level of access to their territory by regulating the territory's boundaries. CPM theory was originally developed to explain how an individual reveals or conceals private information to a confidant(s). CPM theory uses the analogy of a boundary to explain individuals' privacy management behaviours.	Territory coordination is a more significant indicator of privacy management behaviour on SNSs than private disclosure. Based on the work of Altman, individuals can regulate inputs from others in the form of interaction and outputs to others in the form of information.	Altman's privacy theory contends that controlling access to the self includes not only control what information about the self is communicated to others (information privacy) but also controlling the level of access to and interactions with the self (territory privacy).
JAIS	(Gerlach, Buxmann & Dinev, 2019)	mental shortcut—users' stereotypical thinking	Individuals do take mental shortcuts, making their judgments prone to systematic errors or predictable mistakes when judging specific services. For example, the possibility that users might not recognize a privacy-friendly service as such, given their tendency to take mental shortcuts.	Mitigating the judgment errors caused by stereotypical thinking	The resulting misjudgements lead to an inflation of privacy risk perceptions and, overall, stereotypical thinking exerts a significant indirect effect on users' perceived risk.

JAIS	(Chanson et al., 2019)	Design theory & design principles	Mapping Design Principles to Design Features	Propose a design theory, including requirements, design principles, and features.	The adoption of smart products may depend on the ability of organizations to offer systems that ensure adequate sensor data integrity while guaranteeing sufficient user privacy.

As indicated in the previous sections (Section 2), the topic Privacy by Design can best be treated under three themes: technology, privacy, and privacy by design. Based on conducted literature review privacy and technology have distinct roles in understanding privacy by design as they influence *PbD*.

Table 2 below presents a summary of the theoretical background derived from three main themes: technology, privacy, and privacy by design. To show the details of each of these themes, Table 2 illustrates that in terms of the following columns: Themes, concepts, reference, and theme representation.

Table 2: Summary of the theoretical background

Theme	Concepts	Reference	Theme Representation
Privacy • **Regulatory Frameworks**	Privacy for benefits Self-protection failure General Data Protection Regulation California Consumer Protection Act	(Bélanger & Crossler, 2011; Calder & Watkins, 2008; Cavoukian & Popa, 2016; Eagan, 2019; Gjermundrød et al., 2016; Lee et al., 2018; Pavlou, 2011; Wunderlich et al., 2019)	This illustrates failure by individuals to protect their personal data, personal information disclosure for certain benefits, and regulatory frameworks.
Privacy by Design	Proactive/Preventive Transparency & Visibility Full functionality End to end security Privacy as a Default Setting Privacy Embedded in Design Respect for User Privacy	Lee, Cho and Lim (2018), Cavoukian (2013), Spiekermann (2012), Xu et al. (2011) Karwatzki et al. (2017), Cavoukian, (2020), Cavoukian (2009), (GDPR, 2020, Chapter 4 Article 25).	This illustrates privacy by design and guiding principles that organizations ought to follow when developing products and systems using privacy by design approach. Additionally, representing literature that suggests privacy by design as a better approach to solving privacy breaches.
Technologies	Internet of Things Advertising based on behavioral patterns Data analytics	(Calder & Watkins, 2008; Cavoukian & Chibba, 2018; Chanson et al., 2019; Culnan, 2019; Spiekermann, 2012; Sutanto et al., 2013b; Wunderlich et al., 2019)	This illustrates the impact of new technologies on data privacy

2.5 Conceptual Framework

The conceptual framework is developed by a careful undertaking of analysing the topics of data privacy, regulatory frameworks, and data security, followed by these positions highlighted in the literature review from an IS perspective. To adequately investigate privacy by design, all concepts considered to be significant to this study were grouped into three main themes respectively: technology, privacy, and privacy by design considered to be vital to this study. Represented as spheres in Figure 2. Concepts adopted from the privacy calculus theory and prevention motivation theory are used.

Considering the purpose of this study: to use empirical data, based on several qualitative interviews to study design practitioners' awareness and understanding of *PbD*, as well as their ability to realize its principles in agreement with new laws and regulations.

The ***technology theme*** represented by the outermost sphere shaded in green encompasses main technologies identified to affect data privacy such as IoT, advertising based on behavioural patterns, and data analytics. It is important to understand how companies address privacy concerns related to the technologies implemented by their developed systems. Respondents are asked about their perceptions of IoT, behavioural patterns, and data analytics technologies concerning privacy.

Meanwhile, the ***privacy theme*** illustrated by the second outermost sphere shaded in red represents key concepts identified from findings reviewed and considered significant when investigating privacy. At this point, privacy for benefits and self-protection failure which are concepts borrowed from prevention motivation theory (Lee et al., 2018) and privacy calculus (Pavlou, 2011; Wunderlich et al., 2019) are illustrated in the framework. Additionally, including regulatory frameworks particularly, GDPR and CCPA. These are represented by a brown sphere depicting a mutual dependence between privacy and privacy by design. Regulatory frameworks are represented as a subtheme and they are in charge of enforcing regulatory requirements that companies should meet to prevent privacy breaches. However, since this study is focused on GPDR, concepts in this sphere are investigated by asking the respondents about measures used to prevent privacy breaches regarding the new regulatory requirements. Additionally, inquire about the impact of GDPR and CCPA on design teams in companies. On the other hand, the design thinking cloud is a representation of a privacy protection perspective suggested in the conducted IS literature review. This implies implementing privacy in the design of a system. Design thinking is a perspective required in addressing the concepts of privacy as default and embed privacy in design. Leading to a proactive approach method of addressing privacy. Since privacy and technology affect privacy by design, it is positioned at the centre of the conceptual framework.

The ***privacy by design theme*** shaded in blue contains foundational principles of privacy by design which are: proactive, transparency & visibility, full functionality, end to end security. Other principles are privacy as a default setting and privacy embedded in design which are similar guidelines the GDPR and CCPA regulatory frameworks suggest hence the link showcased in the conceptual framework. To investigate awareness and conceptualization of these concepts' participants are asked about the practices they have adopted to ensure transparency, end to end security, full functionality, and whether privacy implementation is addressed during the design of a system.

Additionally, competitive advantage abbreviated as CA is added to investigate the relationship between privacy and competitive advantage. The designed framework below is used as a guide

to show the influence that technologies, privacy and regulatory frameworks have on privacy by design. Subsequently, using the developed themes as a guide for the theoretical summary and interviews.

Conceptual Framework

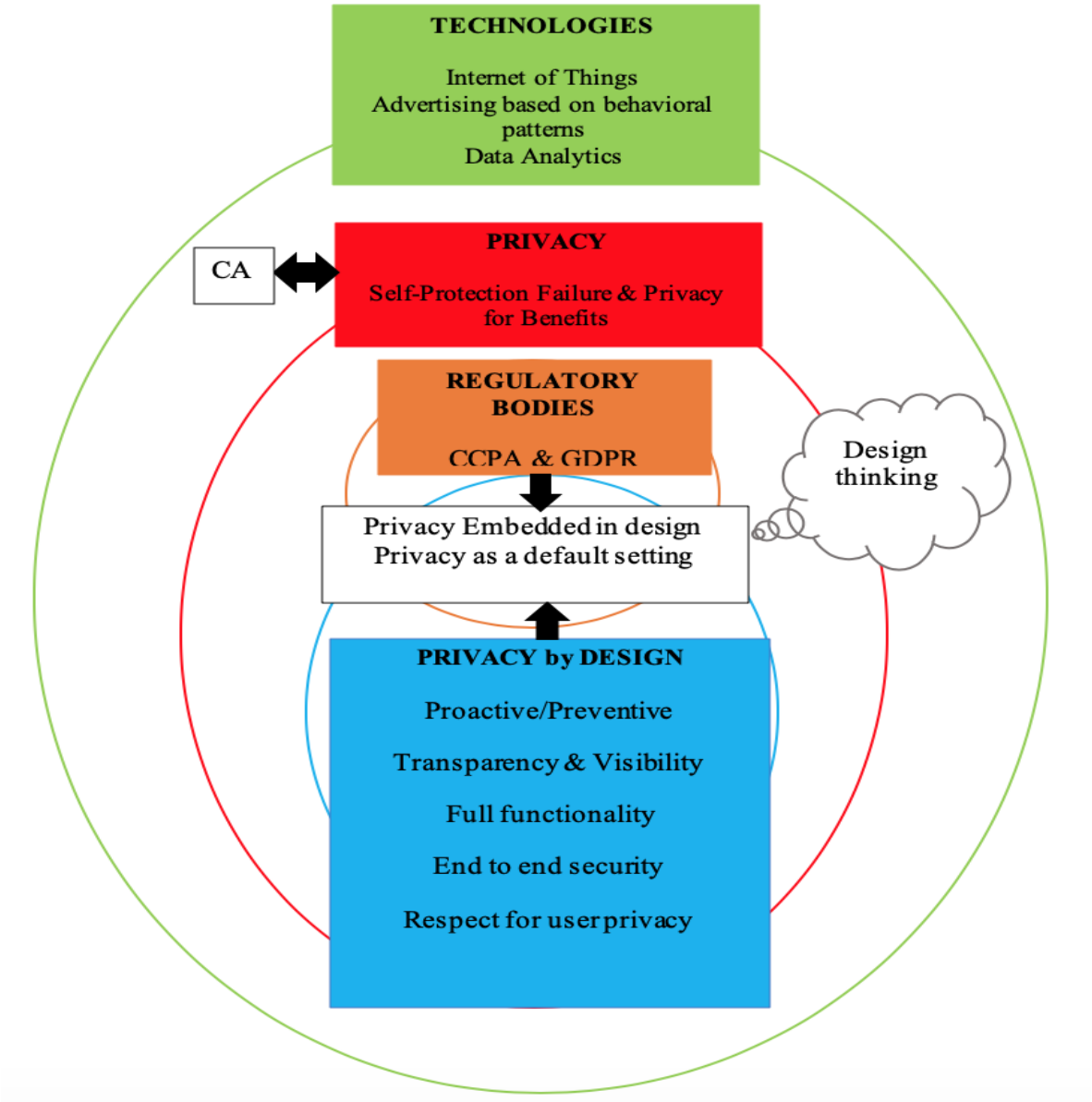

Figure 2: Conceptual Framework

In conclusion, the conceptual framework is developed by categorizing key concepts of data privacy and data security discussed in the previous sections (Section 2) and literature review (Section 2.4) into three themes: privacy, privacy by design, and technology. These themes are further used in the next section as guiding principles when formulating interview questions meant to generate insights that can address the research question.

3 Methodology

As far as this research is concerned, previous chapters have served as a foundation to guide the exploration of the phenomenon *PbD*. In this chapter, the process followed to acquire empirical findings that enable investigation and contribution to the scientific body of knowledge is described.

3.1 Research Strategy

"You've got to think about big things while you're doing small things, so that all the small things go in the right direction" - Alvin Toffler (Patton, 2015, p.45).

Research methodology can be defined as the path through which researchers need to conduct their research while prioritizing required actions in general (Patton, 2015; Recker, 2013). According to Recker (2013), research methodology, or strategy of inquiry is the most important design choice in the research process. This research is exploratory in nature as it attempts to explore the awareness of *PbD* and proactive measures used to prevent privacy breaches concerning new data privacy laws and regulations. The subjective perception of UX and UI designers formed the core data of our study; hence it required a method that would address the research question in an exploratory nature.

To effectively tackle our research problem, our research strategy was to generalize the interpersonal views of UI and UX designers to acquire an in-depth, highly contextual understanding of the current *PbD* practices (Patton, 2015). Therefore, for this study, the research paradigm that was followed is qualitative, and by conducting semi-structured interviews we attempted to explore what kind of practices were adopted by companies to successfully implement *PbD* (Recker, 2013). As opposed to quantitative interviews, this method allowed us to acquire rich data through elaborative interviews with participants, which are not predicted in questionnaires (Schultze & Avital, 2011). To further support our study, a review of the academic literature on *PbD* was conducted. As stated by Recker (2013), the importance of reviewing academic literature lies in the understanding of the current state of the problem and existing theories. This study aims at drawing conclusions based on observations of empirical data and a systematic literature review, in the hope of contributing theoretically to the identified and delimited problem area.

3.2 Research Approach

3.2.1 Conducting a Literature Review

The first step once a decision to study *PbD* had been made, was to critically examine the existing literature to generate a theoretical basis for our investigation. When conducting our systematic literature review, Bhattacherjee (2012) three-folded purpose of a literature review was applied. These purposes were presented as:

1. Exploring the already existing literature within our selected area.
2. Identifying key authors, articles, and theories in that area.
3. Identifying certain gaps that require further investigation due to a lack of knowledge.

Although the process of conducting a systematic literature review was the most time-consuming and intense, it was an indispensable part of generating a conceptual framework that served as a guide to drive further empirical investigation (Table 3). To conduct a thorough literature review, major journals of IS discipline were studied. Using the term "*privacy by design*" as a keyword, journal articles were provided. Unfortunately, these articles only contained specific words and not *PbD* as a term. Therefore, we were required to critically review privacy-related articles to find information related to *PbD*. As a result, ten utilizable articles were identified and a detailed review of these was conducted. However, the results were not sufficient. Consequently, a search for different articles from the interdisciplinary journals was carried out.

The major journals used in the literature review are:

- Management Information Systems Quarterly (MISQ)
- Journal of the Association for Information Systems (JAIS)
- Journal of International Technology and Information Management (JITIM)
- Electronic Journal of Information Systems Evaluation (EJIS)
- Journal of Strategic Information Systems (JSIS)
- Information Systems Journal (ISJ)
- Information Systems Research (ISR)
- Journal of Management Information Systems (JMIS)

Table 3: Literature selection from major IS Journals

Major Journal	**Archive**	**Privacy**	**Privacy by Design**	**Actually about *PbD***	**Useful for the thesis**
MISQ	14637	495	28	0	4
JAIS	7074	191	25	0	5
JITIM	N/A	120	4	0	0
EJIS	525	44	0	0	N/A
JSIS	N/A	44	0	0	0
ISJ	1079	119	0	0	N/A
ISR	152	15	0	0	0
JMIS	N/A	8	0	0	1

3.2.2 Data Collection

In our qualitative study, we preferred to conduct interviews to collect the required data. Although many different methods are used when conducting qualitative research, the most prominent form is interviews, either face-to-face, one-to-many or via conferencing (Bhattacherjee, 2012; Patton, 2015; Recker, 2013). Interviews are most useful when investigating issues in an in-depth way, as they provide detailed information derived from personal feelings, perceptions, and opinions (Recker, 2013). Since we are approaching UI and UX designers from different countries, cultures, and backgrounds, a qualitative study based on interviews was the most suitable method for our study (Schultze & Avital, 2011). With that said, we must consider that there are some limitations of the interview process as it is not free from defects. For one, interviews are prone to the interviewer effect (Recker, 2013). To produce valid data, honest and personal answers are required (Recker, 2013). Recker (2013) refers to the interviewer effect as the possibility that an interviewee will be influenced by the presence of the interviewer and therefore might provide responses, they believe to be desired, rather than sharing their honest experiences and opinions. To alleviate the interviewer effect, we decided to provide an overview of the purpose of our study to the interview respondents beforehand as it would make them more comfortable when conducting the interview (Kvale, 2006).

As COVID-19 continues to affect and alter our lives we are deprived of the opportunity to conduct face-to-face interviews, failing to exploit its many advantages such as a controlled interview environment. However, this allows us to take advantage of the benefits of conducting video conferencing interviews. According to Brinkmann and Kvale (2015), computer-assisted interviews are not only capable of delivering similar quality data, but they are more cost-effective and increase possibilities to talk to geographically distant respondents than face-to-face interviews. Furthermore, all our interviews were conducted via video conference, enabling us to assess the interviewee's body language and expressions (Bhattacherjee, 2012). Additionally, our limitation allowed us to reach out to a much broader population situated all over the world without having to consider geographical restrictions which ultimately resulted in a broader perspective in our research. To conduct our interviews with respondents all over the world, a variation of video conference platforms such as Skype, Zoom, and Google Meet was tested. Ultimately, based on the preference of our respondents as well as the quality of sound and security, Google Meet was chosen as our preferred platform to conduct interviews during our research. To maximize the interaction with our respondents and to observe with an open mind, the entire research team was present during each interview (Corbin & Strauss, 2008). The tasks of recording and taking notes were divided into the group and full support was provided between the members to avoid any difficulties during the interviews (Brinkmann & Kvale, 2015; Corbin & Strauss, 2008). To prepare ourselves for the official interview and interaction with our respondents, we used the "dramaturgical model" of social interaction, playing the role of the interviewer and the interviewees several times (Myers & Newman, 2007, p.12). Moreover, we wanted to be able to overcome embarrassment as well as the fear of interacting with strangers by preparing for various scenarios and most importantly to prepare ourselves to improve the quality of the data collection process (Corbin & Strauss, 2008). Lastly, a pilot interview was conducted to test the questions and to gain some experience in interviewing (Magnusson & Marecek, 2015). The pilot interview was conducted with a participant from India. However, it should be noted that a transcript for the pilot interview was not produced.

3.2.3 Interview Guide

We decided to design a predefined interview structure of a semi-structured nature. Recker (2013) further explains the advantages of semi-structured interviews, by stating that they encourage a two-way communication making it more personal and allowing the respondent to reveal hidden and perhaps, sensitive information. Furthermore, a semi-structured interview follows a conversational form that allows for follow-up questions and customized questions based on the answers of an interviewee (Recker, 2013). Oates (2006) argues that this approach is appropriate when the objective of the interview is to acquire new information, rather than acknowledging what has already been established. The result of a semi-structured approach is a higher level of validity, making it more likely to derive the truth about a phenomenon that has not been studied to any great extent, which is the case with *PbD* (Recker, 2013). All interview questions were developed from concepts adopted from literature and preventive motivation theory, making it easier to review and replicate our study. The interview guide was developed following the conceptual framework that is presented and the questions were categorized based on the different themes in the framework (see Section 2.5). The compatibility between the interview and the conceptual framework ensures that the question and the answers provided by the interviewee target the identified issues; thereby succeeding in meeting the purpose of answering the research question (Table 4).

Table 4: Interview Guide based on theoretical Framework

Theme	Reference	Theme Representation	Question representation	Interview Question
Privacy	Lee, Cho and Lim (2018); Bélanger and Crossler (2011); Eagan (2018); Pavlou (2011); Gjermundrød, Dionysiou, and Costa (2016); Cuscik (2018); Calder and Watkins (2008); Cavoukian (2020); Cavoukian (2009); Redman and Waitman (2020)	This illustrates failure by individuals to protect their personal data, the privacy offered for expected benefits, and regulatory frameworks.	Questions in this theme seek to understand how privacy perceived and what measures companies have put place to address privacy concerns. Additionally, investigating the impact GDPR and CCPA have imposed on privacy.	Questions 5- 10
Privacy by Design	Cavoukian (2013); Spiekermann (2012); Xu et al. (2011); Karwatzki et al. (2017); Lee, Cho, and Lim (2018); Cavoukian (2020); Cavoukian	This illustrates privacy by design and guiding principles that organizations ought to follow when designing	Interview questions in this theme are aimed at investigating the proactive measures companies take to prevent privacy breaches and examine	Questions 11-17

	(2009); (GDPR, 2020, Chapter 4 Article 25)	products and systems using privacy by design approach. Additionally, representing literature that suggests privacy by design as a better approach to solving privacy breaches.	the privacy by design phenomenon.	
Technology	Culnan (2019); Chanson et al. (2019); Cavoukian and Chibba (2018); Spiekermann (2012); Sutanto et al. (2013); Wunderlich, Veit and Sarker (2019).	This illustrates the impact of new technologies on data privacy.	Questions in this theme see to obtain knowledge about the influence of IoT, behavioral patterns a data analytics on privacy	Questions 18-20

3.2.4 Selecting Respondents

Before reaching out to possible respondents for our interviews, we decided to establish certain criteria that would be suitable for our study because purposeful sampling could help us to collect data with good quality (Patton, 2015). After establishing the criteria, we reached out to our respondents using LinkedIn and e-mail, requesting an interview (Table 5). Our main target was professionals who are currently working with the implementation of *PbD*,

The inclusion criteria used for participating in the study included the following:

- UX designer
- UI designer
- UI/UX designer
- Digital designer
- Respondents from a variation of companies - We assume that the same policies are applied to respondents within the same company. The results from our empirical data are enriched by conducting interviews with respondents from a variation of companies
- Respondents that work with personal information, both before and after the implementation of GDPR/CCPA - To acquire a wider perspective on the relationship between *PbD* and privacy regulations.

Table 5: Overview of Interview Respondents

No	Country	Gender	Job Title	Used platform	Date	Duration
Pilot Test	*India*	*Male*	*UI/UX Designer*	*Google Meet*	*06-May-20*	*01:16:00*
R1	Uganda	Male	Senior Product Designer	Google Meet	06-May-20	01:50:00
R2	Japan	Male	UX Designer	Google Meet	07-May-20	00:44:48
R3	Sweden	Male	UI/UX Designer	Google Meet	07-May-20	00:21:36
R4	Greece	Male	UX Designer & Researcher	Google Meet	08-May-20	00:20:59
R5	Canada	Female	UX Designer & Researcher	Google Meet	08-May-20	00:34:35
R6	China	Male	UI/UX Designer	Google Meet	09-May-20	00:31:42
R7	Italy	Male	UI Designer	Google Meet	09-May-20	00:39:54
R8	Bangladesh	Male	UX Designer & Researcher	Google Meet	10-May-20	00:45:08
R9	India	Male	UX Designer	Google Meet	10-May-20	00:32:16
R10	Sweden	Male	UX Lead	Google Meet	11-May-20	01:07:45
R11	Ireland	Female	Digital Designer	Google Meet	11-May-20	00:35:19
R12	UK	Male	Product Designer (UI/UX)	Google Meet	13-May-20	00:25:51
R13	Australia	Male	Head of Product (UX)	Google Meet	14-May-20	01:03:19

Since we seek different perspectives about the adoption of *PbD*, our targeted participants are UI/UX designers from various companies on a global scale. LinkedIn was used to find respondents for our interviews. The process was time-consuming and required continuous effort since only a small percentage of our total inquiries responded. Using our criteria, we spent over a month trying to find suitable respondents for our study. Ultimately, we were able to conduct 13 different interviews with participants from 12 different countries, excluding the pilot testing interview. Participants included, among others, design practitioners from the automotive industry, IT sector, finance, and retail. The participants were from different companies such as Apple, Google, Huawei, Axis Communications, and Deloitte among others.

Respondent 1, Uganda - Senior Product Designer

Respondent 1 has 6 years of experience as a design practitioner. In recent years he has worked exclusively with UX design. Currently, *respondent 1* works as a UX designer within the FinTech industry, trying to improve the lives of users. As described by the participant, a UX

designer needs to be conscious of certain key dimensions and design touchstones that every financial service platform should include.

Respondent 2, Japan – UX/UI & Graphic Designer

Respondent 2 works as a UX/UI designer as well as a graphic designer. Currently, he is based in Tokyo, Japan and has been working as a freelancer since 2016. His practices are strongly shaped by the principles of design and typography. Previously, *Respondent 2* was employed by Portal Japan Inc where he had the role of a web designer.

Respondent 3, Sweden – UI/IX Designer

Respondent 3 began his career in android development. After launching several start-ups, he began to pursue a career as a UX designer. Currently, he works as a UX designer and Android developer at a company based in Malmö, Sweden. *Respondent 3* has a huge passion for UX and UI design and cares just as much about creating a good user experience as he does about writing organized code. In recent years, he has mainly worked with third-party integrations, focusing on lock vendor integrations with Assa Abloy, Salto, and Dorma Kaba.

Respondent 4, Greece – UX Designer & Researcher

Currently, *Respondent 4* is based in Athens, Greece, and works as a UX designer and UX researcher for Blueground, a real estate tech company that offers furnished apartments to vetted guests. His main tasks consist of identifying currents user needs and transferring these needs into wireframe design that is later presented to the UI team. *Respondent 4* has previous experiences in e-commerce, digital marketing, and web development.

Respondent 5, Canada – UX Designer & Researcher

Respondent 5 is a seasoned UX Designer at a company based in Toronto, Canada. In the last decade, she has worked in both Turkey and Canada, taking a variety of roles, ranging from agencies to corporate across different industries. Currently, *Respondent 5* is responsible for transforming the digital ecosystem of one of Canada's most prominent automotive brands. Focused on the creation of end to end experiences, she takes insights from research to crafting elegant solutions that balance usability and uniqueness.

Respondent 6, China - UX Designer

Currently, *Respondent 6* is based in Lund, Sweden. *Respondent 6* has a degree in industrial design and has previous experience as a UX designer at one of the biggest technology companies in China where he mainly conducted usability tests on cloud platforms.

Respondent 7, Italy – UI Designer

Respondent 7 is a UI/UX designer based in Foligno, Italy. *Respondent 7* is a freelancer who prefers to work by himself or with other freelancers as it provides an opportunity to build a better relationship with the client, resulting in a better product.

Respondent 8, Bangladesh – UX researcher

Respondent 8 started his career as a frontend developer six years ago. He then decided to pursue a career in design and has previously worked in the FinTech and eCommerce industries. In

some of his earlier projects, he developed several mobile banking applications. Currently, *Respondent 8* is working on a telemedicine application.

Respondent 9, India – UX Designer

Respondent 9 has over ten years of experience in designing and delivering customer-facing products and enterprise applications. Currently, *Respondent 9* works at Nagarro, global software development and technology consulting company founded in 1996 that provides services to companies and Independent Software Vendors (ISVs). In his most recent role as the Co-founder of 'Experiential Services design', he owned design from inception to research, development, and post-launch iteration.

Respondent 10, Sweden – UX Lead

Over the past three years, Respondent 10 has been one of twelve UX Leads at Axis Communications. The Swedish company which was founded in 1984 is a manufacturer of network cameras for the physical security and video surveillance industries. As described by Respondent 10 himself, the title says it all, as a UX-lead there is far less design and much more leading. His responsibilities include being able to explain to stakeholders, designers, and engineers why something should be accomplished. Previously, he worked as a graphic designer and marketing designer at Lime Technologies.

Respondent 11, Ireland – Digital Designer

Respondent 11 is based in Ireland, Dublin. *Respondent 11* is a graphic designer who graduated from IADT Viscom. Currently, she works as a digital designer at a sub-brand of one of the Big four accounting firms. Her work which is heavily focused on UI/UX design is based on projects within digital transformation. Many of her previous projects have mainly been centred around the digital journey of companies that are a step back from where they need to be digital.

Respondent 12, United Kingdom – Product Designer (UI/UX)

Respondent 12 works as a digital product designer at one of the biggest companies in the world, combining UI and interaction design skills with lean UX thinking. Based in London, United Kingdom he has ten years of experience as a design practitioner. Throughout his career, he has aided start-ups and more established companies in their digital journey. *Respondent 12* has an extensive role in leading user interviews and testing sessions.

Respondent 13, Australia – Head of Product (UX)

"Good UX designers must be fighters because compromised designs are not good design" – Respondent 13.

Most recently, *Respondent 13* was working at Google in Mountain View California where he was leading design on special products. Google Meet, the preferred video conference tool for our research was one of those products. Today, *Respondent 13* is the founder of Simby.com, an artificial intelligence start-up. He is a passionate design practitioner that specializes in product strategy, user experience design (UX), and artificial intelligence. By designing and creating products that matter, he solves problems that affect the lives of billions of people. His way of approaching privacy and data collection is unlike anything we have ever seen before, and although some would call his approach revolutionizing, others would call it ahead of its time. *Respondent 13* also gave a talk on a TEDx event in Frankfurt where he spoke about

emotion and artificial intelligence and how these systems can help us connect with reality again, rather than distracting us from it.

3.2.5 Data Analysis

Wolcott (1994) states that the real challenge of a qualitative study lies in the interpretation of data, rather than in the process of collection. Furthermore, as argued by Recker (2013), data analysis is highly dependent on properly coded data. The data analysis process in qualitative research often involves a vast amount of data to be analysed asking the researcher to establish what is relevant to the study (Recker, 2013). To analyse qualitative data, techniques such as coding, content analysis, disclosure analysis, and critical incidents can be employed. However, for this study, we used coding to derive meaningful information and patterns from the qualitative data that was collected through the conducted interviews (Hsieh & Shannon, 2005).

3.2.5.1 *Coding*

In the analysis of our qualitative data, coding becomes an important interpretation tool (Saldaña, 2015). Seemingly, using a coding technique might simply be considered as a way of collecting relevant text and assigning labels (Auerbach & Silverstein, 2003; Brinkmann & Kvale, 2015; Sullivan, 2012). From this research's perspective, coding is an analytical process that is used to bring structure to our interview text and to work out implicit meanings more (Saldaña, 2015). As stated by Saldaña (2015), coding is mainly based on constructs generated by the research team. To generalize findings obtained while conducting our research, identification of patterns in our interview texts were characterized by frequency, similarity, and casualty (Saldaña, 2015).

However, we were aware of certain downsides of using the coding technique, these were often related to the oversimplification of data. As the objective of coding interview texts is to identify patterns on contracts, we might ignore certain codes which do not fit in the analytical framework (Saldaña, 2015). Consequently, after completion of the coding process, interview texts were analysed again to find hidden meanings that would further elaborate on our research questions (Alvesson & Karreman, 2001). Subsequently, assigning new codes to text believed to be relevant to our study that could not be categorized using the initial coding scheme (Hsieh & Shannon, 2005).

A concept-driven coding was used in the first stage of our coding process as we had predetermined concepts illustrated in the theoretical framework derived from our conducted literature review (Table 2). According to Saldaña (2015), concept-driven coding is referred to as "analytic coding" where meanings are assigned to related elements within the qualitative data (p. 119). Concept driven coding was chosen for this research as it applies to all types of qualitative data and studies with multiple participants (Saldaña, 2015). Moreover, in our case, it is convenient to use elements derived from our conceptual framework as a basis for qualitative data coding (Figure 2). The table below shows the transcription codes we used during the first coding phase (Table 6).

Table 6: Transcript code (Phase 1)

Theme	Concepts	Code
Privacy • **Regulatory frameworks**	Privacy for Benefits	PB
	Self-Protection Failure	SPF
	General Data Protection Regulation	GDPR
	California Consumer Privacy Act	CCPA
Privacy by Design	Proactive/Preventive	PP
	Transparency & Visibility	TV
	Full Functionality	FF
	End to End Security	EES
	Privacy as a Default Setting	PDS
	Privacy Embedded in Design	PED
	Respect for User Privacy	RUP
Technology	IoT	IoT
	Advertising based on Behavioral Patterns	ABP
	Data Analytics	DA

In the second phase of our coding process (Table 7), the objective was to make sense of the concept coding by reorganizing and reanalysing coded data from the first phase (Corbin & Strauss, 2008; Patton, 2015; Saldaña, 2015). In other words, we tried to logically link seemingly related facts and develop a meta-synthesis of the data corpus to accurately interpret qualitative data (Silver & Lewins, 2014; Saldana, 2015).

Table 7: Transcript code (Phase 2)

Coding phase	Theme	Concepts	Code
Phase 1	**Privacy**	Privacy for Benefits	PB
		Self-Protection Failure	SPF
		General Data Protection Regulation	GDPR
		California Consumer Privacy Act	CCPA
		Competitive Advantage	CA
	Privacy by Design	Proactive/Preventive	PP
		Transparency & Visibility	TV
		Full functionality	FF
		End to end security	EES
		Privacy as a Default Setting	PDS
		Privacy Embedded in Design	PED
		Respect for User Privacy	RUP
	Technology	Internet of Things	IoT
		Advertising based on Behavioural Patterns	ABP
		Data Analytics	DA
Phase 2	**Open code**	Safety with Information Sharing	SIS
		Basic right to be Non-Recognizable	BRNR
		Hire Experts	HE
		Access Restriction	AR

The reliability of coding (Table 8) was ensured through an intercoder reliability check where all members of our research team independently analysed the interview texts, following the coding table as a general guideline (Given, 2008; Neuendorf, 2017, p. 165). Subsequently, after each coding phase, team discussions were held to correctly label codes in the interview text (Brinkmann & Kvale, 2015).

Table 8: Intercoder reliability check

Interview Transcript	Coding Phase 1			Coding Phase 2
	Coder 1	Coder 2	Coder 3	Coder 1
R1	Esther	Arman	Mandukhai	Team discussion
R2	Esther	Arman	Mandukhai	Team discussion
R3	Esther	Arman	Mandukhai	Team discussion
R4	Esther	Arman	Mandukhai	Team discussion
R5	Esther	Arman	Mandukhai	Team discussion
R6	Esther	Arman	Mandukhai	Team discussion
R7	Esther	Arman	Mandukhai	Team discussion
R8	Esther	Arman	Mandukhai	Team discussion
R9	Esther	Arman	Mandukhai	Team discussion
R10	Esther	Arman	Mandukhai	Team discussion
R11	Esther	Arman	Mandukhai	Team discussion
R12	Esther	Arman	Mandukhai	Team discussion
R13	Esther	Arman	Mandukhai	Team discussion

Another approach that we used during our data analysis was the "treat descriptive data as a fact" (Wolcott, 1994, p. 10). Several statements from the interview transcripts were used as quotes, and in many cases, valuable data were able to speak for itself. Furthermore, any computer software was not used to analyse our data, as we found hand coding to be more efficient (Patton, 2015).

The process of qualitative data analysis is not as simple as a mathematical equation where an exact number or value is extracted. It requires creativity and inventiveness from the researcher to reach analytical ambition by "not just transform data but transcend them to find something else, something more, a sum that is greater than its part" (Wolcott, 1994; Saldana, 2015, p. 235). The best approach for coding was reading transcripts repeatedly to engage qualitative data and produce more meaningful intellectual work (Brinkmann & Kvale, 2015; Patton, 2015). Therefore, the research team placed great importance on accurately execute the different coding phases to acquire new perspectives and insights from the qualitative data.

By way of illustration, Figure 3 below shows how the codes were assigned to specific parts of the text in the interview transcripts. Given the exploratory nature of our research, we analysed

the empirical data based on predefined concepts as earlier discussed. To successfully address our research question, we were required to analyse the text by cross-examining the response against the concepts to explore the practices adopted to meet that specific concept.

By exemplification, according to figure 3, when the respondent R13 was asked about the stage of product development when privacy should be implemented, his response depicted approaching privacy from the early stages of product development hence matching with the concept Proactive/Preventive. We also highlighted the text following Patton (2015) recommendation about highlighting text for simpler analysis.

		Yeah, and I think there's some stark differences between the two. So yeah, the long answer is that, the short answer is that privacy is a movement away from the chaotic end game where we have zero control towards an area where we do have control.	
11	I	In your experience, when is privacy implemented in product development?	
12	R13	So, with Simby this was our issue, that it is from day one. It's the very first page of the very first deck slide, you know that you put it together for your investors because you can't undo things with privacy. For example, if you have a server running with Google cloud or with Amazon AWS, that server is logging IP addresses, and you cannot not have it do that. If you have customers, who you make promises to that their data is private and that it will not be sold ever and that it will not be stored. Then you're lying right from the very beginning if you're using a cloud provider because no Cloud providers that I'm aware of are not logging IPS. So there's a lot of stuff that we had to do to purge that data on a daily basis and anonymize our customers intentionally so that if we ever got customers which we don't have any because we didn't go live but when we do and if we do go live our systems are established in such a way that we aren't gathering data that allows us to figure out who somebody is and that was our litmus test. We made the promise that we will never be able to know	PP GDPR, PDS

Figure 3: Assigning codes

3.2.6 Research quality

Ensuring qualitative research quality is a task fundamentally dependent on the researcher (Hafeez-Baig, Gururajan & Chakroborty, 2016). Reflecting on this, it was our responsibility to ensure that our research was reliable and valid. However, few studies discuss how to achieve quality in qualitative research (Hafeez-Baig et al., 2016). Whereby, different studies depict varying identifications of what is regarded as quality in qualitative research (Seale, 1999). This

has led to the use of quantitative quality check concepts being employed in qualitative research hence resulting in avoidable limitations (Stenbacka, 2001). Putting this into account, we considered validity, reliability, generalizability, and carefulness to establish quality during our research (Seale, 1999; Stenbacka, 2001).

The **validity,** a quality concept that seeks to establish a clear understanding of the phenomenon being studied was ensured by selecting UX/UI designers who design the systems and products that are susceptible to privacy breaches (Stenbacka, 2001).

On the other hand, **reliability** is described as the method's ability to produce the same results when repeated (Stenbacka, 2001). To establish the validity of our research, during the conducted interviews, we used digital voice recorders after obtaining the respondents' consent as a means to focusing our interview and achieving accuracy in the transcribed dialogue (Brinkmann & Kvale, 2015). Subsequently, using the audio files to create interview transcripts (see Appendix 2 to 14). Meanwhile, during the interviews, one of the team members wrote down keynotes that were used to confirm the content provided by respondents while closing the interview as a method to improve the reliability of the study (Brinkmann & Kvale, 2015). Additionally, Recker (2013) advises that coding is subject to bias which affects the reliability of research. To address coding reliability, when the coding activity commenced, we simultaneously coded the same transcripts of data obtained through open structured interviews and thereafter compared the configurations before selecting the final codes as a team to examine differences (Table 9).

Generalizability which entails the formulation of conclusions based on generalization beyond empirical data (Recker, 2013) was addressed by strategically selecting participants dealing with the technologies under investigation and presenting general findings in relation to themes discussed in the theoretical chapter (Stenbacka, 2001).

Lastly, **carefulness** established through a systematic and informative description of all the steps involved throughout our research study.

According to Brinkmann and Kvale (2015), video conferencing platform interviews are not only capable of delivering similar quality data, but they are more cost-effective and easier to conduct than face-to-face interviews.

In summary, we considered validity, reliability, generalizability, and carefulness to ensure the quality of this research. Based on recommendations made by researchers that validity and reliability are not adequate to establish quality in qualitative research.

Table 9: Summary of the Data Transcription

Appendix Number	Interview Number	Respondent	Transcribed by	Edited by	Verified by
2	1	R1	Arman	Mandukhai	Esther
3	2	R2	Arman	Mandukhai	Esther
4	3	R3	Arman	Mandukhai	Esther
5	4	R4	Arman	Mandukhai	Esther
6	5	R5	Arman	Mandukhai	Esther
7	6	R6	Arman	Mandukhai	Esther
8	7	R7	Arman	Mandukhai	Esther
9	8	R8	Arman	Mandukhai	Esther
10	9	R9	Arman	Mandukhai	Esther
11	10	R10	Arman	Mandukhai	Esther
12	11	R11	Arman	Mandukhai	Esther
13	12	R12	Arman	Mandukhai	Esther
14	13	R13	Arman	Mandukhai	Esther

3.2.7 Research Ethics

Ethics is considered as a notion that seeks to define the distinction between right and wrong moral conduct (Davison, Kock, Loch & Clarke, 2001; Bhattacherjee, 2012; Recker, 2013). According to Bhattacherjee (2012), research is subject to manipulation often done to suit private agendas. Since ethical issues while conducting research mainly arise from the design, data collection and analysis processes (Davison et al., 2001), ethical principles followed during this research are those suggested by Bhattacherjee (2012) discussed below:

- **Voluntary participation and harmlessness**
  We ensured the establishment of this principle by personally sending interview participation requests via email and LinkedIn which necessitated either a response about willingness to participate, unwillingness to participate or no response at all. Subsequently, scheduling interview meetings with those who volunteered to participate.

- **Anonymity and confidentiality**
  All participants were first questioned about their decision on anonymity and being recorded as seen in the interview guide (See Appendix 1). However, since we conducted video google meet interviews and saw the participants' faces, complete anonymity could not be guaranteed. Nevertheless, all names were anonymized in this report to established integrity.
- **Disclosure**
  This was established by incorporating a brief description of our study in the participation requests that were distributed via email and LinkedIn. Therefore, the potential participants who were not in a position to discuss anything about the company privacy practices had an opportunity to decline the requests.
- **Analysis and reporting**
  We ensured the establishment of this principle by presenting all the findings obtained from the interview in the findings and discussion sections.

In summary, the conduction of this study was done following ethical principles: voluntary participation and harmlessness, anonymity and confidentiality, disclosure, analysis, and reporting with all the collected findings discussed in the subsequent chapters objectively.

4 Empirical Findings

In this chapter, the findings of the semi-structured interviews that were conducted for this research are provided. These findings are presented concerning the predetermined themes and concepts illustrated in the theoretical framework (See Table 2).

4.1 Privacy theme

4.1.1 Privacy for Benefits

Companies strategically design products with features that require the submission of personal data for users to be able to utilize the products. The concept is not commonly mentioned among respondents and only a few of them raise the subject during the interview (R3; R9; R13). R13 states that: "and I myself, caring about privacy will scroll quickly with my thumb and hit agree. And I care, right?" (R13:34). However, another respondent claims that: "sometimes people are not so concerned about their privacy in certain countries. They are not concerned because they do not know what people will do with their data" (R9:46).

4.1.2 Self- Protection Failure

During our interviews, this concept was expressed the least among respondents, and only two respondents raised the subject (R5; R9). According to R9, people fail to protect their privacy because they simply do not understand privacy policies (R9:46). On the other hand, some people are aware of their privacy and they try to avoid certain features such as: "a persistent question like submit your location and users are hating that, they don't want to submit their location." (R5:26).

4.1.3 GDPR

Among most respondents, GDPR was a well-known concept (R1:10; R1:14; R3:20; R4:14; R4:8; R5:14; R7:14; R10:14; R11:14; R12:14; R13:10; R13:16; R13:34). GDPR has been deeply adopted by respondents from Sweden, Australia and Ireland comparing to other respondents (R10:10; R10:16; R10:18; R10:24; R10:26; R10:32; R13:12; R13:18; R13:20; R13: 26; R13:28; R11:12; R11:28: R11:32; R11:34). Notably, compared to other participants, respondents from Sweden expressed the highest engagement with GDPR (R10:10; R10:16; R10:18; R10:24; R10:26; R10:32). Moreover, the discussion around GDPR generates insights about collaboration of legal and design teams (R10:16) and the ability to protect them "by not gathering too much information" (R10:24).

During the interviews, several respondents made explicit references to data minimizations which is one of the more important principles of the GDPR, as one of the privacy measures they are taking to prevent privacy breaches. When it comes to data collection, the strategy of R1's company is described in the following way:

- "we need to be strategic when we ask for information" (R1:10)

  "What information is required from the users; what information is absolutely necessary?" (R1:10)

However, several respondents refer to the data minimization in GDPR when responding to different questions throughout the interview. For instance, when R11 was asked about her company's design measures employed to ensure full data lifecycle protection, her response explicitly referred to data minimization as she points that they ensure that the minimum amount of data required is gathered and later removed after a week when it has served its purpose (R11:32). Similarly, the topic of data minimization surfaced in the dialogue with R13 when discussing the stage in which privacy is implemented in product development. Towards the end of the dialogue he stated the following:

"[...] our systems are established in such a way that we aren't gathering data that allows us to figure out who somebody is, and that was our litmus test" (R13:12).

Meanwhile, respondent R13 was aware of the GDPR and compliant with the regulation before it had been enforced as mandatory (R13:18). R13 further elaborates that:

"[...] GDPR is like table stage for use, we've gone over and above that. We are compliant before we've even started. And our issue was not managing to obtain compliance. It was to maintain compliance because we were compliant before we began. And what makes an interesting point is new organizations who begin today and receive funding or begin with a plan to create a company in Europe are not obligated to be compliant before they get started. They're obligated to be compliant from when data is being collected" (R13:18).

"So, they need to obtain compliance rather than maintain compliance and it would be an interesting concept to build into the creation of organizations..." (R13:18).

Through this, when respondents were asked about how the GDPR had affected their work, based on information received, it became clear that the GDPR had affected businesses that were located beyond the borders of the European Union. R1, a respondent located in Kampala, Uganda stated:

"it was around that time, 2018, we started exposing privacy policies and making them clearer to the user" (R1: 16). "…before, we didn't really worry about what information we asked for, we could ask for anything we wanted, and it was easy to get information because in my experience the average person really doesn't care" (R1:16).

"Especially when you work with cloud solutions, legal is basically a part of everything. Like when you're planning features" (R10:16).

In a parallel argument, respondent R3 had an alternative comment about the influence of the GDPR on their work stating that the approach they had adopted was to establish a legal team to avoid getting sued. R3 further discusses that user privacy was not considered as anything important before GDPR.

Throughout the interview and as a response to various questions, R10 and R4 extensively talked about the use of opt-out and opt-in options in their design (R4:14; R4:24; R10:10; R10:18). They both described the options of opt-in and opt-out as important design considerations

concerning privacy as a default setting. Having this in mind, R10 presented interesting statistical findings, showing that the inclusion of opt-out and opt-in in design considerations does not affect a company's business negatively, as less than 15 percent decided to opt-out when given the opportunity (R10:10). When concerning opting in, approximately 60 percent will decide to opt-in when given the opportunity (R10:10). According to R10, these statistics emphasize the fact that the common user tends not to care about privacy in this context and about privacy measures adopted.

On the contrary, respondents from Japan, China, India, and Bangladesh were not familiar with the regulation at all (R2:14; R2:16; R6:14; R8:14; R9:16). For example, R2 said that "...to be honest I don't know about the details. GDPR I know because I recognized the acronym, but not in details. Basically no, it doesn't ring a bell..." (R2:14). Furthermore, another respondent stated "I heard about that. I have never read them in detail..." (R9:16).

Overall, the acceptance level of the GDPR is high and it is clear that regardless of geographical location, digital products or services need to align with major regulations eventually (R1:14; R3:20; R4:14; R5:14; R7:14; R10:14; R11:14; R12:14; R13:16).

4.1.4 CCPA

The findings from our interviews made it clear that the CCPA is indeed a newly enforced regulation. The regulation was only known to three respondents, these were from Greece, Sweden, and Australia. (R4:24; R10:14; R13:16). Several respondents admitted that they were not familiar with the CCPA (R2:14; R2:16; R6:16; R8:14), while others simply skipped the questions without a response, such as R2 who stated the following:

"I do not even know when it was enforced" (R2:16).

However, most respondents question the importance of CCPA (R2:38; R5:22; R5:26; R9:36; R9:16; R12:10; R12:34; R12:36: R13:10; R13:24; R13:28; R13:34; R13:42).

4.1.5 Competitive Advantage

In this context, competitive advantage refers to a concept in which a business attracts more users due to the provision of better privacy. On this account, an investigation was conducted on the relation between privacy and competitive advantage by asking respondents about their perception of the impact privacy has on competitive advantage.

Generally, the competitive advantage was seen as an outcome of the successful implementation of privacy protection measures by most respondents. Both internally in the organization and as a means of attracting new customers (R1:20; R6:20; R8:20; R10:20; R12:12; R12:20; R12:38; R13:22). Furthermore, when asked about the opportunity to obtain competitive advantage due to better privacy provisions, R1 said claimed that:

"...people get a lot more comfortable in the platform and trust you a bit more than your competitors... Right now, the competition has increased which means privacy is becoming more important" (R1:20).

When asked the same question, the response of R2 was quite the opposite concerning the statement made by R1, as he would not see it as a competitive advantage since he is often

contracted by digital agencies to work on their projects as a UX designer and the contractors oversee the privacy of the product. However, R12 fully believes there is a strong connection between good privacy and competitive advantage. He states:

“Yeah, absolutely. Personally, I care a lot about this specific subject. I have seen excessive collecting of data just because they can collect it “(R12:20).

Meanwhile, he had earlier mentioned that one of the practices his company has in place to ensure the right privacy protection was a push towards the provision of better privacy as a service acting as a:

“...differentiator from others...” (R12:12).

“...It will definitely bring advantages because people care about privacy, and they will care more and more...” (R12:38).

R13 also discussed the relation between privacy and competitive advantage and argues that:

“...we will start to see that it becomes highly valuable that an organization behaves in this way or similar ways. You can start to see it with Apple...” (R13:22).

Meanwhile, the rest of the respondents presented a different view on whether privacy would bring certain advantages to their business operation (R2:22; R3:26; R4:18; R5:20; R7:22) Yet only a few of them would further elaborate on why they disagree:

“... I don't think because of the visible privacy. You know, the one that you can see as a user is, most of these are the same for everyone. I think the most critical part is the back end. But the back end is not visible to other competitors...” (R4:18).

4.2 Privacy by Design Theme

4.2.1 Proactive/Preventive

Proactive/preventive is one of the foundational principles of *PbD* which in this case was used to investigate the different approaches adopted by companies to address privacy concerns and prevent privacy-invasive events. In our interviews, responses from respondents that pointed towards this concept were obtained from various questions that were asked.

Against the provided description, proactive/preventive was the second most discussed principle of *PbD* during the interviews (R1:10; R1:40; R2:10; R2:44; R4:22; R4:38; R5:10; R5:42; R6:40; R7:10; R8:10; R8:40; R9:44; R10:10; R10:42; R11:10; R11:44; R11:46; R12:10; R12:12; R12:34; R12:42; R13:8; R13:12; R13:14; R13:44).

When respondents were asked to give insights about when privacy should be implemented in development, many responses pointed towards the ideation process (R1:10; R2:10; R5:10; R8:10; R11:46; R12:10; R12:34). R1 said that:

“We need to think about permissions as well. Also, we have to think about legal things right away, because they affect our development” (R1:10).

"It saves you a lot of bad experiences, and a lot of headaches in the future" (R1:40), and "the more proactive you can be, the more profitable it will be for you in the long term" (R4:38).

Meanwhile, data analytics was pointed out in the literature review findings as one of the technologies susceptible to privacy breach since it requires large volumes of data to provide insights. To investigate the relevance of the adoption of a proactive approach towards privacy, respondents were asked to give their opinions. One of the respondents explained that the adoption of a certain proactive practice is usually dependent on the context:

"...we were talking about services within the bank sector, a banking site, then it is very important, and a proactive approach is required. But if I am going into a particular website where I need to sign up, and if it requires too many security questions, I will not sign up" (R9:44).

In a parallel argument, R12, a respondent from a major company in the UK strongly expressed the importance of a proactive principle (R12:10; R12:12; R12:34; R12:42). He stated the following:

"A proactive approach, I think it's really fundamental, it is beyond important" (R12:42). "...if you start from scratch and privacy is a core value of your company, then there is no trade-off, you just build it in the way you want it to be built. That means, when you implement privacy reactively, like an after thing, then there is definitely going to be a trade-off" (R12:34).

Among all the respondents, R13 described a proactive approach most accurately as:

"...you can't undo things with privacy..." (R13:12).

However, some respondents have controversial standpoints about the adoption of a proactive approach (R1:24; R2:10; R3:10; R8:12; R12:34). Also, the approach must be specific to what you do and the perspective on a proactive approach depends on the scale of the project. It is however less considered in small projects (R2:10; R3:10; R7:10; R8:12). More precisely, one of them argues that:

"It depends on the scale of the project for my experience. If the product you know is only for small segments, a small target of people then probably we will put less importance on privacy... Other than that, if it's a big project, again, we need to probably think about privacy and security in many pretty much all the phases" (R2:10).

Additionally, R4 presents an interesting perspective on the subject of proactive approaches. Although he highlights the importance of a proactive approach when it comes to privacy, he acknowledges one of its fundamental difficulties, which is in order to be proactive, you must first know what can happen. He argues:

"I think it is very important. If you can secure your website or the app and the data you store before the breach happens, that is ideal. However, in reality usually it's difficult because you can be proactive on some things, but you cannot think of everything. There are always breaches happening, so you have to be quick and adapt quickly. But the more proactive you can be, the more profitable it will be for you in the long term" (R4:38).

4.2.2 Transparency & Validity

This principle is familiar amongst most participants (R1:12; R1:16; R1:26; R1:36; R1:42; R2:38; R2:42 R3:22; R7:28; R8:26; R9:26; R9:28; R9:30; R10:20; R11:28; R13:14; R13:28; R13:42).

During our interaction with R1, the introduction of the GDPR affected their work in a way that they now had to provide users with more transparency, choice, and control. He claims that: "What really changed after GDPR, for the better I would say is that you had to explain to users why you needed certain information" (R1:16). Similarly, R2 said that "...more transparent, having more control..." (R2:42) when sharing insights about embedding privacy by default in products and systems using IoT. However, as stated by (R2:38; R7:28) it will usually depend on the project.

In the same way, R3, R9, and R13 extensively talk about transparency and highlight the importance of allowing users to have the right to know why certain data collection is required, how it can be retrieved as well as how it can be deleted (R3:22; R9:26; R13:28).

In comparison, respondents from Greece, Canada, China, and the UK do not point out anything that could be mapped to the concept of validity and transparency (R4; R5; R12). However, R6 stated that "At least in China, I think they are using the data of the users without them knowing. Or they know but they rarely notice the terms of privacy. But still they are using the data, and there is no denying many can get access to your data" (R6:26).

4.2.3 Full Functionality

Although many understood the concept of full functionality, they did not find it to be part of the reality of system development and emphasized the inversely proportional relationship between functionality and privacy (R1:34; R2:36; R3:10; R3:30; R3:34; R3:46; R4:32; R5:30; R5:36; R7:36; R9:38; R11:38; R12:28; R12:34; R13:36). When asked whether there is a trade-off between completing core functionality and embedding by privacy by design R1 claims that: "I think there is a trade-off. You are a business, and when you launch a product you have goals and projections which you need to meet. If you do it the right way, and you embed privacy during the process, you probably won't get where you want in time" (R1:34). R2 in a similar manner stretches the fact that consideration to privacy during development often results in a trade-off of functionality (R2: 36). Additionally, R3 elaborates on the scenario by saying that "Let's say you have your core functionality, and you're designing a product from a privacy point of view, there are times where core functionality will suffer (R3:46). "I know that we had to remove features due to privacy" (R3:34).

Another respondent, R5 expressed her concerns regarding the trade-off as a UX designer when she says: "...I am sacrificing usability to a lot, you know, if you are working as a sole UX designer in a company, you have battles more than one, because like you have to battle with client, with your colleagues with many other departments and you're like to advocate of the user and you have to tell them like this is not usable and you have to be usable but they say like, oh, we actually care about sales and as long as they get the numbers, they don't care about usability..." (R5:30).

Different responses received concerning full functionality:

- "Depends on the budget and the requirements and actual client's preferences on how much time and budget they would allow" (R2:28)
- "I think by building products with privacy in mind definitely limits what some companies can do" (R12:28)
- "You have to finish certain core functionalities and the privacy comes second" (R4:32)

Several respondents were already familiar with this principle (R2:18; R2:28; R4:26; R8:28; R8:34; R10:36; R11:38; R12:34; R12:34). Also, as opposed to other respondents, one claimed that: "I think privacy is just some options you give but these are like making usability better rather than sacrificing it" (R4:26). Another respondent stated: "In my experience, I have seen that only big corporations are able to maintain privacy because they really focus on that. But in other countries, such as third world countries, they are not investing much money on privacy" (R8:28).

4.2.4 End-to-End Security

The concept of end to end security implies that companies protect user data throughout its lifecycle. This is the least implemented *PbD* principle among respondents with a few showing concerns of the need to ensure end to end security (R1:30; R3:16; R4:12; R4:28; R8:30). Among those that consider end to end security to be highly relevant, R1 mentions that "when the data is with us, in our database, it is our responsibility to protect it" (R1:30). Similarly, R4 says that: "...when we take some information from our users and we try to deposit them in secure spaces and also apply secure ways of transferring data so that there are no leaks at this process" (R4:12). But later making a contrary statement that they transferred the data protection responsibilities to third party payment providers believed to offer better security for their users (R4:28).

4.2.5 Privacy as a Default Setting

When it comes to the concept of privacy as a default setting, most respondents find it simply essential (R1:32; R2:34; R3:40; R3:44; R4:30; R5:34; R7:38; R8:32; R9:36; R10:24; R10:26; R10:28 R10:32; R10:34; R11:32; R11:34; R12:12; R12:32; R13:12; R13:12; R13:14; R13:26; R13:34; R13:40).

According to R3, it is "a good way to make users comfortable" (R3:44). Additionally, other respondents suggest that: "provide privacy options for all users" (R5:34), and "privacy has to be ensured for anyone" (R4:30). This distinction is further explained by R10 that: "Of course, in some businesses you have to collect personal information. But in our business, it really does not matter who says what. And in those businesses, I think it is important to give consumers the maximum privacy as a baseline. Or in any business where they are using personal information" (R10:34).

The concept is more strongly supported by respondents from Sweden and Australia in comparison to those from other countries (R10:24; R10:26; R10:32; R10:34; R13:12; R13:14; R13:26; R13:34; R13:40). These are more precise responses that define the concept of privacy as a default setting:

- "Anonymize our customers intentionally..." (R13:12)

- "A broad sweeping promise that we would never know who our customers were so that we did not want to store any personally identifiable data" (R13:26)
- "We could not ask our customer upfront. Do you want the private version of our product or the non-private version of our product?" (R13:34)
- "I haven't seen any reason to collect and use information that would identify you as a person" (R10:32)

However, respondents from Japan and Ireland have a different position (R2:10; R11:36) as below.

- "It depends on the scale of the project for my experience. If the product you know is only for small segments, a small target of people then probably we will put less importance on privacy. And if it's like a big project or existing project with let's say 10,000 users or so, then it would be different" (R2:10)
- "In a lot of context, they don't have a choice right..." (R11:36). Here, R11 refers "they" as users

4.2.6 Privacy Embedded in Design

In regard to the concept of embedding privacy in design, many respondents reflected positively (R1:36; R3:48; R5:10; R5:38; R8:36; R9:40; R10:10; R10:38; R12:38; R13:12; R13:14; R13:38).

Under these circumstances where technology is constantly changing, it is important to prioritize privacy by implementing it in the design so that users can confidently share personal data without any hesitation (R8:36). Embedding privacy by design is essential and through this, provide clear instructions and explanations as to why users should choose to consent to something (R1:36). According to R8, "infrastructure should be secure enough to ensure privacy" (R8:36) since "embedding privacy helps us" to improve client relationships and increase reliability (R5:38).

Furthermore, R12 argues that: "I don't think it's even that difficult to embed privacy in any product ... It's just a matter of doing it and doing it at the right time" (R12:38). Finally, R13 a respondent from Australia referred to design goals regarding the principle as:

"...So, another maxim that we had inside of our organisation is that it is not a matter of if we will be hacked it is a matter of when we will be hacked. So we just assumed by default that one day we would be hacked and our responsibility was to make sure that after getting through all of the barriers of protection that were put in place the hacker would arrive at an empty room with a note from me saying: ha-ha, we don't have your data..." (R13:12).

When it comes to privacy embedded in the design, R2, R4, R6, R7, and R11 are quite restrictive in their arguments and do not discuss anything that relates to this principle.

4.2.7 Respect for User Privacy

Based on previous experience, ensuring that users understand their privacy builds flexibility instead of them having to read a long text of privacy policy (R6:18). This is confirmed by R6 who states the following: "In my experience, it is important to make the users understand

their privacy because it makes them more agreeable instead of just putting in some long text" (R6:18).

Among respondents, Respect for User Privacy is the most discussed principle of the PbD framework (R1:12; R1:16; R1:18; R1:28; R1:36; R2:18; R2:20; R3:24; R3:34; R4:16; R4:24; R4:30; R5:18; R5:26; R5:38; R6:18; R6:32; R6:34; R8:24; R8:30; R8:32; R9:20; R9:32; R9:46; R10:10; R10:18; R10:30; R11:16; R11:18; R11:30; R12:18; R13:20; R13:28; R13:30; R13:34). R1 mentions that: "it's good to mind about people's privacy on your platform" (R1:28). Given that: it's pretty easy because we try to have like a bit minimal UI" (R4:16).

Several respondents were strongly engaged in the discussion about privacy policy readability and how it is important not to trick users with lengthy texts (R6:18; R6:34; R:32; R2:18; R9:46; R10:18). For instance:

- "You need to make this information more visible to people, so they can understand your privacy maybe just by looking or glancing through your site" (R6:34)
- "Privacy policies should be easily readable" (R8:32)

Furthermore, more than most, R8 promotes a user-centric perspective regarding the concept. He argues that "we are making products for humans, not for technology" (R8:24). Furthermore, he claims that:

"...There are various methodologies on those things which we can follow. Like empathy mapping. Again, the users are in the centre. We can see where users are scared or where they are comfortable. From those points we can start to make privacy policies, ensuring them that their information is hidden. I think empathy mapping is one methodology where we can start..."

Few respondents that factor such as project scale (R9:32) and "...sometimes if the budget, time and the client allow..." (R2:18) have to be taken into consideration.

During the interviews, we discovered a good example of a privacy policy. R13 claims that:

"...we made it very clear at https://simby.com/data-privacy... it's not like some terms and conditions in a very small font that we hide but instead we elevated it to make part of our differentiating value. The font was huge, you know, we don't want your data..." (R13:20).

It was quite interesting and revolutionizing to see that a small start-up like Simby could have such a bold statement. According to R2, the size of the company has an impact on the practices implemented about the respect for user privacy, he states: "not many companies do, but recently the bigger companies do" (R2:20). Furthermore, R2 and R3 express their appreciation towards creative ways of respecting user privacy, both promoting Google as a good example (R2:18; R3:24). Furthermore, R2 argues that:

"...I like the way that Google does with their privacy terms. When they change the terms, we receive emails. We receive emails saying that this is what we changed and it's super easy to understand. And you don't have to go and click and read whole terms of agreement..." (R2:18).

However, a few of the respondents convey contrary opinions about the concept of respecting user privacy (R1:26; R7; R11:16; R11:18; R13). R1 argues that in most cases, *"people don't read your terms and conditions they just don't do it*" (R11:18). Sometimes, they had to remove some product features due to privacy restrictions (R3:34; R11:30). Therefore, their

thoughts in this regard are that they sacrifice their ability to serve their customers (R3:34). Regardless, "*it makes things easier*" (R10:30), and "*it is a short-term sacrifice*" (R13:30).

4.3 Technology Theme

4.3.1 Internet of Things

The concept was openly discussed amongst many respondents (R1:36; R2:38; R3:48, R4:34, R5:38, R6:36; R7:38; R8:36, R9:40, R10:38, R12:38). Below, a statement made by R3 about integrating privacy in IoT devices: "When we're talking about IoT, you have things in your own house, connected to you. Then people would not only know information about you, but they could come into where you live" (R3:48).

Provided that "IoT devices require personal information" (R10:38), a user's "information is being exploited a lot, because the more devices you are connecting, every device has some services that require certain information" (R1:36). R2 argues that "people need to have control in any device" (R2:38) to create "flexibility of providing their private information" (R5:38). Meanwhile, R1 argues that:

"...it is important to let people know why we are recording your voice, or what they are using face recognition for. I think transparency is important especially when it comes to IoT" (R1:36).

Despite these arguments, some of the respondents discuss the many opportunities for IoT. For instance, "assurance in privacy opens the door for IoT acceptance among users" (R4:34). Even then, R1 says that "IoT needs to be approached with caution" (R1:36). Moreover, R6 suggests a way to overcome IoT weaknesses as below:

"If I'm using those kinds of devices, they are like recording my sound every time, so I feel it is more disadvantaged rather than an advantage. You can't replace the sound interaction; you can't replace it or do much about the function. The function requires that data. But I think there are products that pay more attention to privacy, products that only record your time and sound if you give permission. Or they record surroundings only and give random sounds" (R6:36).

4.3.2 Advertising based on behavioural Patterns

Companies need to employ the use of advertising based on behavioral patterns to market their products (R2:40). This discussion generated a variation of opinions and responses from our respondents as can be seen in figure 4.

Several respondents agree that it mainly depends on how it is being used. That said, advertising based on behavioral patterns can be a double edge sword (R1:38; R3:50; R4:36; R8:38; R9:42; R12:40). With an account of this, some state that "I hate it and I love it" (R8:38) as well as "intuitive and suspicious" (R9:42). R5 explains that we are inevitable from advertising based on the behavioural pattern and it is a part of our society (R5:20; R5:40). For instance, R5 uses organic search data from Google and she says "we are following them, and we are targeting them just to make sure that they are not keeping that money. They have to spend that money" (R5:20; R5:40). Therefore, R5 argues that:

"I personally believe that we are slaves of capitalism right now. Especially North American culture is based on changing people's minds to make sure that they are spending more money every day. This is happening right now in the whole world" (R5:40). She further adds:

"So, we need their private information, but eventually we use their private information to target advertisements. I'm not sure if that replies to your question, but we all play with specific personal information because we have a large analytics team and there are media paid search teams and they all work with their privacy, actually private information" (R5:20).

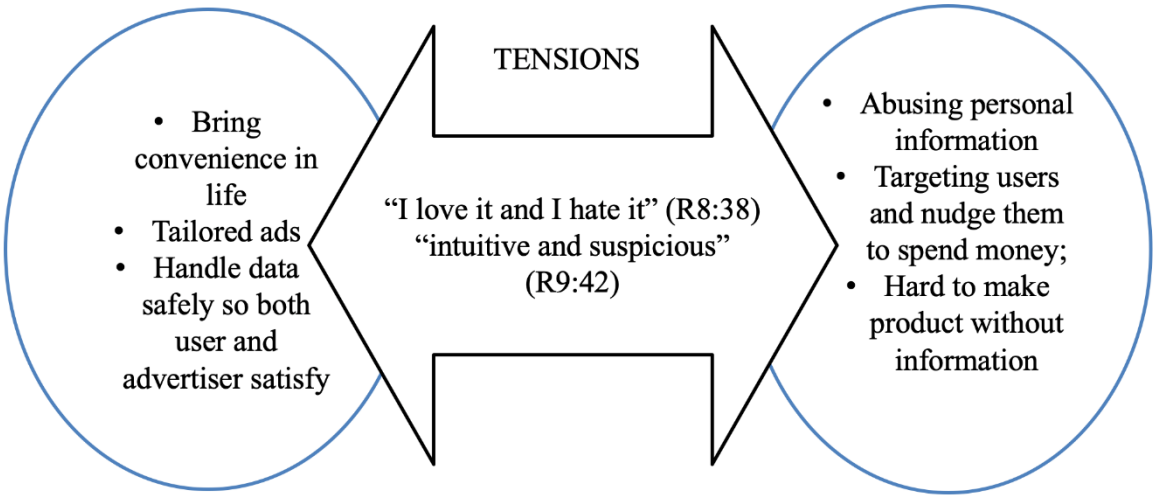

Figure 4: Tensions in advertising based on behavioural patterns

R8 discusses the importance of this phenomenon and makes the following argument: "if we cannot have that information, it is hard to make a product" (R8:38). However, companies need to seek a better way to do it (R10:40; R13:42). Leading to R13's suggestion about how companies should monetize as:

"...low frequency high conversion model, which means you will see one ad that is tailored specifically to you because it's being presented to you as good advice from a trusted friend... instead of a high frequency low conversion advertising model, which is what happens with Facebook or Instagram or Google which is you see a lot of ads, they are personalized and there are many of them..." (R13:42).

Other respondents have a positive perception of the concept (R1:38; R2:40; R4:36; R6:38; R11:42). According to R4, "if these data are handled well, they can prove beneficial for both the user and the advertiser" (R4:36). Meanwhile, R6 argues that "most people are getting used to this type of function and there is no denying it brings a lot of convenience" (R6:38).

4.3.3 Data Analytics

Early considerations to privacy in data analytics would help organizations a lot in the future. This is mainly because new regulatory frameworks are bound to be introduced, the GDPR and the CCPA were only the beginning. Also, people are becoming more aware of how their data

is being manipulated (R1:40). This is one of the insights obtained from R1, a UX designer from Uganda.

Due to nature of the interview question regarding data ta analytics (see Appendix 1), most respondents provide responses related to a proactive approach and finding a balance between data analytics and data privacy by asking users for relevant information (R1:40; R2:44; R4:40; R5:22; R5:42; R6:40; R8:40; R10:42; R13:44). A big part of the privacy concern is related to big data (R4:40). Since data analytics is all about personal information, accessing private information with a proactive approach is important (R5:20; R5:42; R8:40). Moreover, know your limits when you are gathering data (R11:44) and you do not have to collect everything (R12:42). Other responses received are:

- "Data analytics requires information, and if we want to collect that information it needs to be secure first and handled with respect" (R8:40)
- "I think it's hard to know what some apps really are doing with your data, and whether their promises are really reliable promises" (R6:40)
- "If you work with systems and I use the term systems, you sort of have to be proactive because you will create so much work for yourself and it will always come back and bite you later. But it can be hard to be proactive of course, because you can't know everything" (R10:42)

Meanwhile, R13 already developed creative ways to deal with data privacy (R13:44). According to R13, nothing is impossible and there are ways to work around these functionality necessities that often reduce privacy. For instance, it suggested the use of ultrasonic when transferring phone data *(R13:44*). If they had not been proactive, the simple solution would have been to simply use what was suggested by their tech advisor and by every known paradigm of how to create a user database, which would be to use an email. Additionally, when it comes to already established companies, they adopt a proactive approach with the help of a tech advisor that should be "empowered to actively seek out the flaws, proactively seek out the vectors for attack, the potential for the breaking" (R13:44*)*.

4.4 Other Empirical Findings

New concepts were adopted through the qualitative data collection, thereafter, our coding table was improved (Table 7).

4.4.1 Safety with Information Sharing

Many respondents use this concept rather than privacy for benefits to define privacy (R1:8; R2:8; R2:38; R3:52; R4:8; R4:30; R5:8; R5:34; R6:8; R6:12; R7:8; R7:12; R8:8; R9:26; R12:8; R12:32). When users feel comfortable, they offer more data (R4:30; R9:26). Users seek safety guarantee (R6:12) and trust (R7:12). R7 uses points out that he ensures the establishment of user trust to a point where a Non-Disclosure Agreement (NDA) is not required by his clients (R7:8). Our focus is on the safety of personal information of clients and gives them an option to be safe (R5:8; R5:34; R7:8; R9:26). Safety with information sharing concept is explained more precisely as "Important information, valuable information that needs to be shared with only eligible people" (R2:8), "privacy should only be shared with those who will handle it correctly and in a way that will benefit you" (R8:8) and "Privacy is quite broad, but it is an

opportunity for whoever has access to this information to show me as a user that my information is safe and used in the right way" (R1:8).

Some respondents expressed their concern about the safety of personal information shared on digital platforms (R2:38; R3:52; R4:8; R6:8). "It's basically just asking for data and then moving that data from you somewhere else" (R3:52). "I will not be able to control it and my information available there" (R4:8). Also, R6 claims,

"...in China we have a weird phenomenon... It's kind of weird but maybe you don't know that your phone might be recording and collecting data then sending that to different apps that maybe benefit from it. As a user or as a consumer we have a right to know if our privacy and personal information is used by business" (R6:8).

4.4.2 Basic right to be Non-Recognizable

Respondents mostly describe privacy using the concept of basic right to be non-recognizable than the concept about Self-Protection Failure (R2:38; R2:40; R3:8; R4:10; R5:8; R5:34; R6:8; R6:36; R9:10; R10:8; R10:26; R10:32; R12:8; R13:10; R13:12). According to R9 "privacy is something basically something I want to hide which I don't want to disclose to anyone" (R9:10) and "in simple terms, to be able to be non-recognizable" (R3:8). Because "it is a fundamental right" (R12:8). One of the interview respondents, R13 shares an interesting scenario:

"...If I'm rude to a person in a shop and somebody videos me screaming at a shop assistant. Is it my right to prevent that video from ending up on YouTube? ...I'm just using it as a hypothetical but If it was me and I was rude to somebody and it was captured.... Do I have the right to remove …? I do have a right to know about that. I would say that the issue with privacy also gets mixed up with this like right to be forgotten versus Facebook monetizing my data, and they are very different, but they get called the same thing, privacy..." (R13:10).

Furthermore, R6 argues that "If I'm using those kinds of devices, they are like recording my sound every time, so I feel it is more disadvantaged rather than an advantage" (R6:36). And "as a human being that is concerned about privacy, I'm kind of concerned I tend not to share certain information on Facebook and other social channels" (R2:38).

From a business perspective a few argue that "I don't believe that privacy should be that everyone is anonymous all the time, but I think users should be given the opportunity to affect it" (R10:8). An argument supported by R5 when he states: "we have to give another option for them to be anonymous" (R5:34).

Among all respondents, R10 has a strong standpoint. "Our mission is not to gather information that can be linked to a person" because we don't really have much data (R10:26). "In my experience, I haven't seen any reason to collect and use information that would identify you as a person. It is a lot of work behind" (R10:32).

4.4.3 Hire Experts

Hiring an expert would be one of the measures taken in situations when designing a product for a client who cares about privacy (R2:26). However, when GDPR was enforced, the company had to invest in hiring security and privacy experts (R3:10).

The concept of hiring experts was mentioned by some respondents (R1:24; R2:10; R2:12; R2:36; R5:26; R10:16; R11:12; R11:26; R13:18; R13:36; R13:44). With reference to risk and security experts (R1:24; R2:10; R2:36; R10:16; R11:12; R11:26; R13:36), legal (R2:10: R2:36; R10:16; R11:12: R11:26; R13:18; R13:26) and data analytics team (R5:26).

But even so, R13 suggests the creation of a role for a "*data protection officer and give them the power to hire and fire and all of the scary stuff*" as a proactive measure to addressing privacy (R13:44).

Meanwhile, most reasons pointed out to justify hiring experts are:

- Scale of the project (R2:10)
- Because of the nature of consulting business (R11:12)
- Experts have benchmarks that cover everything (R11:26; R13:36)
- Client requirement for assurance purpose (R2:12; R2:16)
- Investor requirement (R13:18)
- GDPR enforcement (R11:12; R13:18)

According to R3 and R10 from Sweden (R3:10; R10:16), security and legal expertise demand increased because of the GDPR enforcement. Moreover,

"...evaluate like the functionality versus like the privacy... I think it got more focused on privacy when GDPR came into play. Then we really had to hire people who oversaw that aspect..." (R3:10) and "...what GDPR did great was that it started to create headaches for everyone. I mean it affects our work in a way that I mean legal wasn't this involved earlier in the process like that definitely changed. Especially when you work with cloud solutions, legal is basically a part of everything. Like when you're planning features. It is there in the process, and they identify areas where we need to call in legal or security teams..." (R10:16).

Finally, R5 talks about expertise from data analytics team and the ongoing battle she has with them because:

"what I do is I'm recommending them to just like remove it but there are some certain aspects that I can't tackle. Like I can't break" (R5:26).

4.4.4 Access Restriction

The last concept introduced by respondents is access restriction. A few of the respondents mention that this practice is worth considering (R3:14; R3:16; R5:12; R5:32; R12:24).

Briefly, access restriction is defined by R3 as "remove or reduce connection to sensitive data" (R3:14; R3:16). When asked about measures taken to prevent privacy breaches, R12 states:

"I know in our company, all the data is super protected, and we have a lot of regulations and it is very difficult to access any databases. There is a big legal department that deals with that. From what I know, internally there is a lot of work with those legal aspects and it is difficult to get access to any information really. Secrecy which is a bit different from privacy is also a big part of our company" (R12:24).

“our IT team is providing some privacy rules but eventually we all use a common server that everyone can access to many folders. The best they can do is, there was a segmentation for specific users. For example, I'm working for only creative documents. I am allowed to see all of them, but I’m not allowed to see admin documents. So, or for example if there's a finance team and they are not allowed to view all documents that they aren't supposed to” (R5:12).

Meanwhile, R5 brings up the access restriction concept by stating that:

“I'm just in the design phase. I don’t have access to user's data. The only moment when I have access is when, let's say that I’m going to conduct a user research like you do. I'm finding specific users and I'm having online meetings. That's the moment when I have access to the data” (R5:32). Similarly, R2 mentions: “Important information, valuable information that needs to be shared with only eligible people” (R2:8).

In summary, these empirical findings demonstrate that the enforcement of new regulatory rules concerning data privacy has impacted the decisions and considerations made by design practitioners when designing products.

In the next section the empirical findings will be investigated concerning existing literature that will guide towards making informed conclusions hence a discussion about future research recommendations and contribution to the information systems body of knowledge.

5 Discussion

In this chapter, we will discuss our empirical findings in relation to the academic literature. Furthermore, this chapter involves the reconstruction of our conceptual framework (Figure 2).

5.1 Privacy Theme

This theme aims at exploring key factors that influence users to share their personal data. For instance, based on the conducted literature review, one of the suggested factors is the expected benefit in exchange for privacy (Section 2.4; Section 2.5). On this account, measures are taken by companies to address new regulatory requirements and how the design of the product is impacted was discussed to explore it further.

5.1.1 Privacy for Benefits & Self-Protection Failure

Privacy for benefits is a concept that regards users offering personal information in exchange for the benefit expected to be obtained (Pavlou, 2011; Wunderlich et al., 2019). As evidenced by our empirical findings, users are not hesitant to share their personal information, hence, the indecisiveness between sharing not sharing information is already solved (R13:34; R9:46). One respondent makes a clear statement, saying “there is no privacy on the web”. Moreover, to effectively utilize a product or a service, it has become expected to share and provide your personal information, and most respondents explained were explaining how to deal with already shared information (R1:8; R2:8; R4:8; R8:8). Therefore, the concept of privacy for benefit is no longer valid to explain our conceptual framework (Figure 2).

The self-protection failure concept expresses an individuals' failure to protect their personal information (Bélanger & Crossler, 2011). According to our empirical data, self-protection failure was the least mentioned concept among respondents, therefore we consider it a sign a non-compatible concept that cannot be further used in our conceptual framework (Figure 2). There was only one respondent who raised the issue and tried to explore that users fail to protect themselves simply because they do not understand privacy and are unaware of how their data is being used (R9:46).

5.1.2 Safety with Information Sharing & Basic right to be Non-Recognizable (Suggested)

Given our empirical findings, user privacy is no longer explained by the privacy calculus since users no longer have control over personal information privacy. However, what matters is how companies are keeping user’s private information safe. Therefore, most respondents often referred to safety in information sharing concepts rather than privacy for benefit.

Based on the above, the previously mentioned concepts of privacy for benefits and self-protection failure from the prevention motivation theory (Lee et al., 2018) are no longer valid in practice. However, the prevention motivation theory needs to interact from a different

perspective based on how to provide safety with already collected private information through the concept of safety with information sharing. Moreover, based on the basic right to be non-recognizable concept, it would be praiseworthy if companies were to provide an option for users to remain anonymous when collecting their private information.

5.1.3 General Data Protection Regulation

"*There was no concept of data privacy, you know back in 500 BC or even in 50 BC when a lot of interesting things were being written about the fall of the Roman Empire. And if we'd had GDPR back then maybe we wouldn't have learned so much about what we know about Rome*" (R13:10).

Cusick (2018) argues that the enforcement of GDPR in May 2018 permanently changed the way an organization collects and uses customer data. This is represented in our findings (Section 4.1.3) as the GDPR emerges as the most known and discussed concept in the privacy theme and the second most popular concept overall. Even though based on the interviews, it is discovered that GDPR is mostly adopted by developed countries such as Sweden, Australia, and Ireland, of which have already implemented the privacy regulation (R10; R13; R11), the enforcement of GDPR brought privacy to everyone's attention (R4:8).

Some companies are trying to be strategic when collecting user data (R1:10), specifically by applying data minimization (R1:10; R10:24). Meanwhile, one of the respondents from outside of Europe's borders, states that the enforcement of the GDPR influenced several changes in product development when it came to design decisions. Essentially, the GDPR put the user in focus, and privacy policies had to be incorporated into the design and clear to the user (R1:16).

The GDPR introduces new responsibilities that required organizations to integrate data protection into every aspect of their processing activities (Gjermundrød et al., 2016) making it the most known privacy protection regulation in the world (R1, R2, R3, R4, R5, R7, R10, R11, R12, R13). However, the integration of data protection into the design is not clearly known to the UI/UX designers who have the responsibility to design the product features that meet these requirements. Meanwhile, the GDPR does not explain why and how one should go about to protect privacy, which creates a challenge in practice. In an attempt to address this issue, some companies set up legal teams who are involved in the decision-making process so that all decisions made are in accordance with the GDPR (R3:20).

Article 25 of the GDPR entitled "*Data protection by design and by default*" communicates requirements for data privacy by design and data privacy by default. In a bid to meet this requirement, most adopted practices by companies represented by the respondents are data minimization through the collection of required data (R10:24; R1:10; R11:32) and allowing customers to remain anonymous (R13:12). However, most respondents are unable to ascertain if they implement this requirement. Meanwhile, R4 and R10 mention opt-out and opt-in options which are part of the data protection by default principle that acts across both GDPR and *PbD*. According to the stated article, companies collecting user data are required to implement privacy by design in its entirety to meet the data protection requirement. On that note, some respondents mentioned that data protection is entirely handled by their legal teams (R10:16).

However, R13 expresses clear conceptualization of article 25 of GDPR when he mentions:

"We couldn't ask our customer upfront. Do you want the private version of our product or the non-private version of our product? Some companies might offer that and say look we're doing the right thing, but we can't even offer that choice to our customers because we have no mechanism to know who they are or store their answer" (R13:34).

This respondent clearly understands both the concepts involved in this requirement, privacy as default, and privacy. Therefore, GDPR is not *PbD*, merely a tip of the iceberg. In other words, it is not the end of privacy. Complying to GDPR does not mean that companies are implementing the full features of *PbD*, instead, they only comply at minimum and least required level as seen in figure 5 below. Instead, by building a culture of privacy, companies would be capable of going well beyond the privacy policies in the GDPR.

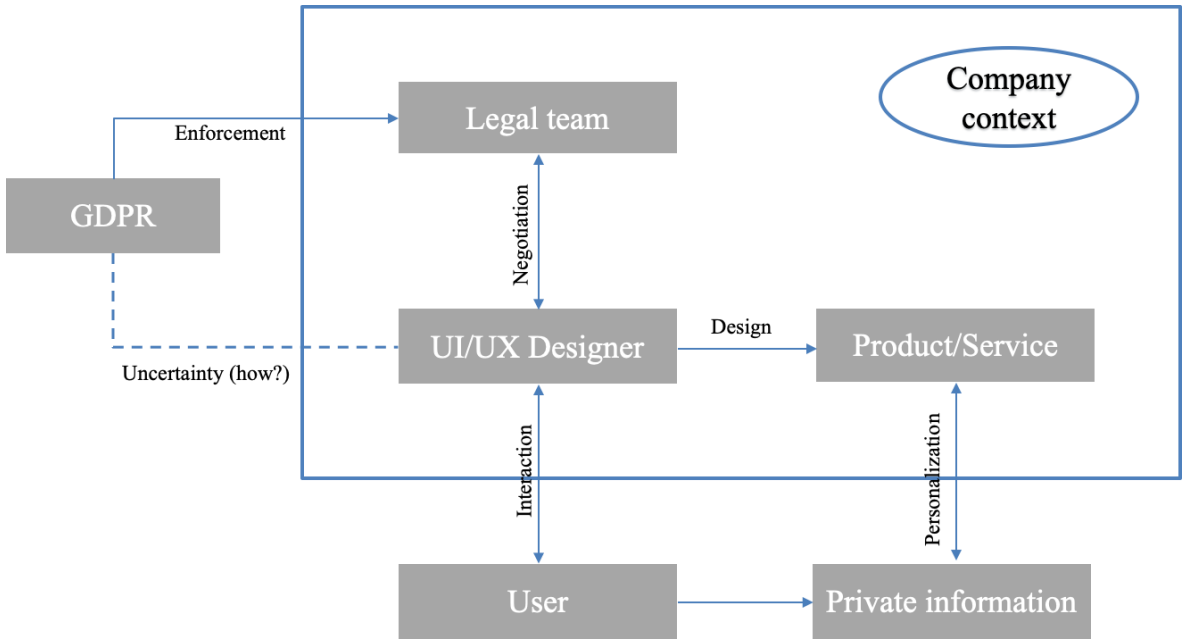

Figure 5: Problems in GDPR enforcement in a company context

Another empirical finding regards to the applicability of the GDPR on newly established companies (Figure 6). According to one respondent it would be easier and more convenient for startups to establish policies following GDPR before the process of data collection, he argues:

"...what makes an interesting point is new organizations who begin today and receive funding or begin with a plan to create a company in Europe are not obligated to be compliant before they get started. They're obligated to be compliant from when data is being collected. So, they need to obtain compliance rather than maintain compliance and it would be an interesting concept to build into the creation of organizations. Are you ever going to capture customer data as a business? Most of them will have customers so the answer is yes. Then okay before you are able to trade as a business, you need to have maintained your GDPR compliance for a period of X days weeks months whatever it is. So that instead of it being this afterthought it is like hey, do you have a tax accountant? Yes, okay. Have you got your privacy compliance in place and is it maintainable? Yes. Okay, you know it'd be table stakes to get into the game rather than this afterthought of like, oh, don't forget we have to also do that thing, you know, I think if they have built-in it would be a lot easier. It would be interesting to build these things into the establishment of organizations rather than it being an afterthought. To create a company in Germany, which is one of our subsidiary organizations, the paperwork was like

two reams of paper of things we had to do and not one of those pieces of paper made sure that we prepared for the GDPR" (R13:18).

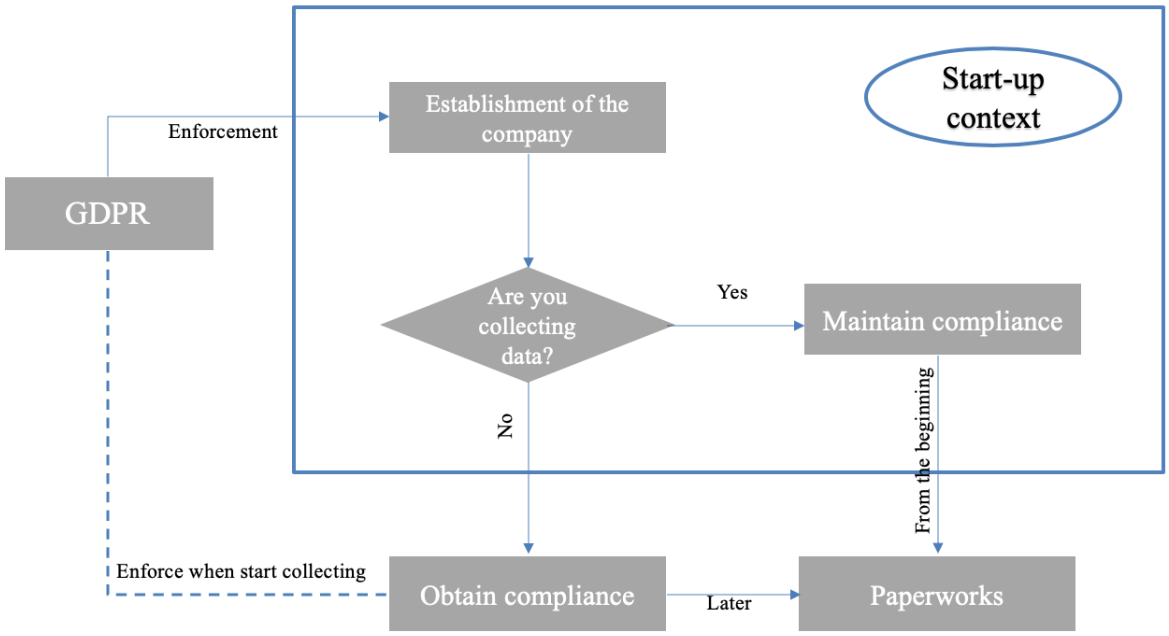

Figure 6: Problems in GDPR enforcement in a start-up context

5.1.4 California Consumer Privacy Act

The truth is, most of our respondents were not aware that the CCPA even existed. Through our empirical study, it became clear that the CCPA is a newly implemented regulation. It should be noted that even though the CCPA was implemented in January 2020, the enforcement date of the regulation remains July 1. However, although the CCPA is seemingly only enforced in California, the impact of the regulation on the rest of the world could be far larger than its European cousin. The state is home to over 2000 tech companies and some of the largest companies in the world, such as Facebook, Google, Yahoo, Cisco, among many others. Companies inside and outside of California are now required to comply with new regulations so that they can continue to do business in the most populous state in the United States.

Many are criticizing the way companies in Silicon Valley are dictating the privacy of the world R2:38; R5:22; R5:26; R9:36; R9:16; R12:10; R12:34; R12:36: R13:10; R13:24; R13:28; R13:34; R13:42). Both Facebook and the Cambridge Analytica data scandal were mentioned several times throughout our interviews. It is no surprise that the CCPA has Silicon Valley shaking in its boots as it will change the reality for many of its companies. Perhaps, the enforcement of the CCPA will provide an opportunity for companies to have their consumer's best interest in mind, thereby changing the perception of both people and governments on many of the companies in Silicon Valley.

5.1.5 Competitive Advantage

According to our empirical findings, there is a strong relationship between privacy and competitive advantage. Many of our respondents find the approach of Apple admirable, as evidenced in our findings, people assume that privacy is something only suitable for larger companies, and only they can start thinking about privacy as a differentiator for competitive advantage. However, R13 strongly believes the landscape is changing, and privacy is becoming more important for all companies, he says, "...we will start to see that it becomes highly valuable that an organization behaves in this way or similar ways. You can start to see it with Apple..." (R13:22). R13 is the founder of "Simby", neither a giant nor a known business, yet they have adopted privacy policies beyond the requirements of known regulations.

Furthermore, as stated by (van Rest et al., 2012), information flows one way: from the data subject to the data holder. Moreover, information is power, meaning that there is an imbalance of power in the relation between the data holder and the data subject which erodes trust. R1 stresses the importance of trust between the data holder and the data subject as it makes the users more comfortable when utilizing your product, he says, "people get a lot more comfortable in the platform and trust you a bit more than your competitors. Right now, the competition has increased which means privacy is becoming more important*"* (R1:20).

Cavoukian et al. (2010) state that, "privacy is good for business" (p. 405). A statement that is further supported by our findings.

5.2 Privacy by Design Theme

The concept of *PbD* promotes compliance with data protection regulations from the earliest stage of initiatives involving personal data. In recent years, the concept of *PbD* has seen adoption by regulators from around the world as an essential component of privacy protection. As stated earlier, *PbD* has been criticized as a vague concept, and the relevant best practices as well as the consequences of adopting it are fairly unknown (van Rest et al., 2012). Following the literature, our findings indicate that the awareness of *PbD* is low. Yet, many of our respondents are trying their best to comply with most of its principles.

However, our results show that there is a positive attitude towards *PbD* and some had already adopted many of its principles. As can be seen in our empirical findings, the most discussed *PbD* principles are respect for user privacy, end-to-end security, and privacy embedded in the design. It is not surprising that RUP is the most frequency principle since UI/UX is all about user engagement, user experience, and by doing what is right by the customer.

5.2.1 Proactive/Preventive

As mentioned throughout the text, privacy has traditionally been approached reactively, jeopardizing the personal information of users (Cavoukian, 2011). According to many of our respondents, users simply do not care about their privacy and do not realize that they are being used as data factories. Although many of the respondents understand the importance of adopting proactive measures, they believe that companies still have a long way to go when it comes to dealing with privacy. When talking about his start-up, R13 claims that they are five years too early (R13:8). Even after the implementation of the GDPR and the CCPA, he believes

that the proactive approach that has been adopted by his start-up might fail simply because they are ahead of their time.

Having said that, several respondents acknowledge the fact that privacy will become an important issue in the next decade as users are becoming more aware of how their personal information is being used. Until now, users have willingly, or unknowingly been lending their personal information to get convenience in return. However, it seems like they are beginning to understand the consequences of this bargain, which is why they are looking to businesses to safeguard their data and hand control back to them.

5.2.2 Transparency &Visibility

This principle translates to ensuring transparency amongst all involved stakeholders when dealing with user data (Cavoukian, 2009; Cavoukian, 2020; Cavoukian & Chibba, 2018). It involves ensuring openness and accountability, but although many UX designers are familiar with the concept, they cannot map it to *PbD*. R1 validates this concept when he talks about the design transformations his company had to incorporate when GDPR was enforced in 2018 (R1:16). He presents an example that is informing the user why specific information is required hence the need to ensure openness when collecting user data. Additionally, other UX designers R3, R9, and R13 extrapolate the extensiveness of this concept by mentioning that it is relevant for a user to know the purpose of why their data is being collected and that it can be deleted on request of the user. However, R6 states that in China there is a contradiction to this concept since there is constantly snooping on users without their knowledge.

5.2.3 Full functionality

Positive-Sum, not Zero-Sum. The full functionality principle aims at encouraging a balance between privacy and other fundamental requirements of a product without trading off any other legitimate interests. (Cavoukian, 2009; Cavoukian, 2020). As evidenced by our findings, this is one of the least adopted concepts of *PbD.* A few UX designers believe that by ensuring privacy one is not trading off other fundamental requirements however, most believe that there is always a zero-sum. Based on the conducted literature in (Section 2.2.1), legitimate interests such as usability should not be compromised. R4 argues that ensuring privacy does not lead to a trade-off between usability and privacy but instead makes the product more usable (R4:26). Similarly, R8 agrees that ensuring that there is no trade-off is possible but only in big companies and specific countries (R8:28). However, from other UX designers' perspectives, privacy is achieved at the cost of usability. Although few UX designers believe that by ensuring privacy, one is not compromising other fundamental requirements, however, most believe that there always is a compromise to be made, a zero-sum (R3:34; R3:46). UX designer R5 mentions that when a UX designer is working for an established company there are many stakeholders involved in a product design and development decision making which often puts the designer in a position that involves sacrificing usability (R5:30).

5.2.4 End to end security

This concept is aimed at exploring the measures that various companies have adopted to ensure data protection of products throughout their lifecycle. According to (Cavoukian, 2009; Cavoukian, 2020), privacy protection follows data throughout its lifecycle. This concept is

addressed by UX designer R8 through a methodology adopted by his company referred to as empathy mapping (R8:30).

Likewise, R1 mentions that his company ensures end to end security by taking responsibility to protect user data on their databases (R1:30). Similar R4 discusses that his company makes use of secure methods of data transfer (R4:12). However, he thereafter mentions the use of third parties with the strategy of transferring the responsibility of protecting user data to third parties believed to offer better security for their users (R4:28).

5.2.5 Privacy as a Default Setting

Privacy as a default setting explores various measures adopted by various companies to ensure address privacy by default. This concept signifies building privacy into products before adding features that enable data sharing (Cavoukian, 2009; Cavoukian, 2020). Most designers that were interviewed argue that it is good for a company to make privacy a default setting (R4:30). A UX designer further argues that companies using cloud services to store user data are not eligible to claim that they ensure privacy as cloud providers do not log Intrusion Prevention Systems (R13:12).

Meanwhile, Gürses et al. (2011) argue that the principles of *PbD* serve as a guideline for adjusting design and implementing privacy requirements with complex social, legal, and ethical concerns. Respondent 13 expresses an opinion that relates to this claim when he argues that a company that cares about user privacy should never provide users with options to choose between a private and non-private version of a product (R13:34). His company Simby, a start-up has a stringent privacy policy that puts a user at the center of product development through the use of measures such as code review to ensure promises that were made to the user concerning their privacy.

Privacy as a default setting encourages the use of data minimization, collection limitation, retention, and disclosure limitations as data collection techniques (Cavoukian, 2009; Cavoukian, 2020). R10 uses and advocates data minimization as a measure to protect user data and to prevent privacy breaches (R10:24). Furthermore, R10 suggests the organization of workshops within the company and the use of templates with important business metrics (R10:28).

On the other hand, R11 uses the use, retention, and disclosure measure by collecting data for a specified period, and thereafter discarding it (R11:34). Moreover, R13 employs the collection limitation measure by only collecting what is required to make the product function, while intentionally anonymizing it (R13:12).

In a parallel argument, a few respondents do not agree to this concept while some argue that they do not visualize how privacy can be built in a product as a default setting (R11:36; R9:36).

5.2.6 Privacy Embedded in Design

Privacy embedded in design is a concept that translates to the incorporation of privacy into the design, the architecture of IT systems and business processes. According to Cavoukian (2009), privacy should be holistically embedded in the design, and not bolted on as an add on**.**

Respondent 8 points out that due to the constant innovations brought about by technology, prioritizing privacy by implementing it in the design would build confidence among users when interacting with a given product (R8:36). Additionally, R1 supports that claim that embedding privacy by design is essential (R1:36).

5.2.7 Respect for User Privacy

One of the important concepts of discussion associated with *PbD* is respect for user privacy. A concept aimed at exploring the measures taken by companies to ensure that the user is placed at the centre of design). This concept requires designing human-machine interfaces that are user-centric, human-centred, and user-friendly which are considered to facilitate easy and reliable decision-making concerning privacy (Cavoukian, 2009; Cavoukian, 2020). Two respondents were confident about their company actions towards respect of user privacy (Apple and Simby). R13's company Simby had the strongest maturity on *PbD*. Moreover, with a strong standpoint as below:

"we had a big fight with one of the potential investors because they offered us a lot of money to build this and launch this because it was the first of its kind but they wanted us to remove that promise and I said, this is a promise that once made cannot be broken so I would have had to shut the company down" (R13:28).

Additionally, at Simby, attention to detail is keenly observed when communicating terms and conditions using a huge font that portrays the message to the user clearly (R13:20). Similarly, R6 supports the use of right fonts for better visibility of policies (R6:34). However, R2 argues that user-centricity is prioritized in cases where the budget allows (R2:18). Meanwhile, R4 and R10 point out the use of opt-in and opt-out options as a way of enabling the user to withdraw consent at any time (R10:10; R4:24). Hence addressing the consent requirement that concerns empowering the user's right to withdraw their consent (Cavoukian, 2009). Access Restriction

Based on our empirical findings, this practice was suggested by some respondents. Meaning "remove or reduce connection to sensitive data" (R3:14; R3:16). According to Cavoukian (2009), access restriction considered as one factor of Privacy as a Default principle by an organization should limit the ways it uses, discloses, and retain personal information. On the other hand, access restriction is a real-life practice adopted by safety with information sharing concepts mentioned in the privacy theme by "Important information, valuable information that needs to be shared with only eligible people" (R2:8). According to respondents, access restriction referred to as an internal privacy policy rather than enforced privacy regulations. Also, respondents accepted access restriction as a casual proactive approach within the company. Therefore, due to duality nature and uniqueness in practice, we coded access restriction independently. But in the conceptual framework (Figure1), access restriction would not impact.

5.3 Technology Theme

This theme aims at exploring effective measures that can be taken to prevent privacy breaches associated with IoT, data analytics, and the use of advertising based on behavioural patterns. Cavoukian and Chibba (2018); Chanson et al. (2019); Culnan (2019) point out that ensuring data privacy in regard to new complex technologies such as data analytics, advertising based

on behavioural patterns and cumulative use of IoT devices is not self-evident, a concern validated by most respondents as discussed in the respective concepts below. In account to this, our respondents argue that a proactive approach to managing privacy, by embedding and making privacy a default setting of a product would be the best approach when dealing with such technologies.

5.3.1 Internet of Things

An important area of discussion in regard to technology is IoT. This concept aims at exploring privacy measures that companies have established to address privacy concerns associated with IoT. While many IoT devices have tangible benefits for users, they also provide opportunities for unauthorized users to exploit vulnerabilities. Given the discussions around the impact IoT has on privacy (Cavoukian & Chibba, 2018; Chanson et al., 2019; Culnan, 2019), this relation is explored by obtaining respondent's opinions about the concept and asking them how they deal with the privacy of devices using IoT.

According to Wunderlich et al. (2019), privacy is one of the important motivational factors in the adoption of IoT technologies. Although several benefits of IoT was acknowledged by our respondents, they highlighted the importance of dealing with IoT with caution. R6 provides an example of a creative solution when dealing with the privacy of an IoT device, he says:

"If I understand it correctly. If I'm using those kinds of devices, they are like recording my sound every time, so I feel it is more disadvantaged rather than an advantage. You can't replace the sound interaction; you can't replace it or do much about the function. The function requires that data. But I think there are products that pay more attention to privacy, products that only record your time and sound if you give permission. Or they record surroundings only and give random sounds" (R6:36).

Following his concerns expressed around the uncertainty created in relation to privacy when using IoT devices, R6 further argues that a UI/UX designer would play an important role in the successful adaptation of an IoT device. Furthermore, this argument is supported by other respondents, and due to these concerns, most designers argue that embedding privacy into the design of IoT devices and making it a default setting would be an effective approach in trying to prevent privacy breaches.

5.3.2 Advertising based on behavioural patterns

This concept is aimed at exploring the relationship between privacy and advertising based on behavioural patterns. Respondents are asked to provide their perceptions about this phenomenon and how privacy should be addressed by companies advertising products based on behaviour patterns. Many companies use this technology as validated by the fact that most of the respondents had either experienced or built a system that uses advertising based on behaviour pattern to market products.

Based on our empirical findings, respondents had divided opinion when it came to their perception of advertising based on behavioural patterns. Some were positive about it and considered it to be essential, while others only considered it to be a violation of trust and a lack of respect in relation to its consumers. While R6 understands the negative aspects of advertising

in this manner, he still finds it convenient (R6:38). Additionally, R4 argues that if correctly managed, it may prove to be beneficial for both users and advertisers (R4:36).

Based on a built behaviour profile, Kagan and Bekkerman (2018) recognize the ability to predict behaviour based on online activity as a powerful tool used by companies to market products. Although acknowledged by R13, he suggests a better model as:

"low frequency high conversion model, which means you will see one ad that is tailored specifically to you because it's being presented to you as good advice from a trusted friend, instead of a high frequency low conversion advertising model, which is what happens with Facebook or Instagram or Google which is you see a lot of ads, they are personalized and there are many of them" (R13:42).

This is a model described using a theoretical concept referred to as personalization benefits (Karwatzki et al., 2017; Sutanto et al., 2013a). According to Mandal et al. (2017) targeted online advertising leads to privacy concerns as it is characterized by massive collection and transfer of data. R2 provides a notable example of a privacy breach that occurred as a result of advertising based on behavioral patterns, he says:

*"*The pregnant girl was hiding that she was pregnant, but apparently Target or Amazon through online cookies and online advertises, the algorithm found out that she was pregnant. And they were sending her the baby products to their address and eventually the father found out*"* (R2:40).

The privacy concerns related to this type of advertising is acknowledged by many, nevertheless, they claim that it is an effective way of advertising products. However, R5 disagrees, she has a different perception of advertising based on behavioral patterns mainly due to the risk it infringes on a user's privacy. Working for a company that thrives on such a marketing model has made her reflect on how it violates the trust of individuals and how it puts their private information at risk (R5: 40). This concern is shared by R4 who suggests that advertising based on behavioural patterns must be treated with caution, regardless of the fact that a user actually might benefit from the targeted ads (R4:36).

5.3.3 Data Analytics

Even though "data is the lifeblood of the new economy" (Cavoukian et al., 2010), companies excessively collect data simply because they can, making it difficult to protect that data (Davenport et al., 2010). As a response, companies searched for preventive measures in order to deal with privacy breaches (Sun et al., 2016). According to our empirical findings, the enforcement of the GDPR made them realize the many benefits of strategic data collection, and how it provides an opportunity for better privacy protection. Accordingly, their focus shifted from data gathering to data protection. Data analytics is heavily reliant on data collection, and in order to protect that data, the appropriate security measures must be in place.

5.4 Critical Success Factors/ Other findings

5.4.1 More collaboration/Hire experts

There are many ways to improve organizational accountability for privacy protection, however, the most powerful and effective one is a collaboration between regulations, technologies, and business stakeholders (Cavoukian et al., 2010). This was clear in our interview as several respondents had already mentioned the importance of collaborating with risk, security, and legal experts when developing privacy policies. R1 discusses the importance of the participation of all stakeholders, he says: *"*When it comes to revolutionizing privacy, I think the first question you need to ask yourself is: Who is the first person or body to involve if you want to ensure that privacy is a main concern. The answer is, I think when it comes to enforcing a privacy strategy, the involvement of an organization's management is essential. All the participants in the value chain need to be involved and onboard with*"* (R1:42).

As indicated by our empirical findings, design practitioners do not control the decision-making process. However, we believe design practitioners, and UI/UX designers, in particular, plays a crucial role in helping companies successfully complying with new privacy protection regulation as well as implementing *PbD* in practice. Instead, companies are simply blindly confirming whatever is suggested by legal teams or known paradigms instead of seeking creative and innovative solutions. Corporate UI/UX designers do not directly face privacy regulations because they are consulted by their legal teams and required only to comply with regulations at a bare minimum (R3:10; R10:16). *PbD* offers an opportunity to better embedded privacy in the system. Therefore, a collaboration between designer practitioners and legal teams are required to successfully implement better and more creative privacy practices.

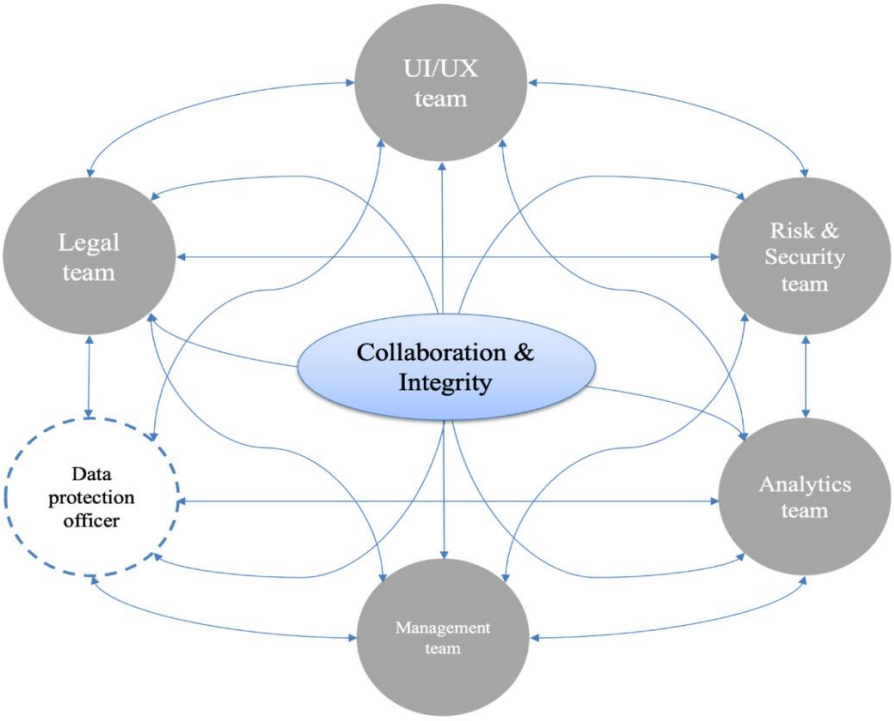

Figure 7: Collaboration & Integrity

According to the GDPR and our empirical findings, we can conclude that a Data Protection Officer (DPO) is required to incorporate context. According to GDPR (Article 25), some organizations are required to have a DPO. The position is further explained in the GDPR: "The controller and the processor shall ensure that the data protection officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data" (GDPR, Article 38).

The importance of a DPO is further evaluated by R13 who discusses the privacy protection efforts of already established companies. He argues:

"I think it can be implemented in companies that are not new as well, but they have to create a role of a data protection officer and give them the power to hire and fire and all of the scary stuff" (R13:44). Against this background, DPO is placed in the collaboration (Figure 7) to ensure better privacy practices.

5.4.2 Socio-economic condition

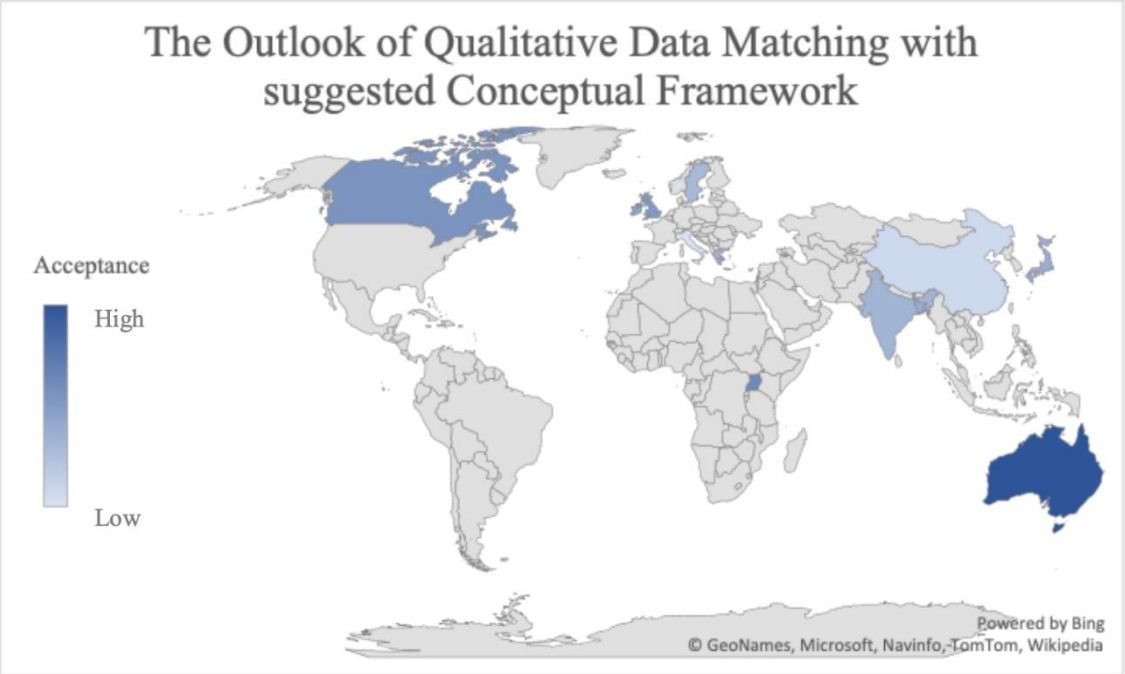

Figure 8: Outlook of qualitative data matching with the suggested conceptual framework

We prepared an illustration of the outlook of qualitative data matching with our suggested conceptual framework (Figure 2) based on the respondent's geographical location (Figure 8). The acceptance level of *PbD* varies from country to country and there is a different maturity level among respondents which is explained by both academic scholars and design practitioners. According to (Wunderlich et al., 2019), "socio-economic status" plays a critical role in being aware of user privacy (p. 675). Furthermore, one respondent said,

"In my experience, I have seen that only big corporations are able to maintain privacy because they really focus on that. But in other countries, such as third world countries, they are not investing much money on privacy" (R8:28).

Respondents from developing countries and freelancers are less inclined to develop the privacy protection practices described by the *PbD*. Furthermore, we noticed a difference in attitude towards privacy protection be between UI/UX designers and freelancing UI/UX designers. The freelancers were less bothered with privacy regulations as their clientele are mostly based on individuals and small or medium businesses.

5.5 Summary of Contributions from Practice to Research

Safety with Information Sharing & Basic right to be Non-Recognizable was more precise to define the privacy rather than the theoretical concepts that described it as self-protection failure and offer privacy for the expected benefit (Self-Protection Failure & privacy for benefit) (Figure 10).

Moreover, our findings prove that the seven foundational principles of *PbD* are adopted at various acceptance levels.

Figure 9: Word cloud of Privacy by Design 7 principles current state of adoption in practice

Finally, we found that the integration of design practitioners, security, and legal experts are essential when attempting to implement *PbD*. In reality, there is a one-way stream when enforcing privacy regulations and we found that the GDPR does not contain clear guidance about implementation, but rather what to fulfil.

Privacy is a movement and GDPR is a trend, "it is movement towards a world where people are more empowered to take control of information about themselves" (R13:10).

Moreover, we found that some respondents had already met certain aspects of *PbD* to meet the new requirements of regulatory frameworks such as GDPR. However, the phenomena of *PbD* is still rather unknown to them. Therefore, we suggest informing design practitioners to the right academic term by promoting *PbD* study and published articles so they could contribute more in the practical study alongside academic scholars.

Suggested new conceptual Framework

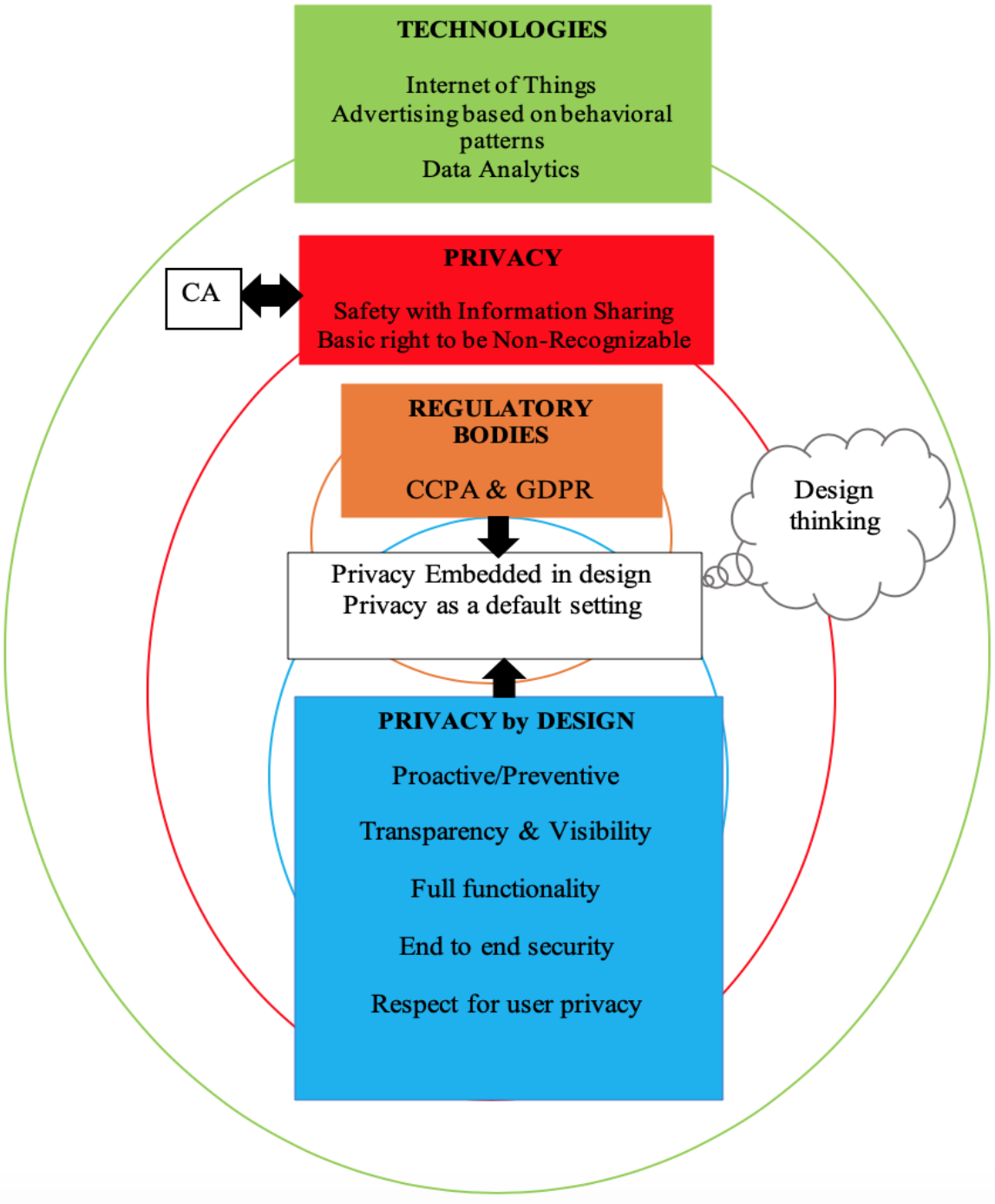

Figure 10: Suggested conceptual framework

6 Conclusion

This section provides a summary of the main findings of the study as well as its interpretation. Lastly, suggestions for further research emerging from the implications of the study's findings are presented.

6.1 Research question

This research set out to identify the privacy protection measures that have been adopted by companies in order to implement *PbD*. The concept of *PbD* is often criticized for being vague. However, following new data protection laws, companies are required to adopt its principles and implement the correct security measures to comply with these regulations.

We aimed to reach a conclusion, by attempting to answer the following question:

"*What practices do companies adopt to implement Privacy by Design?*"

6.2 Key Findings

In this study, several qualitative interviews with UX/UI designers from all around the globe were conducted.

Although we can conclude that *PbD* is a relatively unknown concept among most respondents, there is a positive attitude towards the idea of weaving privacy in the very fabric of systems, business processes, and design specifications. In particular, the utilization of data minimization is emphasized as a necessary safeguard that protects the rights of data subjects. It has become evident that many companies collect data and personal information simply because they can, leaving large databases as attractive targets for data thieves. The rapid rise in our ability to collect data has not been matched by our ability to support or manage it. Conversely, data that has been deleted after serving its purpose cannot be exploited. Thus, in compliance with the GDPR and the CCPA, data minimization is identified as a key element in order to successfully implement *PbD*. Furthermore, the ability to ensure that the data collected is retained only for the minimum time necessary to accomplish the predefined purpose is especially important in the context of IoT and data analytics.

Our empirical data suggests that the GDPR and its privacy by design requirements have introduced new operational challenges for organizations. Nevertheless, the regulation has provided an opportunity for companies to build trust with consumers by offering visibility and transparency. Moreover, our research shows that being transparent is a powerful thing. By empowering users to make decisions about their personal data and by taking the time to inform them of what is happening companies will be better able to rebuild trust. As evidence by our study, at least two benefits are derived from the implementation of *PbD*. First, the user is assured strong privacy over their information, and secondly, companies gain competitive advantage. Trust has become an important asset in the digital ecosystem as customers are now on the lookout for companies who have demonstrated commitment to maintaining privacy.

Additionally, we can conclude that successful implementation *PbD* requires collaboration and integrity between all stakeholders within the company, specifically design practitioners, legal teams, security teams, and management. Although *PbD* is a rather complex approach, in practice it can be implemented by simple solutions such as access restriction, which implies removing or reducing the connection to sensitive data. Human errors are often an overlooked cause of privacy breaches, therefore, PbD requires a user-centric approach where design practitioners seek to understand the needs of users. Suggestively, this can be addressed through empathy mapping.

The original goal of *PbD* was to develop best practices that ensured that designers were building privacy into their services from the ground up. Today, these best practices have become a legal requirement and a growing business requirement for success in the twenty-first century. However, for many companies, the data privacy effort may seem onerous and distract from more strategic activities. Unfortunately, many build their businesses around data mining and data analysis and are therefore rather reluctant to adopt *PbD p*ractices. As these regulations are changing the way data is handled, companies tend to regard privacy as a regulatory burden, therefore, they focus solely on mechanisms of compliance. But merely complying with the GDPR and the CCPA is not enough to implement the principles of *PbD*. Compliance is a continuous process of change, not a singular effort like drafting a data privacy policy or developing a position for a privacy officer. Instead, *PbD* is about transforming the culture at scale across the organization, which regardless of size is a big challenge for any company. To successfully address the issues of privacy and security in digital development, privacy culture must be an essential part of an organization, and a holistic *PbD* approach should be the basis of that culture.

6.3 Future research

The findings of this study diverge from that of the majority of previous research of the area, therefore, we have explored possible interpretations of its result in order to provide a basis for further research into the subject. As *PbD* has been criticized as a vague concept, additional future studies on the subject should address specific ways to implement the principles of *PbD*.

Today, privacy matters more than ever, from both a user's and a researcher's perspective, we all want to see future implications of privacy studies. We hope this research will become the first step in studying the implementation of *PbD* from the perspective of a design practitioner since they are the ones who are capable of crafting *PbD* into a system. Since this study only includes 13 participants from 12 different countries, we suggest conducting future surveys that cover a broader range of subjects to acquire additional insights.

Additionally, the subject of *PbD* requires a future collaboration between interdisciplinary scholars such as security scholars, privacy scholars, human-computer interaction scholars, and design scholars.

Appendix 1: Interview Guide

Introduction

1. Before we proceed, do you mind if we record this interview?
2. Can we use your full name and company name? Or do you wish to remain anonymous?
3. Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?

Privacy theme

4. How would you define privacy?
5. In your experience, when is privacy implemented in product development?
6. What does your company do to make sure that the right privacy protection practices are in place?
7. Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?
8. Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?
9. Does your company make privacy regulations easy to understand for users before they consume your product or service?
10. Do you see any competitive advantage in your business while you provide better privacy in your product or service?

Privacy by Design theme

11. Are you familiar with the concept of Privacy by Design?
12. What measures do you take to prevent privacy breaches?
13. Is your company transparent about the information you gather, and do you give customers control over their personal data?
14. In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?
15. Which design measures do you have in place to ensure full data lifecycle privacy protection?
16. What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?
17. Do you think there is a trade-off between completing core functionality and embedding privacy in the design?

Technology *theme*

18. Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?
19. What is your perception about the use of personal data for advertising based on behavioural patterns?
20. How important is a proactive approach towards privacy in data analytics?

Closure

21. Do you think there is anything relevant to the subject that we have not discussed during this interview?

Appendix 2: Interview Transcript (R1 Uganda)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R1	Sure	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R1	I do not mind, the thing is, there might be certain information I cannot disclose.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R1	I think this is my fourth year as a UX designer, exclusively UX design. But as a design practitioner I've probably worked 6 years. My very UX experience was when I joined my first company, and it was a very big privilege to work there. There was a very diverse culture there which meant I got to learn a lot and it gave me a very good introduction to the field. Now I am at another company, where I have a different kind of project.	
7	I	How would you define privacy?	
8	R1	To me, privacy is an opportunity for anyone, platform, service or individual to have access to my information, the one I am comfortable to share, and also explain to me what this information is going to be used for, where they are going to keep it, how long they are going to keep it. Also, how you exploit me, because of things I don't know. Privacy is quite broad, but it is an opportunity for whoever has access to this information to show me as a user that my information is safe and used in the right way. In my experience a lot of apps and services, a lot of them don't consider privacy, and to be fair people don't really care much. So that is an area they exploit. No one reads terms and conditions; a lot of businesses are taking advantage of that. I think there is an interest from certain legal aspects from the governments who want to look into privacy.	SIS
9	I	In your experience, when is privacy implemented in product development?	
10	R1	Let's say we are building something from scratch, I think the very first point that should be considered is what	

		information is required from the user, what information is absolutely necessary. And if we require information from the people, we also need to think about which information we can do without. And when we don't need the information, we can remove it. Like for instance, if someone is required to create an account, do I need both a phone number and email or can I do without one of them? We need to think about which information is really valuable for us. We need to think about permissions as well. Also, we have to think about legal things right away, because they affect our development. I think it is important that people have a way of handling information. We need to be strategic when we ask for information. These are things we should think about before we even think about developing a product.	GDPR PP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R1	I think I can answer that better with my previous company. Initially, we had the approach of everyone else, where we asked everyone for every information. But when we needed to launch a product in Nairobi, it opened up our eyes a lot. Because unlike Kampala, they had already had some legal policies to handle privacy and information. So, when we were launching our product in Nairobi, we realized we had to modify certain aspects of our application. Simply, privacy needs to be adapted depending on where you are. Earlier, one of the things we used to hide in apps were the privacy policies. They were there but you needed to scroll to find the policies and the terms of use. That was hidden information, really hidden. But in order to get into Nairobi we needed to make sure that information was clear for the user and in his face immediately. Now instead, we put in the sign in page, so every time you login you see those links to privacy. There were also times where we made short videos explaining what all the terms and all the long documents meant. So, to summarize, the terms and conditions are very long yes, but it is the way it has to be. What you can do is to try to create some kind of video or walkthrough that describes the most important things in the terms and conditions. Like for instance, let people know what happens to the information and let them know it can be removed if they want to. The terms are too long, but it is the nature of them, the problem is they can be used to exploit people because no one reads them. The least you can do is to provide some ideas of what will happen to the information.	RUP TV

13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R1	I know GDPR, I don't know the other one.	
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R1	Yes, very much. I don't know exactly how it affected me, but I remember the conversation about GDPR. But it was around that time, 2018, we started exposing privacy policies and making them clearer to the user. Before terms and conditions were separated from privacy. Now they have become connected. The application we had was country based. So, it varied from country to country because there were different policies. I think, before, we didn't really worry about what information we asked for, we could ask for anything we wanted, and it was easy to get information because in my experience the average person really doesn't care. Before you would ask for information and permissions whenever you want. And you wouldn't care why you asked for these permissions. What really changed after GDPR, for the better I would say is that you had to explain to users why you needed certain information. Also, the feature of having users being able to remove their information is implemented now which is important and in accordance with GDPR.	GDPR, RUP TV
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R1	I think generally, the answer is no. It has not been common in the locally created applications. Now it is becoming more common and the conversation is there. But legal documents in their nature are too long, so it is tricky. Here we have the advantage of people not caring about giving their information. I think we can improve how people share their information but addressing the whole legal stuff when it comes to privacy is quite difficult.	RUP
19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R1	I think so very much because people get a lot more comfortable in the platform and trust you a bit more than your competitors. Collecting information is one thing, but managing information is another thing. And if you don't have those privacy scandals people get a lot more	CA

		comfortable. Right now, the competition has increased which means privacy is becoming more important.	
21	I	Are you familiar with the concept of Privacy by Design?	
22	R1	I am not, I think I understand the fundamentals though.	
23	I	What measures do you take to prevent privacy breaches?	
24	R1	This is not a department I took much place in because it is a bit technical. One of the areas that my last company invested a lot in was fraud. A lot of resources were dedicated to managing fraud. There were also a few consultants that were brought on to handle cybersecurity. I don't know exactly what they did because it is very consultant, but they spent a lot of time making sure the users were comfortable.	HE
25	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
26	R1	I would say, yes. To some extent yes. The thing is, the information is there for sure, but the process of accessing it is not as easy. But it is there, and we are transparent. My opinion is, the users should be able to access their information, but taking it out should be a more difficult process. It is tricky.	TV
27	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
28	R1	In my opinion no, I think it's good to mind about people's privacy on your platform. Like often you think about just collecting a lot of data, but it is very easy for this to backfire, in the event of the people that you are collecting data from realize that you are exploiting them. This approach is a bit aggressive, but if you try to gather information in a more respectable way people will be more comfortable.	RUP
29	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
30	R1	I think when the data is with us, in our database, it is our responsibility to protect it. To ensure that people feel comfortable and confident that the information is safe. That we don't abuse it or sell it. It is also our responsibility to make sure that if people want their information gone, we will respect that request. When it comes to measures, that	EES

		is probably for someone more technical, but I think most of the measures are not really visible.	
31	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
32	R1	I think it is very good. By default, your systems not only become more secure, but people will feel more comfortable as well.	PDS
33	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
34	R1	I think there is a trade-off. You are a business, and when you launch a product you have goals and projections which you need to meet. If you do it the right way, and you embed privacy during the process, you probably won't get where you want in time. But it is also like shooting yourself in the leg when you know these things are going to come back and bite you later. I think it requires some kind of balance where you need to balance both core functionalities and privacy requirements. You need to seriously consider what privacy measures you have to put in directly. You can't completely rule out privacy, but you can think about which privacy requirements are the most important and implement them gradually. I think there is a trade-off, businesses have targets and often they compromise privacy requirements, but I think what they can't do is completely ignore all privacy but it is simply postponing an eruption, postponing your problems that will probably result in a larger cost than if you would put effort into it earlier.	FF
35	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
36	R1	I think so yes, especially when it comes to IoT. I think IoT is an area where your information is being exploited a lot, because the more devices you are connecting, every device has some services that require certain information. So, you are sharing more information. I think IoT needs to be approached with caution. When we talk about these services that extensively require your information in order to provide a better experience, I think it is very important to let people know what is happening. I think IoT is good, but there is more they can do. I think it is important to let people know why we are recording your voice, or what they are using face recognition for. I think transparency is important especially when it comes to IoT. I think it is important to embed privacy by default but make it more	PED, TV, RUP IOT

		useful. Giving me steps to consent to something is one thing but explaining why I need to consent is another. I think they can do more there.	
37	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
38	R1	I think it is important. It is good to get personal data about people so you can customize their experience and make them feel very personable. It makes them feel important, feel special and feel in charge. But it should also be done in caution, just because you have my information it doesn't mean you should exploit me and make me try to buy things I am not looking to buy. When it comes to this question, I am on the edge. I think it is quite genius, and it is quite good sometimes, but it doesn't take away the fact that you have played me. So, it is important, and it drives business, but it should not ignore the fact that people can get angry and react.	ABP
39	I	How important is a proactive approach towards privacy in data analytics?	
40	R1	I think it saves you a lot of bad experiences, and a lot of headaches in the future. If you think about it early, ultimately GDPR and CCPA is just one thing, but regulations are going to increase because people are becoming more aware of how their personal information is handled. It is just the beginning; every country is going to implement these laws. And when they implement it, and your organization has been exploiting the personal information of users, it means you have to go back and invest resources to clear out your system. So, the earlier you do it, the better for you, and it means that people's trust in you increases. And trust is very important, if people feel comfortable on your platform, they will come back. People have come aware of the fact that people are exploiting their data, and they are tired of it.	DA, PP
41	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
42	R1	When it comes to revolutionizing privacy, I think the first question you need to ask yourself is: Who is the first person or body to involve if you want to ensure that privacy is a main concern. The answer is, I think when it comes to enforcing a privacy strategy, the involvement of an organization's management is essential. All the participants in the value chain need to be involved and	TV

		onboard with the process, investors, management and so on.	
43	I	Thank you for your time and stay safe! We really appreciate your contribution to our research.	

Appendix 3: Interview Transcript (R2 Japan)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R2	For academic purposes, absolutely!	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R2	Yeah, why not as long as it is an academic paper.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R2	I work as the UX/UI also as a graphic designer. I based in Tokyo, Japan. I've been working as a freelancer since 2016 so it's been four years. Before that I used to work as an employee of the agencies or the companies but similar roles since I was a developer at first and then I was a web designer.	
7	I	How would you define privacy?	
8	R2	Important information, valuable information that needs to be shared with only eligible people. Who has permission to have access to that information? That's what I would say would be my definition of privacy.	SIS AR
9	I	In your experience, when is privacy implemented in product development?	
10	R2	Yeah. It depends on the scale of the project for my experience. If the product you know is only for small segments, a small target of people then probably we will put less importance on privacy. And if it's like a big project or existing project with let's say 10,000 users or so, then it would be different. The team will probably have someone knowledgeable in security, privacy and in any legal issues. And we need to hire those kinds of people, you know, because of the scale of the project. In terms of the process of the when we will implement privacy it also depends on the scope of the project the scale of the project if it's a small project like if it's like, let's say a website for my friend then I will probably just go ahead and use the common generator or template for terms of use and privacy. I'll just replace the placeholder with my friend's company or my friend's name. That would be it, that would	PP, PDS HE PP, PDS

		be at the very end because we are less concerned about it, unless my friend is really into privacy. Other than that, if it's a big project, again, we need to probably think about privacy and security in many pretty much all the phases, starting from the wireframing, starting from the sketches, even starting from the concept, you know. Idealism, from the time we talk about the concept of a product even. So, as thoroughly as possible	PP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R2	Well as I don't own a company I work as a freelance designer. I would be a private business owner, right? So, it would probably be different from a company. For me, I make sure I implement, you know, all the minimum requirements. Based on the common, you know standards and guidelines, you know, I try to like for instance the EU recently, they forced all the websites in the world to have the cookie policy, you know. So yeah, so everyone started doing it. I would probably do the same way. It depends on whether it is one of those standards that needs to be implemented or commonly recognized. Then yeah, I would do it. But otherwise if it's not, you know that needed or commonly recognized privacy guidelines, then I would probably skip it because it just adds more time. Well, unless the client has the requirement to have, you know solid guidelines requires the privacy to be well done and correctly executed then I would probably find or hire some expert in that area to collaborate on this project.	GDPR HE
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R2	Not in details to be honest. To be honest I do not know about the details GDPR. I know because I recognized the acronym, but not in details. Basically no, it doesn't ring a bell.	GDPR CCPA
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R2	I do not even know when it was enforced, so there is no difference in my experience.	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	

18	R2	Again, it depends on the project scale of the project, I might just copy and just replace the placeholder with some names. Sometimes if the budget, time and the client allow, you know, cares about them. Then I would definitely think about it to make it easier. For instance, I like the way that Google does with their privacy terms. When they change the terms, we receive emails. We receive emails saying that this is what we changed and it's super easy to understand. And you don't have to go and click and read whole terms of agreement. No one does.	RUP FF
19	I	Is that common or just Google?	
20	R2	Not many companies do but recently the bigger companies definitely do. To make it easier for people to understand about privacy and the terms.	RUP
21	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
22	R2	For my case. No, it doesn't make any difference. Well in my case, the way I work, the way I get a job or project is basically there will be companies or clients who will find me directly to work with me, but most of the time there are digital agencies or companies marketing companies that would contact me because they have a specific need on their specific project right? So, they would need a UI designer or UX designer to this part of their project. but they oversee the privacy of the product or all privacy and security and they talk with the actual client, so I don't talk about that. That's my case. I'm not sure. For me, no. by saying that my answer would be different as an end user. And as a human being I would definitely increase my trust in the brand if they would provide better privacy in their products.	CA
23	I	Are you familiar with the concept of Privacy by Design?	
24	R2	No, sorry.	
25	I	What measures do you take to prevent privacy breaches?	
26	R2	Depends on the project. Well the most effective thing I would do would be to talk with the client or the whoever asking me to do the certain work to think about the privacy and talk about the importance of privacy. And if they really care, if they think it's important, then we might hire an expert or hire a certain company to do that part because I cannot do that. So that's the probably most important way to do it, I guess.	HE

27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R2	Again, it depends on the project. Depends on the budget and the requirements and actual client's preferences on how much time and budget they would allow, you know. It's not up to me to decide. If they don't want to spend any time on that then we'll probably must generate most of it, copy paste type of stuff. But let's say we would have an app with thousands of users, then it would probably be different. You know, it will be different and I'm willing to if there is a budget, I'm willing to make it transparent and allow the users to have certain controls over what kind of the information they share.	TV FF
29	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R2	I don't think so. I don't think the privacy settings would really affect the usability Most of the time It's just the apps or the services that have it, or don't have it. You know, that's the only difference and of course having is always better. I don't recall any examples where privacy would interfere with the user experience. I don't think so. I've never seen those kinds of scenarios.	FF
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
32	R2	I'm not sure honestly	EES
33	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
34	R2	Okay. Yeah, I think it's good because the common user would probably press the button either way. I'm pretty sure there is research data saying that most people would press a button if the sign said that your privacy is safe with us. Yeah, people would definitely do that. So, I think the best way to do it would be to do something in between. Inform in the easiest possible way. Convey in a short and simple form, convey important information only without you know, showing the whole two or three pages of terms and conditions or privacy policies and stuff. It will be effective, but I'm not sure. I think there should be a fine line in between simplicity and covering all the requirements of the policy. Yeah, but it will be effective. If you flick it. I think that I	PDS

		gave you the example of Google, so Google does a pretty good job doing it.	
35	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
36	R2	Yes. Yes, there is always yes, of course. As I mentioned, I mean thinking about privacy, privacy would also mean security. So that additional effort of designing a product that has more importance on those kinds of aspects would definitely increase the amount of development and work overall. Not just developing I mean were talking about the legal department, were talking about security experts. So, it's definitely a big trade-off. I think in most of the cases it will only be possible to implement those if the project or if the client or if the budget allows.	FF HE
37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R2	As a tech person, as a design person, I think it's awesome to be able to control my lights or my Spotify play with just you know, voice command. I like it. But at the same time as a human being that is concerned about privacy, I'm kind of concerned I tend not to share certain information on Facebook and other social channels. I have a son. So, every time I share a photo with his face on Instagram or Facebook. I'm concerned about that every time I think about it and how that might be abused in any way, you know. So, there's always a worriedness, as a designer and as a user. That's my feeling, I don't have an opinion about it. But that's my feeling. That's my experience. Well I always feel like it should be transparent. You know that people need to have control in any device. Like it doesn't matter whether it's the video camera or the Google what was it called Alexa and any new technology or IoT, all of them should you know be concerned about privacy and allow users to have control over their private information. And the company should be really transparent about their privacy policy or the way they use the information because not many companies do that, I guess. I don't think that's very clear to me how they use the data, right? It's always fishy. I am really concerned about it. I'm very sceptical about it and I'm scared of it too.	SIS BRNR TV IOT
39	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	

40	R2	Yeah, that reminded me of the case of the Target. I think it was Target or Amazon perhaps. The pregnant girl was hiding that she was pregnant, but apparently Target or Amazon through online cookies and online advertises, the algorithm found out that she was pregnant. And they were sending her the baby products to their address. And eventually the father found it. It reminded me of that case. I don't know. Because advertising, digital marketing, online marketing is a big thing. I don't think I can't see any other way without them. I mean I don't know how companies would market without online advertising. I don't see any other way. So, it has to be probably it will stick. It has to be there.	BRNR ABP
41	I	Is that a problem?	
42	R2	There are many problems with that I guess but there's no way we would survive without it. And that's my opinion. It needs to be refined. It needs to be better. I guess more transparent, having more control. But completely removing it, I don't think it's possible these days.	TV
43	I	How important is a proactive approach towards privacy in data analytics?	
44	R2	How important is it? Okay, it's very important. It's very important, I think. More and more companies would like to know more personal information because they want to refine the data more and more clearly. They want to have more accurate data with personal information. They would obviously try to get more personal information and it's important for them. And for analytics, it's important for analytics. Because in order to come up with a concrete, like for instance as a user experience designer, we do A/B tests, right? So, knowing more information about the users, like where they come from. or maybe what age they are. Even that would give us much more valuable data than just by knowing what their browsers are. And then we will make very important decisions based on that information. So, it's very important. But again, privacy yes. I'm not sure what the balance would be between these two sides, but it is important. But to answer your question, it is very important and without the more concrete refined information, analytics will not give us valuable insights.	DA, PP
45	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
46	R2	I don't think so.	

47	I	Thank you for your time! We really appreciate your contribution to our research.	
48	R2	My pleasure!	

Appendix 4: Interview Transcript (R3 Sweden)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview? Can we use your full name and company name? Or do you wish to remain anonymous?	
2	R3	I would like to be an anonymous, but you may record it.	
3	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
4	R3	I started out working with this design, graphic design and stuff like that, way back. I then decided to pursue a career in development, so coding and android development and things like that. Me and my friend who I studied with tried out starting some companies working with other people doing some consulting work and stuff like that. And that's where I really got into like the UX and UI part of the design of digital products. But then I got hired as an Android developer at my last position, but that grew into an UX role instead because we started to rewrite the whole app from the scratch. We outsourced to another country with a UX designer that really did not meet our expectations. So, my boss decided to switch up my role.	
5	I	Are you more comfortable in that position?	
6	R3	Yeah, I think, even when I was working with writing code I could never really like letting go of the aspects of user experience. It's so important and so I rotated towards that. I have been working at my last position for let's say 8 months as an UX designer. And I'm working at another place in Malmo and haven't been working there for too long. So, I'm just getting the hang of things there. But yeah, there I am working as a UX/UI designer.	
7	I	Okay. How would you define privacy?	
8	R3	In simple terms, to be able to be non-recognizable	BRNR
9	I	In your experience, when is privacy implemented in product development?	
10	R3	I mean usually like the last project that I worked on we did have it in the beginning, but we didn't have it in a way where we were designing the product from a privacy point	PP

		of view. More of a, “we kind of need to have this” kind of way. And I think it's been like that most of the time that you have an idea, and you focus more on the core functionalities. And then and then we evaluate like the functionality versus like the privacy. I think it got more focused on privacy when GDPR came into play. Then we really had to hire people who oversaw that aspect.	FF HE
11	I	Sure.	
12	R3	Before, when we added a new feature or before we saved anyone's data we didn’t need to make sure that we could remove and things like that	
13	I	What does your company do to make sure that the right privacy protection practices are in place?	
14	R3	I can't say much about the position I am working in now as I haven't been working there for too long. I haven't really gotten into the whole structure of the Privacy aspect of it. But in the projects that we have we use a lot of third-party reliance as well. Like for example signing with apple, signing the Google that kind of features so that we don't necessarily need to save people's data	AR
15	I	I see	
16	R3	I can tell you a little bit about my previous role, about the product. We both had an SDK and we had applications where people could use the app, check into the hotel, save their information. Like credit cards and all those sensitive points of data. And the approach that we took there was also similar like we used a lot of third parties already established libraries or partners who could really like, remove all the privacy connection with our company so that we don't have to be thinking about sensitive type of things	EES AR
17	I	Sure, is that common would you say?	
18	R3	I think so. There's a lot of there's a lot of companies who work with this, especially when it comes to things like payment and data collection, like it's hard for smaller companies to have those policies. So, both the companies that I've been working on are small and I think it's hard in the beginning, especially for start-up companies to have a person dedicated to making sure the right privacy efforts are in place. So, the solution is outsourcing and other third-party options that has been made by developers	

19	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
20	R3	Yeah, when I started there was talk about the GDPR. When it hit in 2018, people really did not care about it. The approach of the company when it hit was basically just, let's have a legal team to make sure we're not going to get sued. No one thought, we must care about the users or anything. Just, what are the rules, let's follow them.	GDPR
21	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
22	R3	I mean there were small things that affected my work in the way that, we need to better inform the user of what information we save, when we save it, where they can remove it and those kinds of processes.	TV
23	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
24	R3	I would say so yes, so before you sign up to do anything you will have terms and conditions kind of like right in your face. I know that other companies, like Google, started coming up with creative ways to inform the users about terms and conditions. They started making like full designs for one aspect of the terms, for instance saving data. I don't think most companies do that as it demands a lot of resources.	RUP
25	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
26	R3	Not sure actually	
27	I	Are you familiar with the concept of Privacy by Design?	
28	R3	I am, not into detail though.	
29	I	What measures do you take to prevent privacy breaches?	
30	R3	I find that basically it wasn't up to me. Basically, the product designer was telling me like not we like we don't care about this we care about this. And I kind of just had to follow the flow.	FF

31	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
32	R3	I'm saying no comment on that one because I don't know.	
33	I	In your experience, by adding privacy requirements into your product or service, are you sacrificing the usability or the ability to serve your customer?	
34	R3	Yeah, I mean, I know that we had to remove features due to privacy for example, that was kind of a big thing.	RUP, FF
35	I	Is that a big problem does you think?	
36	R3	I think that everything is possible to solve but you need to make sure that you put the time and effort into fixing a problem	
37	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
38	R3	We didn't have any really to be honest	
39	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
40	R3	Personally, I think it's a good thing overall. Personally, don't care as much about privacy as other people, I think	PDS
41	I	As a user or as a UX designer?	
42	R3	As a User	
43	I	Okay.	
44	R3	As a UX designer I do think about it. I need to imagine myself as the user or the target group, and most likely the target group will most likely not want to give away their privacy. And a good way to make them feel comfortable when it comes to data is to make privacy as a default setting	PB PDS
45	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
46	R3	I spoke about that. Let's say you have your core functionality, and you're designing a product from a privacy point of view, there are times where core functionality will suffer. For example, now with all face scanning technologies. For instance, let's say you’re trying	FF

		to open a door using face scan, the function itself would require a certain limitation on privacy. And if privacy is the most important factor, how would it work? So how does it do that? And so maybe its privacy is like the most important thing	
47	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
48	R3	Yeah, I do think so. I mean, I think especially IoT, then we're going to have a lot of bio solutions. But I think having privacy in mind, for those kinds of products is very important. When we're talking about IoT, you have things in your own house, connected to you. Then people would not only know information about you, but they could come into where you live.	PED, IOT
49	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
50	R3	I have like two thoughts on it. In one way, I think it is good. If I'm looking for something and I can't find it. And then suddenly there it is. The problem is the market kind of disappears. Using my information, companies will basically tell me what I want, I'm not going to get exposed to something new that I might like.	ABP
51	I	How important is a proactive approach towards privacy in data analytics?	
52	R3	I think it's depending on like a product and what it is that you do with it. And yeah, I think it's a really big difference so like for example, if I were collecting data, I think like for example fitness apps and stuff like that. I think a good thing for the user. Because without for example taking the polls or without counting the steps that they take and stuff like that. It's not going to be very like a useful experience. Whereas, there could be another product where it has nothing to do with anything that's beneficial for you. It's basically just asking for data and then moving that data from you somewhere else.	SIS
53	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
54	R3	I think we touched on many aspects and covered a lot.	
55	I	Thank you for your time! We really appreciate your contribution to our research.	

Appendix 5: Interview Transcript (R4 Greece)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R4	No problem	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R4	You can use whatever you want. There's no problem.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R4	Yes, currently I am a UX researcher based in Athens Greece and I work for Blueground. So Blueground is a real estate company that offers furnished apartments for stay for 30 days or longer. So currently I'm a UX researcher in Blueground's website. So, you know, my main parts are finding out user needs and transforming these needs into some wireframe designs that I offer to the UI team.	
7	I	How would you define privacy?	
8	R4	Privacy is something that's a trend. You know, after GDPR, everyone has it in mind. I think probably is really important but it's something that is very vague. I know that I can, you know, tick some boxes and check boxes and everything but in the end, they will be so huge that I think I will not be able to control it and my information available there. So, I think I'm just living with it, I know there is no privacy on the web and that's it for me.	GDPR
9	I	In your experience, when is privacy implemented in product development?	
10	R4	I think privacy from one point is that I don't want to be contacted. So, there are the checkboxes that I will sign up for a newsletter or I will be contacted Via SMS or anything. So that's one part of the privacy that I can choose who can contact me. So, I think that's good. Also the second part of privacy which is the most important is part of the security because I give some personal information when I sign up so I have to be sure that this information will remain only in the company and not be spread out. I think that is the most critical factor in privacy.	BRNR

11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R4	First of all, like for whatever we need to contact one of our users or customers to have options for them to choose their contact preferences. And secondly, we try to make our website and our database and everything that has sensitive info as secure as possible. So, the methods that we use when we take some information from our users and we try to deposit them in secure spaces and also apply secure ways of transferring data so that there are no leaks at this process. Yeah, I think these are the main parts	EES
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA? Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
14	R4	When GDPR launched I was in another company. I was in an e-commerce company and I was in the digital marketing department. I would schedule every day to send out a newsletter. So until one day and we were sending out a newsletter without thinking very much who we need to exclude from our database and it was more free, but after the GDPR, especially in the beginning then it started to get a bit softer, but especially in the beginning there were like rules making sure we needed to send everything to our customers. We need to get their consent that we can send them email and then this consent has to be stored in a way that there is no fault and we do not send emails to customers that don't want to be contacted. So that was a big part of our work every day. I remember GDPR a lot as it was critical for my previous company	GDPR
15	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
16	R4	Yes, I think it's pretty easy because we try to have like a bit minimal UI, but all the actions are clear. We try to keep them clear. So, whenever you sign up like to create an account or you want to sign up for a newsletter, all the options that would affect your privacy are clear to you so you can select. We try to implement this also with our payment terms and contract terms. All these are visible to the customer. So before booking he can check all the terms and then proceed and after booking, they are available to him so he can access it whenever you want.	RUP

17	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
18	R4	You know, I don't think because of the visible privacy. You know, the one that you can see as a user is, most of these are the same for everyone. I think the most critical part is the back end. But the back end is not visible to other competitors.	CA
19	I	Are you familiar with the concept of Privacy by Design?	
20	R4	I don't know to be honest. I haven't heard of this concept. So, I would be eager to hear what it is.	
21	I	What measures do you take to prevent privacy breaches?	
22	R4	Privacy breaches okay, so we try to secure our database first of all, and so that there are no attacks to our database. Secondly, we try to secure the ways we transfer data from the website with the user and enter them to our database, so the obvious path can be as secure as possible. And finally, we try to secure our website from harmful attacks like to our forms and everything that can have input to be secure. So, there isn't going to be like scripts or whatever intact there and harm our website in this way.	PP
23	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
24	R4	We just recently launched the user profile. And we see there what data we have collected from the customer. We also have the option to opt in and check out opt out from the use letter and as we progress, we want to give more options there. But as it's a very new feature, the newsletter is the only option you have to opt out at the moment.	GDPR, CCPA, RUP
25	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
26	R4	I don't think so because usability is not very much affected by privacy in my mind. I think privacy is just some options you give but these are like making usability better rather than sacrificing it. So, I think yes, if you have privacy, and you have privacy concerns, it raises the usability of the website instead.	FF
27	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	

28	R4	We have some third parties we use for payment but usually these data are not handled within our system. So, what we do is we have a wireframe. We load the screen as a pop up within our website, but everything that the user enters there is not visible to us. It's just visible to our third-party provider. So, the security is on his head and usually because they are payment providers there is much security. But these data are not stored within our database. We are just stored on our third-party.	EES
29	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
30	R4	For me that's a must. I mean privacy has to be ensured for anyone and also like to know that these data are available on the web. So, you don't need to do anything bad for you to get more data. You already have enough data. You don't need more than that. You have to ensure usability. In order to ensure usability, the user must feel safe, if he feels safe within your app or website, then he will use it better. And she won't have to look you know for what are they hiding here or what's happening? And by ensuring that I think that the user will then feel comfortable he will also hand you more data than he would if you try to cheat and take his data.	PDS RUP SIS
31	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
32	R4	You have a budget. You have to finish certain core functionalities and the privacy comes second. Yes, usually you have some extra work to do and that raises the effort of the team I see yes. It depends on the feature on your website or app. I mean if you handle payments there is no way that you cannot take care of privacy for your user. But if it's a blog, okay, I think I mean you won't need much info from your user so you don't have to care much for privacy, if you don't ask for privacy it would be on the level that you need it. So probably depends on your actual product. If your product needs privacy, you have to give more cost and give effort in order to ensure it. Otherwise, you might go out of business.	FF
33	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
34	R4	Yes, I mean when your product seems and feel safe it will be more easy for you later on. If you want to move on to the internet of things or that stuff. To find people who trust your website and would be a third-party provider or would connect with your device. I mean, let's say that you want to	IOT

		get to Apple home, then there are very strict requirements to get there. If you ensure privacy you might have a chance, otherwise this door will be closed to you and you have to go an inferior provider. There are very strict requirements to get them. So, if the privacy is there you might have a chance. Otherwise these doors will be close to you and you have to go to maybe an inferior provider. So secure privacy opens the door for those kinds of things.	
35	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
36	R4	I think that if these data are handled well, they can prove beneficial for both the user and the advertiser. I mean the advertiser will get to the target group that were related to his product and he will show products that are going to be bought more and also the user me as a user I would see ads that are related to my interest. And maybe also I find out some things that even I didn't know that would interest me. But because someone analysed my behavioural pattern, saw that this will be interesting for me. But of course, there are many ways where this data is not handled well. I might see excessed advertising about something and that might become annoying in the long term. I think it's good to have this data but also, it's important to use them well and provide value both for the advertiser and the user.	ABP
37	I	How important is a proactive approach towards privacy in data analytics?	
38	R4	I think it is very important. If you can secure your website or the app and the data you store before the breach happens, that is ideal. However, in reality usually it's difficult because you can be proactive on some things, but you cannot think of everything. There are always breaches happening, so you have to be quick and adapt quickly. But the more proactive you can be, the more profitable it will be for you in the long term.	PP, DA
39	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
40	R4	I don't think so at the moment because I mean you got me deeply, I thought of many things that I connected that I haven't thought of usually. I mean a big part of privacy and privacy concerns is I think the big data, you know, the huge mass analysis of data, so maybe that’s something you could look into as well. Otherwise I think it's pretty good.	DA

41	I	Thank you for your time! We really appreciate your contribution to our research.	
42	R4	Glad to help you!	

Appendix 6: Interview Transcript (R5 Canada)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R5	No problem.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R5	Yeah, you can use my name. I'm not sure about the company name.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R5	Yeah, for sure. I've been working as a UX designer at a notion. You know, she is a global in-house agency of actually in-house agency of certain sister brands, car brands. KIA, Hyundai and Genesis are three of our main clients. These brands are owners as well as our clients. We basically work for them. My experiences, I've been working for their digital products applications' websites. And as well as internal needs sometimes clients may need some internal projects. I've been working on the user experience and delivering some recommendations for existing products as well as new ideas, for example if there is a new website idea coming up. I've been discussing the opportunities, pain points, needs and providing some user insights and delivering some wireframes for them to understand what might be what new product may look like and also conducting some user testing, I can't say like it's a proper a hundred percent correct test and research process that I've been following because it's due to the nature of agency environment. We have some new business clients, for example, like cannabis business. I've been working for a new cannabis client as well. Or some insurance brands, but my main focus is more on automotive websites.	
7	I	How would you define privacy?	
8	R5	I'm not sure what privacy were talking about, but my understanding is user privacy because like for example if I'm conducting a user research like you do right now, my main focus is not providing personal information of the user that I've been interviewing. And for example, I've been following many users with some user testing tools. So	SIS

		even though I know the location and IP number for example, there is a lot of information. I'm not involving any information about users so when it comes to client privacy or like for example, if you know, I'm working in an agency and there are maybe 10 different clients and ten different projects and most of them are NDA so I am not supposed to provide any information. For example, how can I explain? In our agency we have blue side and right side, so we have KIA and Hyundai so I'm a purple one because I'm working on both sides. But I'm not supposed to talk about any upcoming project with each other so I have to be really strategic about what I'm recommending to one because like two projects shouldn't be overlapped and because like they are audiences different, their content strategy is different. So, how can I provide privacy to one and other is to basically not to give any formation and also not to share any documents that I've been working on. Yeah, or like for example, if you're talking about the tools that I've been using mostly I'm adding some passwords to projects that I've been sharing with them.	BRNR
9	I	In your experience, when is privacy implemented in product development?	
10	R5	So again, if we are talking about clients, but like project privacy, I would say from the start because like if there are if we are talking about ideation process, for example, which we let's start with a scenario. We identified the needs of lines, but there are user says well and the client asks for a product but we are trying to identify if it's usable for the user or not and when you identify the actual needs and pain points, we move forward with some ideas or sketches or like brainstorming sessions. We have to start from this moment because like there's a creation process and it should be unique for this specific product. So, in that specific moment, we have to start thinking about privacy and we have to keep it for us only.	PP, PED
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R5	Well, that's a good question because my company is not really, I mean our IT team is providing some privacy rules but eventually we all use a common server that everyone can access to many folders. The best they can do is, there was a segmentation for specific users. For example, I'm working for only creative documents. I am allowed to see all of them, but I'm not allowed to see admin documents. So, or for example if there's a finance team and they are not allowed to view all documents that they aren't supposed	AR

		to. Because eventually there's an employment and human resource process there as well. So, they have to be really careful eventually. One other thing that's companies doing I'm not sure if it's the right process to follow but I think it's something common that agencies are doing because this is my first agency experience. I've been working in corporate environments for a long time. I've never seen such a process before but if someone is laid off from work at that moment, they are agreed that that person's last day at work, from that moment, the whole system is blocked. And I asked the reason why and I said like it's kind of weird like why they blocked the whole system they can't access any email or anything and they say like, you know, it's an agency and they might take all documents with them and share with other clients. That's really interesting, for example if they decide not to move forward with someone. They say like OK; this is your last moment. Take all your stuff and go and they just give you 15 minutes and they don't allow you to access your computer and it documents. And yeah, this is actually an example privacy and it's so weird for me but like I'm being honest here, so that's an interesting process policy my company following.	
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R5	GDPR yes, not sure about CCPA.	GDPR
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R5	No.	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R5	I'm not sure about the GDPR but we are trying to make them understand some regulations. Some regulations are mandatory to add. For instance, we have some rules and regulations, only like provincial regulations. For example, only for Ontario or Canadian web regulation that we have to add some explanations to our websites. But I'm not sure if we're providing GDPR correctly so to say.	RUP, GDPR

19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R5	That's a good question. I'm not sure actually. I'm not sure if there's a benefit for our users or clients for their privacy. So just wanted to give an example about privacy, but we're working with cookies and they're keeping their location because we have to provide the prices and we have some field and price calculators for cars. So, we need their location. We need their private information postal codes and everything so that we can provide correct prices specifically for that location or for example, if you have some dealers close to that address, we have specific campaigns for them. So we need their private information, but eventually we use their private information to target advertisements. I'm not sure if that replies to your question, but we all play with specific personal information because we have a large analytics team and there are media paid search teams and they all work with their privacy, actually private information.	ABP, DA, CA
21	I	Sure, absolutely. But do you see any benefits to securing that information?	
22	R5	So, here is the thing we get the benefit, but I don't think our client is getting the benefit of it. Like we definitely get the benefit of accessing to their privacy because like we were bidding, we have media team and we are bidding to their location or like Google history and all like YouTube and we have Instagram team, Facebook team and they all work with their privacy information.	DA
23	I	Are you familiar with the concept of Privacy by Design?	
24	R5	I'm not actually. I would love to learn.	
25	I	What measures do you take to prevent privacy breaches?	
26	R5	Oh. Well, to be honest, I'm working in a team named Digital Labs. And the Privacy aspect of the projects that we're working on is more for example, as I mentioned like analytics and data team and paid search biddable search and biddable media team, so they are more into that. So, what I do is my role is more on the ideation process of projects. And so, for example, I'm working on design and usability and user research part of the projects. So, the measures that I'm taking are for example, I'm delivering some recommendations just one example. There is a persistent requirement on the website as soon	

		as you go on Hyundai canada.com. There is a persistent question like submit your location and users are hating that, they don't want to submit their location. They just want to see the cars. Maybe they don't want to provide their information because they already know that we're going to Target them, and they will see Hyundai Ads everywhere, but they just wanted to check one car, but they don't want to see Hyundai ads on Facebook or everywhere. But what I do is I'm recommending them to just like remove it but there are some certain aspects that I can't tackle. Like I can't break. For example, this is something mandatory that our client is asking they say like, oh we need their personal information, they have to submit their personal information to see the cars and I say like it's not about user experience. It's more about service design, the system design like it doesn't work for a client. You're not making them happy. Maybe you are disturbing them and they not they are not even engaging with your brand, but it takes a lot of effort to educate clients. So, I can't go beyond those measures.	RUP, SPF HE
27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R5	Can I skip this question?	
29	I	Yeah, sure. In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R5	Well, unfortunately, I'm sacrificing usability to a lot, you know, if you're working as a sole UX designer in a company, you have battles more than one, because like you have to battle with client, with your colleagues with many other departments and you're like to advocate of the user and you have to tell them like this is not usable and you have to be usable but they say like, oh, we actually care about sales and as long as they get the numbers, they don't care about usability. and think about Canada our population is so low. And for example, we have 36 millions of population. And the target of the client is selling a million cars. And they are making their numbers and you're saying like this is not working, the website is not working, and the user is not happy. Then they might say, we don't want to invest in this because like I don't I don't need to spend money on improving the usability because	FF

		I'm making money and reaching my numbers with existing website, but you have to make sure for your client to understand like they are competing with other brands and they are going really well. Like their competitors are going beyond what they did before, so it's not only about making numbers. You have to be really accessible. You have to be inclusive. You have to think about multiple user models. But the reason why I'm saying most of the time I might be sacrificing usability but not because I want it. It's not my preference, it is because I have to.	
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
32	R5	I'm just in the design phase. I don't have access to user's data. The only moment when I have access is when, let's say that I'm going to conduct a user research like you do. I'm finding specific users and I'm having online meetings. That's the moment when I have access to the data.	AR
33	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
34	R5	Yeah, so I think it became a default for all websites to provide privacy options for all users. The only thing that I'm avoiding is making things like providing privacy and mandatory. We have to give another option for them to be anonymous. Because some websites definitely need your location. For example, this is a case for us as well. We need their location to identify the correct numbers. For example, as soon as you go on KIA.ca, the first thing they see is a pop-up to provide postal code but they can just close it and they can just check the cars without providing any information, but once they decide they want to see personalized products then they have to submit their private information. That should be an option for them, not mandatory.	PDS SIS BRNR
35	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
36	R5	Absolutely, like unfortunately, we're not there yet. The design industry is going to be better about things like privacy or like usability and like accessibility inclusiveness and everything. But the first priority right now is more about functionality, unfortunately.	FF

37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R5	Yeah, absolutely. Like I as I mentioned it's definitely have a lot of benefits but like first of all, I'm not sure if it's about IoT, but embedding privacy helps us to manage client relationships first of all, and secondly, for example, if I'm working an agency or product company that makes me more reliable if I have more privacy functions. I'm using some tools and technology to provide privacy because we may work with government offices. We may work with banks, insurance companies which privacy plays a key role right. So we have to ensure that our workflow, our whole system is a hundred percent private, but when it comes to embedding privacy into design it's also important for again to ensure the end-user to use our products without hesitation like they shouldn't hesitate to use for example, if I'm working with as I mentioned working in a bank or like. Actually, It's like a key thing nowadays. But, when it comes to IoT, I believe that users should have a flexibility of providing their private information. Even today, this is something I am tackling, for instance I'm not using a car but every day I see cars ads everywhere. Totally unrelated things I might come across during my day. But if I have access to any tool that is not using my private information for their sake then I would feel more engaged with that product. And that is something we have to ensure, putting ourselves into the user's shoes. So as a reply to your question, it would definitional benefit our projects	PED RUP IOT
39	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
40	R5	Well, my personal opinion is going to be different from what I do. I personally believe that we are slaves of capitalism right now. Especially North American culture is based on changing people's minds to make sure that they are spending more money every day. they should never stop spending money because that will be an R movie. This is happening right now in the whole world. But like my personal wheel is we where we're harming the ecosystem right now by using private information. I'm in the kitchen off this and I can see that for example, if a user clicks just like type something on Google, I'm working with Google Canada right now to get this information. For example, I'm using their organic search data from Google and then I provide them paid search data on Google and I show my ads everywhere to them until they get sick of it but they	ABP

		don't get sick of it because in marketing there is something like if you show something more than seven times they eventually get used to it. And when you think about this it is actually really dangerous. It's not even dangerous for politics and the whole world and like these methodologies, so I'm not finding it right but I'm working with it. My personal thinking is now like I really hate marketing actually, but I'm working in it's like especially in advertisements like the only thing like the only thing that clients are thinking is selling more even though they don't need. We're practicing for example the lifecycle of the car buying of a person, like how many cars would a user buy in their life cycle? In which track information about when they got married, when they got children, when they got this, when they got a new job, we are trying to identify that moment so that we can target them. So, this is really dangerous because we are actually accessing their whole personal information. We're following them and we're targeting them just to make sure that they're not keeping that money. They have to spend that money.	
41	I	How important is a proactive approach towards privacy in data analytics?	
42	R5	Again, I will talk more about the user perspective. So, from a data analytics perspective proactive approach for privacy is I mean if we're talking about accessing private information, it's highly important because this is how a data analytics team is, their function is based on the private information. If there's no user information. They can't understand the numbers, trends and the preferences of users and even their demographic data. For example, like, you know, all the information about the annual household income or like gender information accessible to information. This is key and highly important for data analytics and also, they keep track of the reasons why they leave our websites or the reasons why how they come into how they land into our websites. Which tools does Instagram or Google use and which of them work? This is the only way for them to understand what worked and what didn't work.	PP, DA
43	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
44	R5	No.	
45	I	Thank you for your time and stay safe! We really appreciate your contribution to our research.	

46	R5	Thank you.	

Appendix 7: Interview Transcript (R6 China)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R6	It's okay.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R6	Yeah, so it's okay.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R6	Yeah, I have to say that. First of all, I have a bachelor for 4 yours in industrial design. It is mostly structured around service design. Or the so called UX design, we also do some UI interfaces. I also had an internship at a company in China, where I mainly did some UX stuff, and I had some projects with different companies. Such as usability testing on Cloud platforms.	
7	I	How would you define privacy?	
8	R6	That is kind of an abstract question. I don't know much about European countries, but in China we have a weird phenomenon where you might say something or do something, like some kind of food and that will be recommended to you on your phone. It's kind of weird but maybe you don't know that your phone might be recording and collecting data then sending that to different apps that maybe benefit from it. As a user or as a consumer we have a right to know if our privacy and personal information is used by business.	SIS BRNR
9	I	In your experience, when is privacy implemented in product development?	
10	R6	I don't have much experience in that, but I think it is not something you have but something you will build up in different stages.	
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R6	It really depends on the purpose of the company. I have experience in the Cloud, this kind of stuff, if you want	SIS

		people to use this you need to guarantee to your users that this is really safe. In terms of answering the question it is probably more of an engineer perspective. As a designer we can only make the users believe the service is safe.	
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R6	Not at all	
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R6	-	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R6	In my experience it is important to make the users understand their privacy because it makes them more agreeable instead of just putting in some long text. Especially when it comes to cloud service.	RUP
19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R6	Yes of course. Though I feel there are more aspects. Like it is easier for well-known companies to guarantee people's privacy, because they have many users. I think it is harder for start-ups.	CA
21	I	Are you familiar with the concept of Privacy by Design?	
22	R6	Not really	
23	I	What measures do you take to prevent privacy breaches?	
24	R6	Actually, I'm not quite sure about it. Not part of the job of a system designer. System design more about the users, instead of the back end.	
25	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
26	R6	At least in China, I think they are using the data of the users without them knowing. Or they know but they rarely notice	TV

		the terms of privacy. But still they are using the data, and there is no denying many can get access to your data.	
27	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
28	R6	Usability testing feels more about patterns and layout, buttons and so on. Privacy is not part of the usability. Privacy is not part of the function so maybe it won't affect much.	FF
29	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
30	R6	If you look at clouds and those types of services, you can see certain terms and conditions. I think they should have that.	
31	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
32	R6	You still need users to understand you have that kind of privacy. I think it is kind of nice if you don't have to read through all those terms but good if you have some items or keywords that explains it	RUP
33	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
34	R6	I don't know much about it, maybe it doesn't affect functionality but you need to make this information more visible to people so they can understand your privacy maybe just by looking or glancing through your site.	RUP
35	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
36	R6	If I understand it correctly. If I'm using those kinds of devices, they are like recording my sound every time, so I feel it is more disadvantaged rather than an advantage. You can't replace the sound interaction; you can't replace it or do much about the function. The function requires that data. But I think there are products that pay more attention to privacy, products that only record your time and sound if you give permission. Or they record surroundings only and give random sounds.	IOT BRNR

37	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
38	R6	Yeah, well, it's kind of tricky. First, I feel like I really hate that because it is reading my privacy. The company or the business knows you better. But I also feel most people are getting used to this type of function and there is no denying it brings a lot of convenience.	ABP
39	I	How important is a proactive approach towards privacy in data analytics?	
40	R6	Like in the last question. If it is sound interaction like Chrome devices. Maybe just give forced sounds so they won't hear you unless you give permissions. I think it's hard to know what some apps really are doing with your data, and whether their promises are really reliable promises.	DA, PP
41	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
42	R6	I don't think so.	
43	I	Thank you for your time! It was nice to meet you!	
44	R6	Thank you!	

Appendix 8: Interview Transcript (R7 Italy)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R7	Absolutely	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R7	Feel free to use it	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R7	Okay, cool. Well, actually I'm based in the center of Italy and my work starts from a client coming to me, because I have a good reputation online fortunately. And they ask me for different kinds of work, among those are UX design and interaction design. I've also been mentioned several times in the Adobe Gallery. I also work with design brand logos and occasionally I teach courses online. So actually, I received several requests from people wanting to employ me, but I prefer to work by myself. In case I need help I contact other freelancers like me. I think it is better than a company. Maybe not quality wise because of course a company has more resources. As a company often has more clients, I prefer to focus on a few clients, it is better. I want people to know they can talk to me and trust me. I am their Italian craftsman. If you trust me, I will drive you to build the best product for your market.	
7	I	How would you define privacy?	
8	R7	Okay, usually my goal is to make the client feel comfortable, if they tell me something, I will be silent and not tell anyone. Because in this line of work it is important that they feel comfortable to open up. Usually, I am a guy you can trust, and people understand this. And so usually my clients are very comfortable with me. Even to the extent that a Non-disclosure agreement (NDA) will not be required, even though I have a huge stack of NDAs. This is my approach with privacy, when I sign up on an NDA, I understand how much a company wants to protect its idea. Unfortunately, the NDA doesn't work too much because I can change the name of the company.	SIS

9	I	In your experience, when is privacy implemented in product development?	
10	R7	It is there from the beginning guys. Because most of my clients do that. We have this idea, first they ask me how much you charge, then they talk about privacy. I have worked in several start-ups and I know of the importance of showing our investors that we are protecting ourselves, NDAs and so on. But when my client shows me his intentions to manage his privacy, I will value that request because I understand how important it is. But it depends as well, if the client tells me they want privacy or not. It is a budget thing as well.	PP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R7	Okay, I got myself a folder, I organize my client in folders and if the work with a client is ongoing, I have folders for it. I don't put anything in Cloud. I don't know why but I don't trust it. I have it in a disc in my computer, and if I finish to work with a client, after two months I transfer all to my private hard disk that I store in a safe. So, if a hacker gets through my laptop, they won't find anything.	SIS
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R7	Yes, GDPR, I am improving this in my new website that I'm going to share this month. And for example, GDPR, I don't save personal information.	GDPR
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R7	My work doesn't require me to handle information in a way that would be affected by the GDPR.	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R7	For example, when I build an application, I put the privacy in the first page before everything, so it's a little button, under the login button and you can check about privacy. But people rarely read it.	RUP

19	I	But do you think there is a way of making those long terms and conditions easy to read and understand for users?	
20	R7	Well, okay a body text is easy to read when it is managed by a short paragraph, because if you do a huge text someone no one will read. Changing the text, using bold or italic for example makes it easier to understand. But I think it is very clear now with cookies and pop-ups. These things people understand.	
21	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
22	R7	No. I don't. I don't promote my privacy.	CA
23	I	Are you familiar with the concept of Privacy by Design?	
24	R7	Not sure	
25	I	What measures do you take to prevent privacy breaches?	
26	R7	Usually the company has a UX designer inside the team and I prefer that because sometimes I don't like UX, it is mostly his responsibility.	
27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R7	I'm transparent from the beginning. As I told you if they ask me for additional privacy measures I will say yes and help them. But usually I won't go to them and tell them I will protect all your information and so on, it usually goes the other way. I use a very personal approach built on trust. Sometimes that is what companies look for.	TV
29	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R7	I think sometimes you have to sacrifice their usability. But if you're smart you don't do it. I prefer to put privacy in the onboarding phase. Onboarding phase is the phase that converts the user to use the app and be an active user or leave the app. So, privacy has to be there right away when they decide to use the app or not. And you are free to not read.	RUP
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	

32	R7	It's like a check mark. It happens sometimes when someone needs security. Like I'm not a robot or this or where you have to identify where the taxi is in this picture or where the umbrella is, those things.	
33	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
34	R7	Usually these things are not managed by the designers. Basically, every kind of platform or application uses something that already exists, generated services. And usually these are very certificated.	
35	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
36	R7	There is absolutely, core functionality come first, usually	FF
37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R7	Yes	PDS
39	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
40	R7	I think this is a very huge problem. It would be great if this is used with respect to the person.	ABP
41	I	How important is a proactive approach towards privacy in data analytics?	
42	R7	I can only speak for myself, but I'm not really interested in the single individual, I'm more interested in different segments, groups of people.	
43	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
44	R7	I don't think so, it was very good. I hope that my information was useful for your study.	

Appendix 9: Interview Transcript (R8 Bangladesh)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R8	No, it's okay.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R8	You can use my name for sure.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R8	Yeah, sure. So actually I started my career as a front end developer six years ago, but after working with some companies and some freelance projects, then I intentionally moved my career from coding to problem solving or design phases and then I started designing for more than three years actually working as a professional level designer. I started working on a fintech company where I developed to two mobile banking applications, which was my first work as a UX designer and it was very tough for me because I was the team leader for a front-end team and I was responsible for designing the whole system by myself. But eventually I learned. Educationally I am a mechanical engineer, but I switched my career profoundly and I am proud of that switch. After working with that fintech company for more than one year, I designed an application for a secondary sales automation system. So, I work with that start-up which was a very mind-blowing experience for me because that start-up was in a very bad phase at that time. And their business was not aligned, so what I did was I did a lot of interviews with their sales representative and the stakeholders and asked what they wanted to achieve. I sorted out their services and corrected their visions and other business policies. Then I started designing for the sales representative. But their educational level was quite low. So, designing for those people was quite difficult, so what I had to do was to make a very good information architecture for them, so they would understand what to do and when to do what. After that I took a little break because I wanted to do UX research, not just the UI design and the wireframing. I think this area is quite user centric and I	

		really want to understand the mind of the users. UX research therefore is more prominent for me. I started designing a telemedicine application, interviewed different people and made some analysis, journey maps and empathy mapping.	
7	I	Thank you for sharing with us. How would you define privacy?	
8	R8	Okay, I think the answer can be abstract because privacy has some different contexts. There is user privacy, business privacy and so on. I really focus on user privacy levels and I make sure the company makes the privacy very good. Because in the end the user really cares about privacy. From my work experience, I did not have to compromise with privacy things, but I had to implement some security things in the applications. When I worked in the Fintech companies, security was much more important in those industries. In my experience, privacy should only be shared with those who will handle it correctly and in a way that will benefit you. Fintech companies you know, what? Security is much more important in Fintech Industries	SIS
9	I	In your experience, when is privacy implemented in product development?	
10	R8	I think in the ideation stage. If I tell you about design thinking, there are five different processes. So, at an empathize level, where I actually do the user research thing, when I come to the ideation phase I start to collect the crucial things that might be important for future business. I think empathy phase is just a phase where privacy things come around	PP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R8	Honestly, I didn't have to. However, I think there should be a standard structure. If I take the telemedicine case for example, I had problems finding problematic factors which makes it hard to know what to implement. But one strategy I used in the design was to use a username for doctors, a patient then had to know the username of the doctor. Then the patient will add the doctor and get consultants for the doctor. So, the patient can not accuse me later that I chose the doctor for the patient. I could probably design it in a different way, but I had problems finding issues and complaints here in Bangladesh related to my subject. I think every government should have structure for their privacy policies, it is every absent here	PP

13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R8	Not yet. I think all researchers have a lesson in how to make privacy, how to keep privacy and how to maintain privacy. But I don't think I've seen many courses where privacy was much of a concern.	GDPR, CCPA
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R8	-	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R8	I did not, but I would love to do that.	
19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R8	Absolutely, I think privacy is important. Typically, I want to use a product to solve a specific problem, and if I can solve it through this product, I will never think about where they are getting the information and so on. But if I cannot use the product to solve my problem, then I really ask: Okay, are they maintaining privacy? What are they doing with the information? I think it works like this.	CA
21	I	Are you familiar with the concept of Privacy by Design?	
22	R8	No, I've heard of it, but I don't think I know much about it.	
23	I	What measures do you take to prevent privacy breaches?	
24	R8	First of all, I really think we need to understand the users. We are making products for humans, not for technology. And most breaches usually come from humans, so if we can understand the user of that product, then we can see how breaches occur from humans. I think this world is a valuable place, and we are really not concerned about privacy. Talking about biometric things, we really can see that face recognition is available in Apple devices, fingerprint available in android and other devices. But companies really don't focus on security things and privacy policies. They are just selling products and promoting their products. Simply, the awareness around privacy is low	RUP

25	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
26	R8	I try to be	TV
27	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
28	R8	I believe the usability will not be compromised if we can understand the actual usability or the actual psychology of the users. In reality, we don't study people, we don't study users. Everyone says they are maintaining privacy, but really, they are not. In my experience I have seen that only big corporations are able to maintain privacy because they really focus on that. But in other countries, such as third world countries, they are not investing much money on privacy. For instance, I'm making products and I have certain things like privacy that have to be done in a better way. But I cannot make a policy on myself, it is not my strength, it cannot be done by one person. Example, in my previous company I was very concerned about privacy, but my managing director was not interested in these things. They only talk about technologies, or software architecture, never privacy	FF
29	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
30	R8	I think those kinds of things can be easily handled in the user research process, in the empathize and ideation process. There are various methodologies on those things which we can follow. Like empathy mapping. Again, the users are in the center. We can see where users are scared or where they are comfortable. From those points we can start to make privacy policies, ensuring them that their information is hidden. I think empathy mapping is one methodology where we can start.	RUP EES
31	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
32	R8	What I can see is that there are long documents of privacy policy, and then a very small checkbox in the end. I'm a hundred percent sure that 99 % of people do not read these because they are too long. It is not our problem that we are not reading these long documents. But if we can see it in a more modular fashion. Like this is your information policy, this is your privacy policy. Then I think we can really	PDS, RUP

		understand what is happening. Privacy policies should be easily readable as well l, they should not always be on the bottom of the page, sometimes it should be on the side bars, sometimes it should be in the notifications. Let's say you have 30 different policies, so then you make a notification for each of these. Send one of these per day perhaps, let the user know about your privacy each day.	
33	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
34	R8	The concept can be critical, actually, I don't think privacy has any compromisation. We should not compromise privacy because in the end if we want the users to come back then we need to maintain these privacy aspects. Google for instance needs to maintain their privacy because they know people will come back and use their features, that is why they need to care about privacy. I think that is one aspect to why Google is successful, because of their understanding, because of their policies, user thinking and so on. They focus on factors beyond just the technology or functionality itself.	FF
35	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
36	R8	I think there are many problems related to this. I think the company's security system is not enhanced enough to keep biometric data very secret. Like all fingerprints or biometric data might be going somewhere else because of the systems security level. At first the infrastructure should be secure enough to ensure that this data is not going away to other places. At that point people will feel comfortable about giving your data. Technology is constantly evolving, and we need to work on the privacy and security aspects.	PED, IOT
37	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
38	R8	It has two answers. Actually, I hate it and I love it. As a designer or as a user research, if we cannot understand users, we cannot make business. And if we want to understand users, we need to collect certain information. If we cannot have that information, it is hard to make a product. However, as a user I think I don’t like it at all and try to restrict the information I provide. I think this data must be handled with respect.	ABP

39	I	How important is a proactive approach towards privacy in data analytics?	
40	R8	I think it is extremely important. The infrastructure of privacy is one of the most important things. Data analytics requires information, and if we want to collect that information it needs to be secure first and handled with respect.	DA PP
41	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
42	R8	No.	
43	I	Thank you for your time! We really appreciate your contribution to our research.	

Appendix 10: Interview Transcript (R9 India)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R9	Yeah, definitely.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R9	You can use my name, and company name also.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R9	I am a graduate Bachelor of computer application. With that I am master's in design. In India's Number one Institute. If you heard about the National Institute of Design. I am a PhD in design for digital experience. So, it's a specialization in digital experience. I graduated in 2007, after that I have majorly worked with the start-ups where I learn to create my own processes because in 2007 UX was very early in the design. People are understanding user experience, right? There is no term in the industry, hardly top industries are talking about user experience at that time. There is a web designer you can say there is a post of web designer not UX Designer right and people are starting with the user experience, those who have graduated in product design or you can say UX or whatever the early adopters. After doing that I started as I said, I am majorly into the start-ups, with the industry of education, e-commerce, e-learning and data visualization. And you can say few of the industry with the airlines. Is there anything specific you want to know?	
7	I	What kind of business your company is providing?	
8	R9	Okay, so my current company is into IT services. We provide services to the industry. So, any industry who is into any business, so we provide that, it's a service-based company. And design is a part of that company. I am employed over there.	
9	I	How would you define privacy?	

10	R9	Okay, so it depends on subject to subject. For example, if you want to install an app where they need your number right, there's no privacy in that. But sometimes they ask forcefully to tell us about your information. At that time, you are not sure, because you want to install but without giving certain information and going through certain steps to use the app, you can't install it, so that is kind of hampering my privacy. So, privacy is very subjective. But privacy is something basically something I want to hide which I don't want to disclose to anyone.	BRNR
11	I	In your experience, when is privacy implemented in product development?	
12	R9	So far in general, it depends on the project. If I'm doing some project for an enterprise for example, then the privacy concerns are more because they don't want to disclose their things to their competitors. Like when I talk about my current company, everything is privacy for them. Because the client is asking for privacy. But at my earlier experience, privacy rarely mattered to people, so it was not as big of a concern. Because they are designing for end users only, end user means B2C customers. So, when there is B2B, privacy is more of a concern than if it's B2C.	
13	I	What does your company do to make sure that the right privacy protection practices are in place?	
14	R9	Generally, people in the industry want to sign some of the agreements. So, whenever we join a company, they do some contract signing related to the different projects. Sometimes these are general and sometimes specific for that particular project.	
15	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
16	R9	I heard about that. I have never read them in detail. In general, we know those things. After the Cambridge Analytica scam, we understood there is some kind of privacy in those things. And now everybody is talking about it. In India now with COVID-19 the government has an application where they can track us. Many talks about how the government is taking privacy, tracking everyone and who they interact with. But generally, we don't get more into detail when it comes to privacy if we don't see a problem	

17	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
18	R9	Not as such, I don't think	
19	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
20	R9	Yes, they do. Definitely, because we are serving the client, so that is necessary for us.	RUP
21	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
22	R9	Yes. In general, when there is B2B business, people want to look for privacy because they don't want to disclose their information to anybody. So that is a very competitive advantage from our point of view.	CA
23	I	Are you familiar with the concept of Privacy by Design?	
24	R9	I'm not.	
25	I	What measures do you take to prevent privacy breaches?	
26	R9	Whenever we use some information, we have to disclose them from where we are picking them up, and why we need that information is very important. So, we have to disclose them to the user why we need them. For example, if I need an email ID or phone number, where are using this email id and why we are using this email ID. And if we can disclose that everything is encrypted then people get more confident into that privacy because they know that what we are sharing we are sharing with the right people. They know we will not misuse the information because these days information is very important for everybody.	TV SIS
27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R9	Yeah, yeah. I would say that.	TV
29	I	So, do you give customers control over their personal data?	

30	R9	That depends on the project. At my current company we don't do intensive user research in general. So, from an overall point of view, I must say that whenever I have interacted with the actual users, I generally ask from the company that they will give me their actual users instead of me recruiting their users. And from those users we create the personas. And then whatever information we get from the users we provide to the company.	TV
31	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
32	R9	So again, it depends on the project. Sometimes they might affect each other but they should be handled separately.	RUP
33	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
34	R9	I am not the right person to answer this since I have never focused on those pointers. Whenever we talk to the client and the client ask what rules they have. For instance, they have their own private folders, where we have to upload files. Then we generally work on those spaces, and we don't use our own space to save it.	
35	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
36	R9	The biggest problem from a B2C perspective is people in general don’t know what privacy is for them. And if you ask somebody for some information, people are concerned about that. And if you will not disclose them, the company will not. If Facebook or google would use your data for something, then you would be very concerned with those things. And you see, 5 years ago we hardly talked about privacy. There is so much concern about privacy now. In the future it is important to make privacy a default setting, but I don’t know how business will grow at that time.	PDS
37	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
38	R9	Depends on the project. In my experience, when I did my freelancing, people rarely were concerned with privacy. They were more interested in functionalities. I don't think it is related to core functionalities, but it is related to when it's needed. So, you have to make sense	FF

		when privacy is important and when features are important, and that is a question mark for everybody these days. It also depends on what kind of company it is and how the business runs.	
39	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
40	R9	Yes, I do think so. I'm not sure how or why.	PED, IOT
41	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
42	R9	So in general, the market will use those information, whenever you look for your Gmail account you see a particular kind of advertisement on the right side and whenever you click a particular website where you want to buy something you can see those kinds of advertisements on the other side. It's very intuitive, but sometimes you get a good deal, but it's very suspicious I must say.	ABP
43	I	How important is a proactive approach towards privacy in data analytics?	
44	R9	So again, it depends on the project. So, for example if we were talking about services within the bank sector, a banking site, then it is very important, and a proactive approach is required. But if I am going into a particular website where I need to sign up, and if it requires too many security questions, I will not sign up.+	PP
45	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
46	R9	In broad terms, I must say its very early age for privacy and it's dependent on what country we are talking about. For example, sometimes people are not so concerned about their privacy in certain countries. They are not concerned because they don't know what people will do with their data. People are not aware. Awareness is very important in terms of privacy and privacy should be very easy to understand. Now if you need to understand privacy it is a long list of terms you have to read, and no one hardly reads it	PB SPF RUP
47	I	Thank you for your time! We really appreciate your contribution to our research.	

Appendix 11: Interview Transcript (R10 Sweden)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R10	Sure.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R10	I would say it depends on what I say. Let's get back to it later. I might say things that my company is not okay with.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R10	Currently I'm 1 out of 12 UX lead, it is not a lot, considering we have 3000 employees. But we are getting there, when I started, we were only 3. So, I work as a UX lead, meaning I could work everything from alone to a project and team together with other designers. Until recently, I was the chairman of UX at the company. Leading our cooperative work. As a UX designer you often work more or less alone. And you are assigned different projects. We are also running a pilot program, so I'm working on a not yet released program, my responsibilities in that is to on one side to have the close relationships with the field test customers. So that is one part of my job, for instance doing these kinds of interviews that you do and supporting the customers when we are trying different products. The second part is the responsibility of the UI design, and doesn't necessarily say I have to design everything, but ultimately, I am responsible for the end product. That is basically my work right now. I work very closely with the product owner. So, we sort of go through interviews together coding up interviews and you know, look at my recommendations and what the market is saying, and we build a road map together. And yeah, it's a very broad sort of work	
7	I	How would you define privacy?	
8	R10	Privacy is not so much to being left alone, respecting your privacy, your right to remain anonymous and respect your integrity. I would say that our world really doesn't look like that, so in mind privacy is that users are given opportunities to be a part decision making. Like the right to be forgotten,	BRNR

		I don't believe that privacy should be that everyone is anonymous all the time, but I think users should be given the opportunity to affect it.	
9	I	In your experience, when is privacy implemented in product development?	
10	R10	I think I always have it in the back of mind. And when you start projects you have close contact with the legal team for instance, depending on what you work with obviously, but the legal team and the IP team is always a part of more or less of product development. Let's say like this, it's a part of the design, but it is not really my responsibility. It is up to people on the legal team to make sure we are doing everything within legal terms. With that said, I mean just because it's legal doesn't mean that you have to do it. I can give an example like when you create a MyAxis account, which is basically, every company that uses Axis products because that's the sort of way to download products or software and to register your devices for warranty and that sort of stuff. And I mean basically when you register everything in the terms of agreement and you know the disclosures points towards that, you know, we might collect some information from you, some information from your use of the product, some information from your devices and so on. So legally we're clear, when doing that. And also, when you download a software for instance, you have that sort of agreement once more for that product, you know, so that the first one is quite general and then it's part of the product. So, with that said we always, and I think I can't think of a product that doesn't do this. That when you actually log into the product, if it's a software you always have the option visible from the get-go to opt out and in some products opt in. Like yes, it's okay for you to start collecting my info or you know. That's actually placed in the products that I work with at the same page where you actually sign into the product. So, you never get anything before that page because when you actually sign in you login into a program from that point everything starts to spin. Everything is collected. But if you place that option before you log in that's you know, nothing. Some statistics if you are interested. When we place it as an opt out usually it's I think it's less than like 15% or something that actually you know opt out. And when it's opted in, I think it is closer to like 60%. But given the industry I'm working in there's not much no fuss around like keeping privacy.	PP, PED GDPR, CCPA, RUP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	

12	R10	If I'm honest, I have way too much to do to sort of dig into that information. I couldn't say.	
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R10	Yes.	GDPR, CCPA
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R10	Yeah, a little bit. Actually, what GDPR did great was that it started to create headaches for everyone. I mean it affects our work in a way that I mean legal wasn't this involved earlier in the process like that definitely changed. Especially when you work with cloud solutions, legal is basically a part of everything. Like when you're planning features. It is there in the process, and they identify areas where we need to call in legal or security teams. Often it is the responsibilities of the project leader, to make sure that every competence necessary is involved. But they are part of the process from the beginning, from the get-go. Legal and IP. They are not considered being a part of the team like a project team, but we have people assigned to that project, you know to be responsible for those sorts of legal things. Talking about our field testing, and coming back to GDPR, if we receive requests from people asking to have their information removed, we remove it.	GDPR HE
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R10	Yeah, I think so. I mean it's not super easy to understand. I think you have to separate the organization ID and the product login or the product use. They are connected because they are not really the same. So your question is that you know, do we make it easy to understand, I think when creating an organization ID for instance, when you create what we call a MyAxis account, you are presented with the terms of agreement and I don't really know if I've seen someone like, no I want to keep my information private. An example of a product we worked on before, we had a text describing exactly what we did. When we collect information users, we never collect any information that can help identify the person. That sort of op-out thing, that clarifies that part, like we are not interested in your data, but the whole product.	RUP

			GDPR, CCPA
19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R10	Yeah, I think so. I mean more importantly I see a huge competitive advantage in being transparent, and that's I think that's a big part of privacy as well. And this becomes extremely clear when you talk to customers, which I do every week. Additionally, I think it is a trust thing. Our company's way of working is based on close relationships with our customer and information sharing that goes both ways. And we are constantly working with cybersecurity issues and constantly working with making the product secure. It is not just about sales and that is why we are market leaders.	CA TV
21	I	Are you familiar with the concept of Privacy by Design?	
22	R10	Not really. I am now though.	
23	I	What measures do you take to prevent privacy breaches?	
24	R10	If you look at the product I'm working on right now for instance, there is nowhere in that product where you as a person are exposed. There's no way for you or a hacker to find a form or something presenting your name Esther, your phone number and so on. There is no such thing whatsoever. What usually happens is that when you use the sort of product that I'm working on right now is that you use your company name. So, we asked for the organization's name and they can put in whatever they want to put in. We don't really care because we don't use that in any way, but usually the customer puts in their company name. I have never seen that anyone put in their personal name, except for my colleagues. So basically, we protect ourselves by not gathering too much information. I can say this, like we have endpoints, like some go to VHS or ABS and one goes to Google analytics. And we met last week where I said, you know, what does Google analytics do for us anyway? So, my point is, if we dont it like a dire need to collect anything, then we simply don't do it. We avoid collecting data we don't really need. Another example, I know that a lot of products do this. When they start designing a product they go like full crazy and collect everything. When you've done that for a system and then you look at the data, you don't even know what you are looking at. There is no way you are going to figure out anything on this data. So, the designers I know are really doing it in reverse. They are actually asking the questions and what you can do with the	PDS GDPR

		answers before actually putting it in. In our case it's actually like this. We have a template with three lines, it is basically this. I can't remember it word for word. But given we had this data, given what the data is saying, what are our actions?	
25	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
26	R10	I mean there's not much data to be honest. I mean some mail address. For instance, if you use a cloud service no matter what sort of service it is, you always have to sign up. And when I use the app, sometimes I wonder why I even have to sign up. But when it comes to our company, we don't have much information about you. Our mission is not to gather information that can be linked to a person. There is optional information there of course. But we are not really interested in the person per se, we are interested in the company behind the person, like how many employees they have or what kind of business they are in.	GDPR, PDS BRNR
27	I	That's great. That's actually one of the principles of privacy by design, data minimization	
28	R10	Oh, then I am using it. The reason why I am doing this and how I learned this is because I made the mistake of actually trying to collect everything. Collect all the data. I think it is quite common as well. And it is so easy, like if you are working on a new project, to say yea, let's go collect all data. The easy answer is always to collect everything. The hard way to do it, which we are doing, is by doing templates, conducting workshops and discussing what kind of data we need and which questions we can answer with different kinds of data. It takes time of course, but it saves you in the long run. Less headaches later on	PDS
29	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R10	No, not at all. Actually, I would say the opposite. It makes things easier to be honest.	RUP
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
32	R10	Yeah, well as I said we don't really have much data. In my experience, I haven't seen any reason to collect and use	PDS, GDPR, BRNR

		information that would identify you as a person. It is a lot of work behind, too much work behind it	
33	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
34	R10	No, I think it's good. Of course, in some businesses you have to collect personal information. But in our business, it really doesn't matter who says what. And in those businesses, I think it is important to give consumers the maximum privacy as a baseline. Or in any business where they are using personal information.	PDS
35	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
36	R10	I do not think so. At least it shouldn't be	FF
37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R10	I mean what I'm working on is IoT. When it comes to IoT, what you're interested in as an engineer, or as a UX designer, is the devices, not the person. But of course, it is important as the devices require personal information.	IOT, PED
39	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
40	R10	I don't like it at all to be fair. Companies are coming up with more creative ways to do it as well, which is even worse.	ABP
41	I	How important is a proactive approach towards privacy in data analytics?	
42	R10	Yeah. If you work with systems and I use the term systems, you sort of have to be proactive because you will create so much work for yourself and it will always come back and bite you later. But it can be hard to be proactive of course, because you can't know everything.	PP
43	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
44	R10	No. Those were good questions.	
45	I	We want to hear about your final decision on anonymity	

46	R10	If it helps you in your work, you can use my name. If you want to write that I work at Axis that's fine too	
47	I	Thank you for your time! We really appreciate your contribution to our research.	

Appendix 12: Interview Transcript (R11 Ireland)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R11	No, of course record away.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R11	You can use my name and my company name.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R11	I studied graphic design or Visual Communications in Ireland for four years and in Dublin focused a lot on all aspects of graphic design. So, you know, a lot of people who finish my course would have went into jobs that are very specifically branding and then as part of our course we did a lot of coding and UX because it was well, that's six, seven years ago now when I graduated so when I started I think UX design and UI design was only really coming to the forefront, but we were lucky that that was actually what we studied and, all of the other fundamental design principles were so key in being able to move into a job like mine at company Y. I won a competition that our college course did with company Y Dublin when I was in my third year where we had to design something specifically for them and then they kind of had a winner and they did an interview for an internship. So, I interned with them and then when I graduated, they actually asked me to come back and work for them. I've been working here for nearly two and a half years three years now and that's where I've been. So, a lot of the work that we do here is very heavily UI/UX focused. It's very based on a lot of digital transformation projects. We help companies who may be way behind in sort of where they need to have digitally and actually brought them into a more marketable place where they can then and actually kind of thrive in that area. So, a lot of the stuff that we do is we take old business processes and actually bring them online which is really good. So, I've worked kind of across different things. We do a lot of creative work as well. But I've been on products before we designed a huge product for a pharma company in America last year,	

		which was essentially to help them and build these kind of like emails for themselves and we worked with an investment company last year, which was one of my projects which was more of like they didn't have a good digital presence. So, we've kind of brought them online a little bit and helped them to figure out how they could get new clients online rather than in a kind of an old school way. And then at the minute I'm making a really interesting product for a company that I can't say who it is. There are a few companies that are going to buy this but it's essentially a right to work product which means that you know, when you travel to different countries for work, you actually have to prove you're right to work. So, you have to submit all these documents and at the minute it's a really manual process. I'm trying to bring that digitally online. So that users can actually get a link from their new employer and upload documents kind of like you do when you know, join a digital bank and you verify your identity online really quickly, so it's kind of like that. So, it's kind of like that. So that's kind of what I'm working on at the minute, which is super exciting, but that's just a really just a quick snapshot of what I do, but there's lots more in that as well.	
7	I	How would you define privacy?	
8	R11	It is an abstract question. I guess if we look at it through a designer's lens, privacy is quite important, right? First of all, it depends on your product, it depends on what you're building. To certain degrees, you won't need anything like that. But if you have a very client-facing product you need to consider where your client wants to import certain privacy settings in terms of conditions. So, when you say privacy I'm thinking of terms and conditions in my head. Okay. I think I don't know if I can elaborate on that anymore. I guess it's more so like just stressing the point that privacy is really important. No matter what you do, especially in a world that we're so hyper conscious about GDPR and you have to be very sensitive with how you lay out that kind of data and how you actually bring that into a product that can be user-friendly and yeah.	
9	I	In your experience, when is privacy implemented in product development?	
10	R11	Okay, so if I think about the way that we work depends, of course on your project, you know, sometimes you can get a project from a client that's very specific and they know what they want. They know what they need to do.	PP

		We do these things called imagine phases where we actually go in and we discover what your problem is and make sure that what we're designing is actually the correct solution. So, a lot of the time you'll think about that kind of stuff there, but it really happens when you actually start to wireframe out your idea, right? So, for the product I am working on now, I'm going to use that as an example. We wireframe that very early on and as it was just a test concept and we were giving it to our clients to kind of like play around with and see if this is something that they want and if this is something that would suit them then you know privacy is not really thought about at that point. Okay you are going to have a few screens here and roughly in this area you're going to have to sign some terms and conditions, but because the projects are not ready yet. Then won't we think about it that much, it's when you actually go into detailed design and sort of prep for development that you're like, okay, so if we're going to develop this thing now and there are going to be somethings that we need. So the designer will always design at their screens and create their specs to make sure that the whole product is fully fledged and then that has to be signed off by the product owners and all that kind of jazz, but at a certain point then you obviously need your content for everything which is where then your BA, their business analyst, the person that you're working with your development team and with your product team, they will then feed into and the content of that so you'll have to reach out to all of the necessary people that need to be involved in writing that content and often those are legal teams. So, it always kind of happens in that detail design phase where you kind of need it because you need that stuff before you go into development. You can go in with less content, but it's not ideal, you know, it's not ideal for a developer and it's not ideal for a product owner who needs to sign off on stuff. They need to see the information and a designer needs to have a good indication of well, how much information do we need to get on the screen? I would say detailed design is when that happens.	
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R11	Okay. So, for my organization, obviously, we're Y digital which is a sub-brand of company Y. I don't know if you guys know company Y, but company Y is a huge accounting legal firm. So, when it comes to stuff like that where very well equipped it's actually harder for us to actually guess these things done because there's so many	

		people and so many regulations that we have to follow under. Whereas I would say if you had a smaller product company or a start-up they maybe wouldn't have as many barriers to kind of come again. I don't know if that is a good thing, you know, they might probably not have a security team, have a risk team, they don't have a legal team. They would probably have to consult with someone right, so depends on your company, but for my specific company because there's a risk and legal and security team all these things have to go through them. So, for my specific product, and I'm just using what I'm building at the minute as an example. One of our business analysts had to reach out to the legal team and ask them what kind of information they needed. The legal team then came back and said this information has to go here, this doesn't have to go here, this kind of has to go here, but we have to give it to them. All of this information, it was like information overload which made it quite hard to design. So that's how our company is so kind of hyper aware of security and bring that they're very good at that. But again, it depends on your product, depends on your company, depends who you're building for as well. So, we've built this privacy based on what our company wants, but that's not saying that the companies buying the products want that, or maybe they won't other regulations there as well. So that will have to be considered too.	GDPR HE
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R11	GDPR yes.	GDPR
15	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
16	R11	I'm going to answer it as best as I can. I'm not good with the regulation or the policies and I don't know them in detail that's why we have teams who do that. It's more that I'm given the content that is needed for me to design in a specific way, that's user-friendly. That's my most important responsibility. But it also kind of will come into play when we do user testing because it's all about how the user feels about what we are trying to do and get them to do. I'll understand why the policy and regulations are required. I understand that. I don't really work with it in detail, if you know what I mean. I design it and my focus is does the user understand what we're asking them to do rather than to actually write any regulation or	RUP

		policies or be part of that essentially. There are times where I would disagree with things as well, you know, because there's times when legal teams will come to you with ridiculous reasoning about, well, something needs to be on this page or this particular link needs to be here, but they're not actually consented to the link and then you know, you have to think well why do we have to show what then, because why are we showing something to a user that they're not actually consenting to. We should be showing them what they actually have to consent to so there's always a bit of battle there because legal teams tend to be very like we need this, we need this and we need this, but in actual fact they compare that a lot more. And it makes for very complicated designs sometimes because they come to you with like, oh, we want this here and here and here. That's what happened with my product. I designed several screens for them and nothing was legally okay, and they were actually coming to me with saying we want it in this way which isn't really the right way to do because you should do it in a way where your UX designer takes the lead on how the page should look and then you user test to make sure that the user understands it and then you work that way rather than a legal team coming to you saying it has to be laid out in this way.	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R11	I would say no, I would say that is my job to do. One thing to remember is a lot of time people don't read your terms and conditions they just don't do it and that's something we found in a lot of cases. I think it depends what you use if you're building like a banking product or if you're building sort of something to do with investments or where maybe there's a lot on the line your user will probably be like okay what am I signing up for here but in our in cases that we've seen that they don't actually read it, but it isn't important to understand especially when you're making a sort of one-off flow. It's not like you're making a fashion website or something where you're going to ask them to accept cookies. It's a little bit more serious. So, you kind of have to take it seriously and assume that they're going to take it seriously as well. I mean, it's tough like but we really try to make sure that what we're showing on that screen is understandable. And we're about to do user testing this week with the product. So the current screen that I have there, when I was writing my script I was like, do you understand what's being	RUP

		asked for here, would you read this, are you comfortable with proceeding because it's all about making sure that the user feels comfortable with what they're about to do.	
19	I	Yeah, absolutely. Obviously, no one reads terms and conditions. But do you think there is a way of displaying them in a more understandable fashion?	
20	R11	Yeah, for sure. And I think that's the battle that you have when you have too much legal involvement. I think there's a balance right here. You're better off having really good legal advice or risk advice on these things. But you know, sometimes it can be a bit too much and get overloaded which is what is happening currently with me. But yeah, I mean you have to make sure that the information on that screen is digestible because if it's not, you know, you're going to get people who arrive there and be like, wait. What am I doing? What am I signing up for? So, it's just about making them feel comfortable and you know using appropriate language which isn't always possible. But you know, you do your best with what you're kind of given.	
21	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
22	R11	For sure because you know, if you've got really good security risk advice with your product, then you'll be guaranteed down the line that if something goes wrong with that product or if some user is looking for their information or asking questions, or if your business is going to go into an audit that you're fully covered with that and that you've got everything sorted. So that's what I mean about having a good balance. You know, you need to make sure that everything is right and above board and making sure that you're not hiding anything. That's the most Important thing because if you hide something then you're going to get in trouble. So, there's definitely an advantage to getting good advice and you know consultation about that kind of stuff, but it is a battle. It's a total balance and act	CA
23	I	Are you familiar with the concept of Privacy by Design?	
24	R11	I see, so it's essentially just using the principle of thinking about privacy way earlier than when a lot of places will just implement it when they need it to. So, I haven't heard of it used in that sense but it's definitely something that is like an ethos that you should think about it when you're designing products like that. I mean from the very first	

		ideation phase, privacy probably is not the main thing that you're going to think about, you're thinking about what the problem is, what the process is. So, it definitionally comes in later, but it should probably be brought in earlier so that you can improve your experience based on it, you know? Like well we have to ask these guys a bunch of these questions	
25	I	What measures do you take to prevent privacy breaches?	
26	R11	I wouldn't be able to tell you for sure. I think definitely maybe find some like legal people or risk advisory people that you can talk to about that. But I mean measures from what I'm saying on my end is that there's a lot of back and forth with legal, right? They obviously have a set of benchmarks that they make sure that they're covered off. So, for a different scenario. So, for our scenario our product probably fell into a certain category that they have, and they were able to be like okay here is what you need to give to the customer based off this particular product. I'm not sure the exact categories or benchmarks that they have but it seems very rigid and very structured. I assume that it's quite a difficult process but know any detail about that really.	HE
27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R11	And again, I assume that's written in the terms and conditions, right? So, if we're, I'm thinking of the product that we're doing now, we're not asking them for that many personal details, but we're asking them to submit biometric documents, it's proof of your identity. You have to submit your passport. So, the terms and conditions are very focused on biometric documents and these biometric documents are used to prove your identity for x, y and z. Very specifically its kind of has to be called out. I wouldn't say that when I'm asking the question. So there's three questions we ask them in the form which is confirm your full name, which we already know because we've got that from the client, confirm the second name then give us your country of citizenship and that is to kind of a security measure to cover when you submit your passport. I wouldn't be designing questions and be like, by the way: I don't use this information for anything because that just makes for quite clunky design that you don't need. I think if you were to be really clear about it at the beginning. We have onboarding screens; they are not	TV, GDPR

		onboarding but just a screen we flick through to say we're going to ask you for some personal details. Whereas in that section I could put something like these personal details will only be used to verify your identity, and all of your information will be sent straight to your employer. So, it's about being kind of transparent in that way rather than kind of overloading them with by the way, we're not going to use your data for anything.	
29	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R11	You can sacrifice usability a lot with terms and conditions. That's what's happening to me at the moment. It's having an unpleasant screen because legally they're required to see all of this information. A lot of the time you can't really get away from that, from a UI perspective if your UI designer it is very annoying, but you know when you look at the rest of the business, mandatory information. So, you really have to do your best to figure out how I can lay this information out so that it's pleasing to the eye because that's what we want. But you know that we're legally still down the right road that we need to be. So, you sacrifice your look and feel and your design a lot when it comes to these things and your kind of just have to do the best you can do. Additionally, here is where user testing enters the process and why they are so important.	RUP
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
32	R11	So, in relation to the product I'm building we obviously gather data for a very small amount of time. We verify that data and then that data goes into another platform that we're using for the backend system and then after a week that data is then flowed straight back out. We had a lot of conversation about how we as a company didn't want to hold the data because it's not our job to hold the data, it's the employer's job to hold the data. There were a lot of conversations happening and they happened in architecture. So that's when a lot of those conversations are like well if we wanted to hold the data then we would need extra space or storage, or we would need to figure out how our company does it. So, a lot of that stuff will happen with kind of tech architects and developers and designers as well. Once they made that decision. Well, we don't want to hold the information then that makes it very easy, right? Because we were only housing it for a certain amount of time and then it's gone. It's gone to the	PDS, GDPR

		employer and so I guess for us those measures come in a lot earlier because that's all about the architecture. Tt's all about the product architecture that will decide what we do. I mean it would probably have been a more in-depth conversation had we said okay will store the documents after somebody's verifying. Do you know what I mean?	
33	I	Yeah. That makes sense. That means you are actually implementing privacy by design unknowingly because it advocates for not holding personal information during a time when you no longer need it	
34	R11	Exactly, and that's what we're doing, you know. So, one of the platforms that we were using. I don't know if you guys have heard of Salesforce, but that's our back-end platform that we're using, and we had built in well how long do we want to hold the information for? Okay, we will hold it for a maximum of two weeks. And after the two weeks are done, it's gone, but that's only for when you have a manual check, when a check is completely okay, like it's gone the next day. So, our developer built in the time frame that is set, so that's decided much earlier.	PDS, GDPR
35	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
36	R11	I don't think it should be default. I think as much of a pain that is, you need to forefront privacy and you need to make sure that people are okay. In a lot of context, they don’t have a choice right. So, for our product if you don't tick the box, you're not getting through the rest of the flow. It could be default, but you have to give them the information up front so that then they know what they're signing up for essentially. When you go into websites, there's the accept or decline kind of cookies button so it depends again on your product, I guess. If you want to you can have a message that comes up on a website that says we have defaulted accepted on all your cookies. I don't know what the language is, but if you need to change it like click here, but I always think it's good you might as well just give them the option so that they have been presented with the rights and that the company is completely safe then you know what I mean?	PDS
37	I	Yes. Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
38	R11	Probably I would say and again depends on your company. If it was my company, they would probably be	FF

		like make sure your privacy is there because of who they are. If you're a smaller start-up you would probably know default to a very basic level of legal advice. I don't know, maybe it depends I guess, and I don't know if there's a real trade-off I think people do think about, especially now and especially depending on what the services your building is, right? So, something like a website might not be integrity focused as something like a banking app. So, it really depends on what you're building.	
39	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
40	R11	I think there is a fear about having privacy as a default in the sense that does it mean that you are hiding something? That is a tricky one. I don't know how I feel.	
41	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
42	R11	So, I'm biased because of this. Because like I said we do a lot of creative work as well. Okay, we are very readers in how to listen to people online and then market to them accordingly This is my personal opinion. I don't care if you advertise to me you can advertise to me all day long as long as it's relevant to me. So, if you're going to show me some good stuff then I'm delighted about that. You know what I mean, but it is annoying when they start marketing weird things. But I don't really mind it. I think it is very good if you do it right. I'm biased because we are the people behind it, but I don't know how on the other side feels.	ABP
43	I	How important is a proactive approach towards privacy in data analytics?	
44	R11	Data analytics. Okay, I don't really work too much with data analytics but a proactive approach to privacy as you know in the design and in the initial scope of the product is super important. But you know when you're gathering data, I think it's important to know what your limits are with things like that. But I think it is very important.	DA, PP
45	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
46	R11	Do remember that different products and services require different privacy approaches. Think about how it is different when you're creating privacy for normal fashion website or like a blog and compare that to a product	

		where you're gathering biometric data. There's different levels of privacy and different categories and you know; the approach has to be specific to what you're doing. I think having a proactive approach is amazing. I think implementing privacy very early in your design and wireframing is super important as well. And I think people do that, but maybe it just falls to a "You know we probably need privacy somewhere here" kind of thing and you don't really think about what you're asking the client or the users. But you know, it does depend on your team, depends on your employer, depends on your client. These things can vary from company to company. I guess a standardized approach is probably the best way to do it which I'd say legal teams do have. I'd say all legal teams all around the world share similar benchmarks that they have to come under and that's kind of their job. So, for a designer, it's all about making sure that you get that information and you distil that information into a really user-friendly way so that the user feels comfortable with what they are accepting.	PP
47	I	Thank you for your time and stay safe! We really appreciate your contribution to our research.	
48	R11	No problem. I hope that was helpful	

Appendix 13: Interview Transcript (R12 UK)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R12	No, it's okay.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R12	Yes, anonymous please. You never know.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R12	Of course. Currently, I am a product designer at company x, combining UI and interaction design skills with lean UX thinking. I am based in London, United Kingdom and I have worked with design for over 10 years, always with a passion for digital products. I prefer to work on digital products from a very early stage, from working on the concept of a product to experiencing the positive impact it has on users when it is finished. Usually, my responsibilities consist of leading user interviews and testing sessions typically. Is there anything specific you want to know?	
7	I	How would you define privacy?	
8	R12	I think in general privacy is, you might already have heard of this of course, but it is a fundamental right for me. It's very important and it's anything that is related to your personal information and the share and use of your personal information. That's how I define it.	BRNR SIS
9	I	In your experience, when is privacy implemented in product development?	
10	R12	It depends. I think it depends. It depends on the product you're working with and of course the uses of data that you do. In the last for the past three years. I've worked in marketing, so data is really important and as you know, some companies thrive and live off data. You know Google and Facebook amongst the big ones and the ones that crave data more than others. So, I would say it depends. A product can be built privacy friendly by Design or it can be built the other way around depending	

		on what kind of product it is. I think privacy should be involved in the early stages of any procurement development in some shape.	PP
11	I	What does your company do to make sure that the right privacy protection practices are in place?	
12	R12	Again, I can't speak on behalf of our company in this case, but what I can say is what is out there, and you know our company cares about privacy because it's not in the business of selling data, you know, our company sells hardware and services but not data. So, compared to some of the other giants it is a very different proposition and I think in general from I see they are pushing this aspect very hard as a differentiator from others as well	PP, PDS, CA
13	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
14	R12	I think I am somewhat familiar, but it is difficult to understand, I haven't gone into it in detail	GDPR
15	I	Have you worked with privacy protection before these regulations? If yes, how have these regulations affected your work?	
16	R12	Yeah, absolutely. I think my specific work maybe not but the engineers that work with me that build stuff that I design, then absolutely in a very heavy way.	
17	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
18	R12	I think so. I'm very clear. So again, I think our company has a big focus on privacy so it is trying to push and make privacy clear for users as much as they can.	RUP
19	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
20	R12	Yeah, absolutely. Personally, I care a lot about this specific subject. I have seen excessive collecting of data just because they can collect it. They collect anything they possibly can and then pass it into different services and store it there for no reason. That is a very silly way of collecting data. And it would affect my choice of course.	CA

21	I	Are you familiar with the concept of Privacy by Design?	
22	R12	I'm not sure about the concept itself but I am aware of the principles of implementing privacy by design. Yeah, so yeah, I am familiar with that	
23	I	What measures do you take to prevent privacy breaches?	
24	R12	I'm not an engineer, so I don't really come in contact with data. Because I don't use data directly in the design. I'm not the best person to ask in this context. But I know in our company, all the data is super protected, and we have a lot of regulations and it is very difficult to access any databases. There is a big legal department that deals with that. From what I know, internally there is a lot of work with those legal aspects and it is difficult to get access to any information really. Secrecy which is a bit different from privacy is also a big part of our company.	AR
25	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
26	R12	I wouldn't know how to answer this question. I don't directly deal with that sort of development. I build internal products, not anything that our users will see or use.	
27	I	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
28	R12	I think by building products with privacy in mind definitely limits what some companies can do. When it comes to data collection, and anonymous nature of privacy, you don't know who the user is. You know what phone they have or if they have downloaded an app but you don't know who they are. So, you can't send an email saying like "Hey Arman thanks for downloading this application, you are now part of our family. It is hard to be personable. So, yeah, having privacy built in and in mind definitely comes with some limits compared to other ways. But I think there are ways around this problem particularly, again it is just a matter of shifting your way of thinking.	FF
29	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	

30	R12	Again, I'm not the best person to answer that because I'm not an engineer.	
31	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
32	R12	I think it's a better place to start for the user as opposed to everything is not private and they opt-in because that's how your mind actually thinks. You know if I meet you, I know what you look like, but I don't know your name, so you're private by default. So being privacy by default mimics more human behaviour. Something I do with users especially, you've got to be able to think like the users, you've got to understand how a human person thinks. You know they might tell you I want to achieve this but then you've got to figure out how to go about it because you know, there could be million ways of doing it and you know, a classic example is, somethings are very technically complicated. For example, a segmentation. Let's say we extract a segment of users from this country, and users who speak this language. And you know a database query looks very computery. Boolean algebra and so on and that is not how a person uses it. So, mapping a human language to that is difficult so sometimes you just have to think how a person thing and then build your queries to reflect that basically.	SIS, PDS RUP
33	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
34	R12	It depends where you start from. If your company is selling data at the beginning and then all of a sudden there is a shift where they decide to be more private like for example, Facebook is doing. There has to be a trade-off, you can't be more private and keep doing things the way you used to do them. But if you start from scratch and privacy is a core value of your company, then there is no trade-off, you just build it in the way you want it to be built.	FF PP
35	I	That means, when you implement privacy reactively, like an after thing, then there is definitely going to be a trade-off.	
36	R12	For sure. Depends on the company as well. Facebook for example has a lot to lose in terms of public image, which means they have to focus on privacy more and implement more privacy measures, but without compromising their business, because at the end of the day they are an	

		advertising platform. They need to sell data. So, they can't compromise that.	
37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R12	First of all, I think it's possible. I don't think it's even that difficult to embed privacy in any product including IoT or a technology. It's just a matter of doing it and doing it at the right time. It will definitely bring advantages because people care about privacy, and they will care more and more, and if you are able to sell that point in your products whether you are building software or IoT, it will be an advantage compared to others now until it is fully regulated.	PED CA, IOT
39	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
40	R12	It depends how you do it. There are examples of positive use, an example could be more targeted advertising meaning that it's something that is more personalized and relevant to you. As personable as it can be, but it is still advertising of course. The negative thing can be that you are just bombarded by the same thing over and over again. But that is not because of a fault in the system, it is how the company uses it, because there are ways in place for that not to happen. Like if you target people in real time you can choose to display the same banner or message a hundred times or just one time, but you have to build it in by design.	ABP
41	I	How important is a proactive approach towards privacy in data analytics?	
42	R12	A proactive approach, I think it's really fundamental, it is beyond important. When it comes to data analytics especially, it depends for what it is used for, but companies use it to understand how well they're doing and how some products are performing in certain areas. They don't need to know everything about the users, all information is not required. You need to think about what kind of information is required and therefore it is very important in my opinion privacy in that aspect is built in.	PP, DA
43	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
44	R12	In my world, in the UI/UX design world, privacy has been a big thing exponentially for the last three years. Along	

		with the implementation of GDPR and such regulations, UI designers really started to question themselves on how to build these aspects into the UI. They are of course making decisions on the products, but it is the decisions of the business as well. But engineers and designers have started to bring privacy into the discussion and onto the surface.	
45	I	Thank you for your time! We really appreciate your contribution to our research.	

Appendix 14: Interview Transcript (R13 Australia)

Row	Person	Transcript	Code
1	I	Do you mind if we record this interview?	
2	R13	I don't, go ahead.	
3	I	Can we use your full name and company name? Or do you wish to remain anonymous?	
4	R13	You can use it.	
5	I	Do you mind telling us a little about your work experience as a design practitioner and what your company does? What is your current work position and responsibilities?	
6	R13	Sure. I began working in design many years ago, before there was the official job title of product designer or UX designer. So I was a front-end developer when I first started working in tech and I was working for different companies in Australia that were making organizational websites for companies or government agencies, and I moved into the field of UX by accident because I was changing people's designs without their permission and then I was forced to meet with the stakeholders from these organizations and explain to them why I was making these changes and eventually that sort of became my job, which was improving designs for organizations as they pivoted over from typically physical interactions like banks with branches or government agencies with branches. And at this time, they were getting mostly, I think their first or first proper digital presence, so websites and what have. And then I worked in the banking sphere. I ended up getting a lot of contracts in banking and finance. So, this was dealing with customer sensitive data, so dealing with organizational transformation projects that involved online accounts, so people and their money. And obviously this is a bit more serious than maybe just changing a website for a, you know, telephone company and changing their front-end digital presence. But this was back end and login, so secure. Yeah, and I remember I've got some really great advice once from a colleague and a senior manager at one of the banks that I worked at and he said what we're doing is like avionics you only get to screw it up once because when you make a mistake in avionics the plane crashes	

		when, you make a mistake with people secure banking, they can't feed their kids, you know, and people lose their money. So, the trust that is imbued from the customer into these systems has to never be broken and it is hard fought and won to you know for these customers, but yeah, Australia has similar to the EU, I think Australia has some very stringent customers. We don't have at this stage anything close to the GDPR, but we always had quite stringent and quite sensitive privacy laws that protected customers. So, organizations in Australia were kind of incentivised to do the right thing by the governments of the day and this ended up transitioning my career over. I was doing some high profile projects for some agencies and then I ended up getting a position at Google and I was working in Mountain View in head office and that role was a product design role so dealing with actually what we're using right now is one of my products so Google Meet. Yeah, and I was also working on some other sensitive projects that have not yet gone live, but it was mostly dealing with consumer facing products that Google offered their customers in both Enterprise and consumer land and end users, but I prefer to say customers. Yeah, and I worked at Google not too long. Actually. I was there just under two years before I decided to leave and make a start-up. Then I left Silicon Valley and moved to Berlin and began working on a deep tech AI consumer product called Simby and that's still what I'm working on. It's a start-up so I don't know if you know much about start-ups, but they tend to fail. A one of our one of our difficulties was to do it right. There were a lot of tensions. Because we made a promise in our manifesto that we would never sell customer data, which was you know, a very bold promise to make. It was very important for me and our co-founders. But when you try to meet with investors and raise money, it gets quite difficult to discuss how you're going to be profitable when you've made these promises that you will never sell data. Now there are a million ways to make money from customers especially if you're offering a product that does something no other product does which is keep them safe, but investors have very narrow short term opinions about how money and start-ups become profitable so I can speak a lot about those tensions. And also I think there was a lot of extra work we had to do when we were setting up our tech stack because a lot of the out-of-the-box software and plugins and you know programs that you use are designed for this world where there is a customer who use name, you know whose phone number you know whose email address you know, so we really struggled at the very beginning with the way we began because we knew what our promise was but we had to re-	

		engineer a lot of problems in very innovative ways to get around very simple things that are solved like that if you're just willing take a customer's email address. And so that was one challenge, well many challenges, which I am happy to speak to you about if it's interesting to you, but that's I guess my background and now I'm in Australia because I decided to take the start-up out of the finance space with investors in the typical sense of doing capital raising where you dilute the company and kind of get on your hands and knees and beg and we are going to look at possibly finishing our attempt at this with a Kickstarter campaign and we'll see what happens. I don't know if we're going to do it, everyone's just lost their jobs because of coronavirus so it's maybe an interesting time. But the project was a labour of love for me and it was more about being able to say that I tried to do the right thing and that I offered the world a product that we could look back on one day and say hey, wait a minute, they were on the right track. I don't know if you saw this in the film that we made but we made a movie that was I think 20 something minutes long check it out, if you go to Simby.com, and we talked a lot about the issue of privacy and data. But yeah that movie for us was our sort of stake in the ground and saying hey we offered you this world, you can take it, or you can leave it. That's fine, but I don't want you saying you weren't given the choice one day, you know. Yeah, so that's the background.	
7	I	So, how early do you think you are with your idea?	
8	R13	Oh, way too early. Yeah, and this was always. My problem as a designer was this issue was that I as a little child, I would I was always trying to finish the tests that were in the year after the study of my year and I was always leapfrogging not because I felt I was smarter or anything. I just was more interested in knowing what was coming than being present. It Makes me a bad Buddhist, but maybe a good tech designer because I find it very hard to live in the now and I'm very focused on what's coming. I've met people like me at Google too who also struggle with this chronology of time and end up being very much focused on future related challenges and problems. And that's why I think Google put me in a position to dream up some products. Because they want people like that who are thinking of the challenges of the future. My struggle was that is that they never get built. So that's why I decided to do the start-up because I thought there would be more chance in a small team not influenced by money so to speak and not necessarily influenced by some of the big factors that change things that Google and see what we	PP

		could do. So yeah, I think I would say we were five years too early.	
9	I	How would you define privacy?	
10	R13	That is a bit vague. Hmm, It's interesting because I'm an archaeologist. I studied archaeology and I studied ancient Rome and I think much of what we've learned about the past especially dealing with contemporary sources in ancient Rome for example comes from people talking about people and saying what they heard had happened. And I've been hugely enriched by learning about the history of our species because of what was written down about individuals as they did things. There was no concept of data privacy, you know back in 500 BC or even in 50 BC when a lot of interesting things were being written about the fall of the Roman Empire. And if we'd had GDPR back then maybe we wouldn't have learned so much about what we know about Rome. So, offered up the idea that privacy is this polarizing thing where it is 100% or zero? I don't believe that's true because I'm too dogmatic about it as this 100 vs zero thing may be impossible because it ends up with all of us having to walk down the streets with our eyes closed and our ears closed and not remembering or even me writing in my journal. That somebody by the name of Mary did something, you know, am I encroaching on her privacy? So yeah, it's sort of an it's a line rather than a black or white and I think we are dangerously at the dangerous end of the line and that privacy is the arrow in the other direction and it isn't a destination, it is movement towards a world where people are more empowered to take control of information about themselves, I would say. But I don't believe that we all have a right to, you know, completely control that. If I'm rude to a person in a shop and somebody videos me screaming at a shop assistant. Is it my right to prevent that video from ending up on YouTube? I don't know maybe not I was in the shop. You know, I was I wasn't I'm just using it as a hypothetical but If it was me and I was rude to somebody and it was captured. Do I have the right to remove that data from the history of the world, maybe not but yeah, but do I have the right to understand how data that I have generated has made multinational conglomerates money? Yes. I think I do have a right to know about that. I would say that the issue with privacy also gets mixed up with this like right to be forgotten versus Facebook monetizing my data, and they are very different, but they get called the same thing,	GDPR BRNR

		privacy. Yeah, and I think there's some stark differences between the two. So yeah, the long answer is that, the short answer is that privacy is a movement away from the chaotic end game where we have zero control towards an area where we do have control.	
11	I	In your experience, when is privacy implemented in product development?	
12	R13	So, with Simby this was our issue, that it is from day one. It's the very first page of the very first deck slide, you know that you put it together for your investors because you can't undo things with privacy. For example, if you have a server running with Google cloud or with Amazon AWS, that server is logging IP addresses, and you cannot not have it do that. If you have customers, who you make promises to that their data is private and that it will not be sold ever and that it will not be stored. Then you're lying right from the very beginning if you're using a cloud provider because no Cloud providers that I'm aware of are not logging IPS. So there's a lot of stuff that we had to do to purge that data on a daily basis and anonymize our customers intentionally so that if we ever got customers which we don't have any because we didn't go live but when we do and if we do go live our systems are established in such a way that we aren't gathering data that allows us to figure out who somebody is and that was our litmus test. We made the promise that we will never be able to know who you are. So, for us that that promise is laced with a number of caveats that make it possible. Right so we can't have your IP address because I could use that figure out who you are, with a warrant of course, but I could still use it. So that promise would be broken. Email address, name, phone number, GPS coordinates because if I have your GPS coordinates, I know where you live, which means I know who you are. So there's just so many data vectors that make it very difficult to not figure who somebody is if you try so our litmus test was: if served a warrant from a government in the world, we would be able to reply to the warrant saying unfortunately, we cannot help you because we do not have the data and for us that meant that we always had to keep that promise. We can't give it to you even if we had to because we just don't have it. And that's really, really hard. Especially if your operation is a consumer-based consumer friendly product because customers come to expect that these systems, these tools know you and they want to feel understood. Which means that they want to be discovered. And it's not important right now. Sure.	PP GDPR, PDS

		everything is going fine, but it's not difficult to imagine a world similar to the 1940s. There is a dramatic change in the political landscape that makes this data valuable to an authoritarian government or to a covert actor who wants to use it for purposes that it was not intended. It's not hard to imagine that will happen. So, another maxim that we had inside of our organization is that it is not a matter of if we will be hacked it is a matter of when we will be hacked. So we just assumed by default that one day we would be hacked and our responsibility was to make sure that after getting through all of the barriers of protection that were put in place the hacker would arrive at an empty room with a note from me saying: ha-ha, we don't have your data. And that was also very difficult because products need to remember, they need a concept of state. However, a lot can be done now with local storage and devices. So, we were able to solve many of our challenges just by moving all of our learning algorithms to the local device to run locally. It's called offline learning, but or sometimes it's called online learning which is weird because it's offline. But yeah, pushing things to the device rather than keeping the data that we need on our server. So yeah, that was one of our other challenges which I have illustrated by answering your question.	PED BRNR
13	I	What does your company do to make sure that the right privacy protection practices are in place?	
14	R13	We have very clear and very understandable broad sweeping promises that we make up front to our customers and to each other. We put them on the wall in our in our office so that they were very clear and we also implemented a system similar to when you're doing code deployments how there is a code check or like the quality of the code is checked and somebody does a code review. We also had a privacy review so we made sure that in addition to somebody being responsible to check that the code is valid, there was somebody who was responsible for checking that it did not break any of our promises that we made to our customers that we still didn't have at that stage. But we wanted to make sure we were implementing their systems right from the beginning. I wasn't any unknown thing; it was not some tact on privacy scheme that we added at the end.	TV, PP, PED, PDS
15	I	Are you familiar with regulatory frameworks that concern privacy in system development such as GDPR and CCPA?	
16	R13	Yeah.	GDPR, CCPA

17	I	Have you worked with privacy protection before these regulations? If yes, how have the frameworks affected your work?	
18	R13	No, in fact, our start-up was funded by an investment firm and the funding arrangement occurred right around the same time that GDPR was coming onto the radar, it wasn't yet in place but it was coming and our investor has a responsibility to contact all of their portfolio companies and say hey this thing called GDPR is mandatory. You must be compliant by this and as your investor, we have exercised our responsibility by informing you about it and our response to it was fantastic because we were just like: Hey, we're way ahead. GDPR is like table stage for use, we've gone over and above that. We are compliant before we've even started. And our issue was not managing to obtain compliance. It was to maintain compliance because we were compliant before we began. And what makes an interesting point is new organizations who begin today and receive funding or begin with a plan to create a company in Europe are not obligated to be compliant before they get started. They're obligated to be compliant from when data is being collected. So, they need to obtain compliance rather than maintain compliance and it would be an interesting concept to build into the creation of organizations. Are you ever going to capture customer data as a business? Most of them will have customers so the answer is yes. Then okay before you are able to trade as a business, you need to have maintained your GDPR compliance for a period of X days weeks months whatever it is. So that instead of it being this afterthought it is like hey, do you have a tax accountant? Yes, okay. Have you got your privacy compliance in place and is it maintainable? Yes. Okay, you know it'd be table Stakes to get into the game rather than this afterthought of like, oh, don't forget we have to also do that thing, you know, I think if they have built-in it would be a lot easier. It would be interesting to build these things into the establishment of organizations rather than it being an afterthought. To create a company in Germany, which is one of our subsidiary organizations, the paperwork was like two reams of paper of things we had to do and not one of those pieces of paper made sure that we prepared for the GDPR.	GDPR HE
19	I	Does your company make privacy regulations easy to understand for users before they consume your product or service?	
20	R13	Yes, we made it very clear at https://simby.com/data-privacy. We made sure that it was part of our product. So,	RUP

		it’s not like some terms and conditions in a very small font that we hide but instead we elevated it to make part of our differentiating value. The font was huge, you know, “we don’t want your data”. Additionally, on our page it says your data protection is more important to us than rainbows are to unicorns. Yeah, we spent a lot of time working on that to make sure that it worked because one of the challenges we also had was people were showing a lot of interest in the product and wanting to get to learn more about it. They were like trying to sign up or give us their email so that we could contact them when it goes live. And we have this challenge of how we store email addresses of potential customers and make sure that that never becomes a database of customers, so we had to build like a black box that captures the: signups that. And then what we did was we said, okay, if we do receive an email address from a potential customer who's showing an interest in our product as we build momentum, how do we prevent that email from ever being you know used or abused? It’s in a database right now with two columns next to the email address, no names and the columns are used once used twice and we make the promise that we will only ever use the email address twice. The first time to tell people when we're about to launch and the second time to send them the invitation to the launch. At that time after the second database column gets a number one in it instead of a zero, that row in the database is purged. So, we no longer have their email address and we can no longer ever contact them. If they were to reply to that email it would be brand-new, we would never know who they were, and it would be a brand-new receipt and we would have no idea how they got in touch with us. Yeah, so that was our promise, but I would have loved to have said we don't even want your email, but then we were in a pickle in that no one would ever know about when we were going to go live+.	GDPR
21	I	Do you see any competitive advantage in your business while you provide better privacy in your product or service?	
22	R13	Oh, for sure. Yeah, but just a few years from now. So right now, in a world where people are signing their grandma and grandpa and everyone up to Instagram. No one cares, investors don't care, even employees. One of our hiring challenges was that we wanted to find people who were ideologically aligned to our mission and most people just don't care so. Yeah, that was the challenge for us. But I would say in a couple of years from now, in the mid 20s, we will start to see that it becomes highly valuable that an organization behaves in this way or similar ways. You can	CA

		start to see it with Apple. So Apple figured out a few years ago that data privacy and protection was maybe one of their differentiators from a company like Google and a lot of work has gone into you know encryption and making sure that they that you know, those very public cases where they refused to give the FBI access to criminals phones and they're trying to make a stand whether they hold on to that is yet to be seen I don't know but I'd certainly appreciate the direction that they're headed.	
23	I	Are you familiar with the concept of Privacy by Design?	
24	R13	I mean I've heard of it. I don't know if it is concrete enough to be called in my mind like a concept. I think yeah, I think for us we certainly what we did was what I would call privacy by Design but whether there is some framework or matrix or checklists. I don't know to be honest. Also, with regards to data and the sale of data we said the generation of data is work. Right? So as a customer to create a data point that has value you have done some work be it, you know, writing a sentence or typing out a thing or tapping on photos that interested you, you've generated value in your work and then that value is being sold at a profit. It's being enriched and sold almost like a mining operation, by an organization. You as the generator of that work have no concept of what the value of that work is; you have no idea when or where the sale took place and you are not remunerated at all for the work. Now the last time an entire generation of people were working for free, we called it slavery and it was not okay, but at the time that there were slaves it there were there were entire cohorts of people who thought it was okay that you could treat people that way and now we look back on it and we say, oh my goodness. That was so wrong that is called slavery and I think we will do the same again about the sale of data in the future. For example, my shoe size is worth about nine dollars on Facebook. So, if Facebook manages to figure out what my shoe size is from a photograph that I take of my shoes or just how I walk, you know the accelerometer, there are ways to figure this stuff out, they could sell that shoe size for nine bucks. And if you said to a customer, hey over the last 15 years, this is how much money you alone have made this one company in profits, most people would become furious, because they would want that money, maybe not all of it but they would want their cut.	
25	I	What measures do you take to prevent privacy breaches?	
26	R13	Yeah, so I don't know our matrix off by heart, but we have a matrix and the matrix includes employee responsibilities	

		that exist, like a part of our employment contract so you can't work for Simby without agreeing to these terms of conditions. So that was that was the first one because if our people are not obligated to do the right thing then we have no way of making sure that it stays done. A broad sweeping promise that we would never know who our customers were so that we did not want to store any personally identifiable data. There is data that we do need to store to run the business, but the rule that we had in place was no personally identifiable data. So no PID and then we had a very clear list of what we considered PID so that there was no chance that PID values could be stored in the database and then a system of recovery, or I think it would I would call it recovery when a breach was identified. So, a way for us to handle a mistake that we discovered we made. And having no customers it was very easy for us to implement that process because we didn't have to contact anyone. But it was important to us. And this happens, so as we were building our products, we were breaching the privacy of our own employees who are using our app because it was built by us for the purposes of looking into the data that was being stored. So we found that interesting that we couldn't keep data privacy protections in place for our employees who were building the product because, it's sort of like quantum theory when you look at the electron the nature of it changes so for an employee to not be able to see the database of the values that were being stored locally on the device, they are unable to do their job. So, we had to have a data privacy rule set for our employees and a data Privacy Rule set for everyone else, and that was a challenge. I would say yeah step number one. Make sure that the data privacy principles are built into your employment contracts. Step number two makes the data privacy principles known to everyone, especially your customers, in our case our promise was we will never have any data that lets us know who you are. And step number three have a system of recourse should any of those promises be broken so that they can be addressed and resolved. Ad I think that's a simple as that like you don't you don't actually need more than those three things because obviously the first one and the second one are quite large the second one being the broad sweeping promise and I think the more complexity you build into it so that you can claw more privacy data from your customers the more difficult it gets because you are trying to keep 50 promises. Our promise was one which was don't take the data, then we've got no way of doing anything wrong with it because we don’t have it.	HE GDPR, PDS

27	I	Is your company transparent about the information you gather, and do you give customers control over their personal data?	
28	R13	Yes, so I'll just read you what we wrote. The first thing is we don't want customer data and we look forward to a time when companies never take any PID from customers and what rights do our customers have over the information, lots. They have the right to know what information we have, how we're using it and they have the right to request a copy of it and they have the right to ask us to delete it. And yeah, so that was our first big, you know, making sure that we had that standard GDPR fair in place, but I just want to draw your attention to something else that we wrote. We believe that technology should do no harm. We believe that technology should be built to care about people and enhance their lives and we believe that through forming these relationships with technology people can have longer and healthier lives. And then in terms of promises, we promised never to sell data. We promised that we would never have the means to find a customer or spy on them and we promised that we would always prioritize our customers' human health and happiness before profit and then our last promise was we promise to shut the company down before breaking any of these promises. So yeah, and we had a big fight with one of the potential investors because they offered us a lot of money to build this and launch this because it was the first of its kind but they wanted us to remove that promise and I said, this is a promise that once made cannot be broken so I would have had to shut the company down and then create a new company just to take their money. So, we were like no it's not going to happen. But yeah, I think saying something like that, as bold as that we promise to shut the company down before breaking the promise. I think that sort of it makes it very clear. And we saw that as value, so while it sounds like handcuffs, if done well and if this company launches and succeeds, that promise being made early puts us in a very optimal position for customer values. I used an example and I'll share it with you because it might be an interesting story. I said to investors, imagine you're a little kid in school and you've got your best friend and you're telling them about you knowing your day and then you tell your best friend that you accidentally wet the bed that night. You're like 7 or 8 and that best friend tells the whole class that you wet the bed and then you come to school the next day and everyone's laughing at you because you wet the bed. Now fast-forward 20 years, that person that told everyone that you wet the bed is 27 and	TV GDPR RUP

		they want a job as your personal assistant to help you with all of your privacy and all of your important data. They want to read your emails. They want to check your bank account. They want to make sure that you're not cheating on your wife or your husband. They want to make sure that your kids are being taken care of, they get access to everything. And they want the job and my simple question is would you give it to them? The answer is no, most people would say even if they're the best personal assistant in the world, I remember they sold me out when I was seven. And so, I say this, name a company of today that has not sold customer data and now fast forward 20 years when they're offering deep tech artificial intelligence systems that can predict your every movement, thoughts and behaviour. How will it be? How easy would it be for us to trust them? And can there be a company that has staked its ground early and say no, our primary object is to never break that promise, we are the kid that never told the secret and while we might not be as big or powerful as Facebook, but what we have that they don't have is the ability to say we never sold your data ever. I love Google. I worked there. They are a great company, but they can't say that thing. We never sold your data. They can never take it back. It's out of the bag, you know, and I look forward to a time when I see more companies, if possible because I don't know of any that say, that we will never and have never sold your data.	
29	R13	In your experience, by adding privacy requirements into your product or service, are you actually sacrificing the usability or the ability to serve your customer?	
30	R13	Yes, but it is a short-term sacrifice. I consider it like installing solar panels. There's an up-front cost and that cost seems prohibitive. But when you look at the big picture over the length of the life of the customer, it was a negligible cost, but up front it's scary because every other product or provider doesn't have pay that cost at all which gives them an edge against you, but I'm interested in winning the race not just being the first runner to leave the block. What I look forward to is a time when those upfront costs that we paid become a value add that investors or customers look for when they're looking for a company. Right now, they don't even know to look for it. We're paying this price to install our solar panels, but all they see is the light switch and can you turn the light on? You know, they don't understand yet that that power is coming from a source that is non corruptible. I look forward to a time	RUP

		when people are looking at the rooms of the houses and seeing the solar panels and saying oh, yeah, that one that one, you know, they didn't do it. So, I don't know if that's a good analogy. But yes, there's an upfront cost and it's big compared to our competitors, but short in the long run.	
31	I	Which design measures do you have in place to ensure full data lifecycle privacy protection?	
32	R13		
33	I	What do you think about making privacy as a default setting so that users do not have to initiate any privacy settings?	
34	R13	I think if you value privacy properly you don't even have a choice to give users the choice. We couldn't ask our customer upfront. Do you want the private version of our product or the non-private version of our product? Some companies might offer that and say look we're doing the right thing, but we can't even offer that choice to our customers because we have no mechanism to know who they are or store their answer. Does that make sense? Also, talking about companies' privacy statements. the more convoluted and the more long the disclaimer or the statement the less likely it is that anyone would ever understand it or read it. And I myself, caring about privacy will scroll quickly with my thumb and hit agree. And I care, right? I've built a company around it. It is reasonable to expect that every other person who cares less than me is also going to do the same behaviour. So, you know, I think we could count on our hands excluding lawyers, the number of times customers have read the entire Facebook privacy statement.	PDS PB RUP
35	I	Do you think there is a trade-off between completing core functionality and embedding privacy in the design?	
36	R13	Absolutely and it speaks to what I mentioned earlier about simple things like IP logging on cloud services. So, for us to be able to use deep learning with Google Cloud, we need to get the data in there, right? I can't invent deep learning offline and run it on my own server stack in a building in Berlin. So, to be competitive I do have to use the best practice, best in products that are available today. However, certain features and aspects of those products have baked in that the data is not anonymized. For us it was a trade-off because we had to put learning models online on the device that we would typically run offline which means on our servers, so that we could run them quicker and cheaper. What this means is that your battery	FF

		as an end user might be slightly impacted by running a model that needed to run locally on your device so that we never know who you are. There are trade-offs because we also want you as customers to not have your phone get blazed and go flat. But we also don't want to not offer competitive product features because we are choosing to do the right thing. So yeah, there's a constant trade off and that would be complicated for us in terms of should we or shouldn't we if we had made our promise less clear, but because our promise was we cannot capture or store any PID, it cannot hit our servers, it cannot traverse the wire our trade-off is not complex, it's annoying but it is not complex. We can't, we can't do it. You know what I mean? So the reason I mentioned that is, there are going to be companies that try to move in the right direction, they make lots of little promises and then they'll get to a point where there's this time to make a trade-off and an employee, not a decision maker, but an employee will choose the path of least resistance because that is what humans do and that path of least resistance will ultimately lead to a breach and I think unless you either elevate your promise to be all encompassing like we did or make sure that all decisions are made by people like a privacy protection Officer or something before any code goes live, there's no way to prevent these mistakes from happening otherwise.	HE
37	I	Do you think that embedding privacy by default will bring advantage to integrate your product or service with advanced technologies such as IoT?	
38	R13	Yes, I think for us, so a little bit about Simby. Simby is an artificially intelligent agent that lives inside your device. So, think of it like maybe Siri but with a brain and cares about you and is not called Siri, but called whatever you call it, and it's yours and it's just you and it and you live together. Like a Tamagotchi, but like you're the pet and the Tamagotchi is taking care of you, right?	PED
39	I	Like Jarvis?	
40	R13	Yes, I would say like Jarvis and we built that, but the issue becomes like when that thing needs to learn about your calendar or when that thing needs to learn about your day or the message you just received from your mum. How is that information being understood by a system that typically would then make a call to a server somewhere to say hey, I received this string, what does it mean? We had to always build in that thing that the learning happens offline or is pre-baked similar to how if you put your phone	PDS

		into airplane mode your language translation thing will stop working right. But there are some language translators now that have downloaded this like a language pack so that you can put your phone in airplane mode and it still understands you when you speak to it. We had to do that. But not just for understanding language but for everything, right? Yeah, so and then one of our biggest challenges was how do I move from this device to this device when none of the data is allowed to go into the cloud and one thing, we did which I'll share with you. We used ultrasonic. We send the data encrypted from this phone to this phone, my new phone using sound so that it doesn't hit any servers anywhere and if somebody's listening in the data packets, the sound is encrypted. It cannot be decrypted by somebody just listening. But essentially, it's like a high frequency like R2D2. And that is an example of just one thing that we had to begin again and reinvent some new technology to solve a very simple problem which you would have solved by going. Well, I just put in my email address on the new phone and it's all there and we were like, oh no, we're going to have to use sound we're going to have to encrypt it. We're going to have to build some technology to understand R2D2 speak and then decrypt it. There are days and days and months of work to do a very simple thing. So yeah. I just wanted to share that with you because when anyone asks you or says to you these things are not possible otherwise, that's not true right, anything's possible, but you really have to be prepared to do the work	
41	I	What is your perception about the use of personal data for advertising based on behavioural patterns?	
42	R13	I think it's fine. If you as the creator of the work, get a cut. And that you know up front what the cut is and that you have visibility on the transaction. So, for example, one of the things with our products that we were exploring is how to monetize our product. So instead of a high frequency low conversion advertising model, which is what happens with Facebook or Instagram or Google which is you see a lot of ads, they are personalized and there are many of them. And eventually you might see one or click on then convert right? That's a high frequency low conversion model. We wanted to invert that and create a low frequency high conversion model, which means you will see one ad that is tailored specifically to you because it's being presented to you as good advice from a trusted friend, your Jarvis. And it's not an ad, it's an invitation to do something and you as the recipient of that are being monetized, you're being remunerated by seeing it. If your Jarvis says hey Nike wants to know your shoe size,	ABP, PB TV

		Facebook would have sold it for nine dollars. How about we sell it for eight and I give you seven dollars 90 and the 10 cents goes to the company that made me. Now as a customer you like wait a minute Jarvis, you're telling me that you're going to sell my shoe size if I say yes to a company and I get seven dollars 90 and 10 cents on top of that goes to the company Simby. And your answer is yes or, no right? As a user experience designer with quite a few years of experience, I'm pretty sure most of us would say yes to that right? We're like actually yeah, I want the money and I think there's nothing wrong with selling my data to an advertiser provided that I know it's happening that I see the transaction and that I get a cut. And right now, you don't get any of those three things. You don't know what's happening. You don't see the transaction and you don't get a cut. You get to use the product so you can further be monetized and enslaved.	
43	I	How important is a proactive approach towards privacy in data analytics?	
44	R13	I would say it's the most important aspect, because like that thing I explained to you about transferring one Simby from a phone to another with ultrasonic. If we were not proactive, the simple solution would have been what was suggested to us by our tech advisors and by every known paradigm of how to create a user database which is to use email and then let them login. If we were not actively trying to break our own promise first so that we could figure out how not to break it. We would have broken it a million times already by accident and by path of least resistance. I think for us it was built into our organization built into our employment contracts built into the hiring and the way that we sourced our candidates. But for an organization, that is all already in flight and adopting these new strategies so that they can do the right thing, they would need to create a data privacy officer who had all sweeping power similar to a lawyer or an accountant or you know an auditor and that no database was off-limits and that this person and their backups were empowered to actively seek out the flaws, proactively seek out the vectors for attack, the potential for the breaking of these promises that have been made. Both promises that are legal because of compliance regulations like GDPR, but also promises that are made by companies trying to pretend that they care and then ultimately not because as a customer, what do you know. Do you know whether your email is hashed and encrypted on a database? You don't know, like you'll never know. So yeah, there's going to be companies that make the promise but then not deliver and you won't know until	PP, DA

		it's too late. So, a proactive approach is super important, and I think it can be implemented in companies that are not new as well, but they have to create a role of a data protection officer and give them the power to hire and fire and all of the scary stuff.	HE
45	I	Do you think there is anything relevant to the subject that we haven't discussed during this interview?	
46	R13	No, I'm excited to see the results.	
47	I	Thank you for your time and stay safe! We really appreciate your contribution to our research.	

References

Abbasi, A., Sarker, S. & Chiang, R. H. L. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda, *Journal of the Association for Information Systems,* vol. 17, no. 2**,** pp 3.

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information, *Science,* vol. 347, no. 6221**,** pp 509-514.

Alessandro, A., Leslie, K. J. & George, L. (2013).What Is Privacy Worth?, *The Journal of Legal Studies,* vol. 42, no. 2**,** pp 249.

Alvesson, M. & Karreman, D. (2001). Qualitative research and theory development: Mystery as method, London: Sage.

Anscombe, T., Bartko, J., Bešina, I., Čermák, M., Fránik, M., Svorenčík, Š. & Szurek, K. (2017). IoT and Privacy by Design in the Smart Home.

Auerbach, C. & Silverstein, L. B. (2003). Qualitative Data: An Introduction to Coding and Analysis: NYU press.

Bednar, K., Spiekermann, S. & Langheinrich, M. (2019). Engineering Privacy by Design: Are Engineers Ready to Live up to the Challenge?, *The Information Society,* vol. 35, no. 3**,** pp 122-142.

Bélanger, F. & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, *MIS Quarterly,* vol. 35, no. 4**,** pp 1017-A36.

Benartzi, S. & Bhargava, S. (2020). How Digital Design Drives User Behavior, *Harvard Business Review Digital Articles,* p. 2. Available online : https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=edb&AN=141655848&site=eds-live&scope=site [Accessed: 25 March 2020].

Bhargava, S., Conell-Price, L., Mason, R. & Benartzi, S. (2018). Save (D) by Design, Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237820 [Accessed 25 April 2020].

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices.

Blix, F., Elshekeil, S. & Laoyookhong, S. (2018). Designing GDPR Data Protection Principles in Systems Development, *Journal of Internet Technology and Secured Transactions,* vol. 6, no. 548-555.

Brinkmann, S. & Kvale, S. (2015). Interviews: Learning the Craft of Qualitative Research Interviewing: Sage Thousand Oaks, CA.

Buckbee, M. 2020. Data Security: Definition, Explanation and Guide, Available online: https://www.varonis.com/blog/data-security/ [Accessed 12 March 2020].

Calder, A. & Watkins, S. (2008). It Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002: Kogan Page Ltd.

Camhi, R. & Lyon, S. (2018).What Is the California Consumer Privacy Act?, *Risk Management,* vol. 65, no. 9**,** pp 12-13.

Campisi, P. (2013). Security and Privacy in Biometrics: Springer.

Cavoukian, A. (2006). Creation of a Global Privacy Standard, *Published November,* vol. 8, Available online: https://danskprivacynet.files.wordpress.com/2009/11/up-gps.pdf [Accessed 25 February 2020].

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles, *Information and privacy commissioner of Ontario, Canada,* vol. 5, Available online: https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf [Accessed 2 March 2020].

Cavoukian, A. (2011). Privacy by Design in Law, Policy and Practice, *A white paper for regulators, decision-makers and policy-makers.*

Cavoukian, A. (2012). Privacy by Design [Leading Edge], *IEEE Technology and Society Magazine,* vol. 31, no. 4**,** pp 18-19.

Cavoukian, A. (2018). The Game Changer: Privacy by Design. Available online: https://www.echoworx.com/wp-content/uploads/2018/05/Echoworx_Costs_Reactive_Security-2.pdf?pdf=Costs_Reactive_Security-WhitePaper [Accessed 3 April 2020].

Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time, *IEEE Consumer Electronics Magazine,* vol. 9, no. 2**,** pp 78-82.

Cavoukian, A. & Chibba, M. (2018). Start with Privacy by Design in All Big Data Applications. *Guide to Big Data Applications.* Springer pp 29-48.

Cavoukian, A. & Dixon, M. (2013). Privacy and Security by Design: An Enterprise Architecture Approach: Information and Privacy Commissioner of Ontario, Canada.

Cavoukian, A. & Popa, C. (2016). Embedding Privacy into What's Next: Privacy by Design for the Internet of Things, *Ryerson University Privacy & Big Data Institute,* vol. no. 1-10.

Cavoukian, A., Taylor, S. & Abrams, M. E. (2010). Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, *Identity in the Information Society,* vol. 3, no. 2**,** pp 405-413.

CCPA (2020). California Consumer Privacy Act of 2018, Available online, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100&fbclid=IwAR1HbFUGreAyZmKXZpctWiJacEeEqngZCi5uSOwh8XLAFiVR1wYN1G_QfQA [Accessed 5 March 2020].

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E. & Wortmann, F. (2019). Blockchain for the Iot: Privacy-Preserving Protection of Sensor Data, *Journal of the Association for Information Systems,* vol. 20, no. 9**,** pp 1271-1307.

Corbin, J. & Strauss, A. (2008). Basics of Qualitative Research (3rd Ed.): Techniques and Procedures for Developing Grounded Theory. Thousand Oaks, California: Sage.

Culnan, M. J. (2019). Policy to Avoid a Privacy Disaster, *Journal of the Association for Information Systems,* vol. 20, no. 6**.**

Cusick, J. (2018). The General Data Protection Regulation (GDPR): What Organizations Need to Know, *CT corporation resource center,* vol. no. 1-6.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R. & Schiffner, S. (2015).Privacy and Data Protection by Design-from Policy to Engineering, *arXiv preprint arXiv:1501.03726.*

Davenport, T. H., Harris, J. G. & Morison, R. (2010). Analytics at Work: Smarter Decisions, Better Results: Harvard Business Press.

Davison, R. M., Kock, N., Loch, K. D. & Clarke, R. (2001). Research Ethics in Information Systems: Would a Code of Practice Help?, Communications of the Association for Information Systems, vol. 7.

de la Torre, L. (2018). A Guide to the California Consumer Privacy Act of 2018, Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571&fbclid=IwAR3pFFX31mJ_tzFdFoG8pLJFIdHY73mRkBJp1Qvrssvy_lRa4TYFBDd3RzA [Accessed 3 March 2020].

Eagan, M. (2019). Businesses Struggling with GDPR after One Year, Says Thomson Reuters Survey [Online], Available online: https://www.thomsonreuters.com/en/press-releases/2019/may/businesses-struggling-with-gdpr-after-one-year-says-thomson-reuters-survey.html [Accessed 4 March 2020].

Fuller, M. (2019). Big Data and the Facebook Scandal: Issues and Responses, *Theology,* vol. 122, no. 1**,** pp 14-21.

Galitz, W. O. (2007). The Essential Guide to User Interface Design: An Introduction to Gui Design Principles and Techniques: John Wiley & Sons.

GDPR. (2020). General Data Protection Regulation, Available online: https://gdpr.eu/tag/gdpr/ [Accessed 2 March 2020].

Gerlach, J. P., Buxmann, P. & Dinev, T. (2019)."They're All the Same!" Stereotypical Thinking and Systematic Errors in Users' Privacy-Related Judgments About Online Services, *Journal of the Association for Information Systems,* vol. 20, no. 6**,** pp 787-823.

Given, L. M. (2008). The SAGE Encyclopedia of qualitative research methods. Thousand Oaks, CA: SAGE Publications.

Gjermundrød, H., Dionysiou, I. & Costa, K. (2016). Privacytracker: A Privacy-by-Design Gdpr-Compliant Framework with Verifiable Data Traceability Controls. International Conference on Web Engineering, 2016. Springer, 3-15.

Gürses, S., Troncoso, C. & Diaz, C. (2011). Engineering Privacy by Design, *Computers, Privacy & Data Protection,* vol. 14, no. 3**,** pp 25.

Hafeez-Baig, A., Gururajan, R. & Chakraborty, S. (2016). Assuring Reliability in Qualitative Studies: A Health Informatics Persective. Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Pacific Asia Conference on Information Systems.

Heng, X., Dinev, T., Smith, J. & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, *Journal of the Association for Information Systems,* vol. 12, no. 12**,** pp 798-824.

Hsieh, H.-F. & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis, *Qualitative health research,* vol. 15, no. 9**,** pp 1277-1288.

Hustinx, P. (2010). Privacy by Design: Delivering the Promises, *Identity in the Information Society,* vol. 3, no. 2**,** pp 253-255.

Jae Kyu, L., Daegon, C. & Gyoo Gun, L. (2018). Design and Validation of the Bright Internet, *Journal of the Association for Information Systems,* vol. 19, no. 2**,** pp 63-85.

Jandl, C., Nurgazina, J., Schöffer, L., Reichl, C., Wagner, M. & Moser, T. (2019). Sensitrack-a Privacy by Design Concept for Industrial Iot Applications. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, 1782-1789.

Kagan, S. & Bekkerman, R. (2018). Predicting Purchase Behavior of Website Audiences, *International Journal of Electronic Commerce,* vol. 22, no. 4**,** pp 510-539.

Karwatzki, S., Dytynko, O., Trenz, M. & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization, *Journal of Management Information Systems,* vol. 34, no. 2**,** pp 369-400.

Kifer, D. & Machanavajjhala, A. (2011). No Free Lunch in Data Privacy, pp. 193-204.

Koops, B.-J. & Leenes, R. (2014).Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design'provision in Data-Protection Law, *International Review of Law, Computers & Technology,* vol. 28, no. 2**,** pp 159-171.

Kurtz, C., Semmann, M. & Böhmann, T. (2018). Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors, Available online: https://pdfs.semanticscholar.org/c701/a9d03f44c612430677239b44d0e243ae5fd2.pdf [Accessed 4 April 2020].

Kvale, S. (2006). Dominance through Interviews and Dialogues, *Qualitative inquiry,* vol. 12, no. 3**,** pp 480-500.

Lee, J. K., Cho, D. & Lim, G. G. (2018). Design and Validation of the Bright Internet, *Journal of the Association for Information Systems,* vol. 19, no. 2**,** pp. 63-85.

Li, T. & Unger, T. (2012). Willing to Pay for Quality Personalization? Trade-Off between Quality and Privacy, *European Journal of Information Systems,* vol. 21, no. 6**,** pp 621-642.

Lund University. (2019). Avoiding plagiarism, Available online: https://www.lunduniversity.lu.se/current-students/academic-matters-support/academic-support-centre/avoiding-plagiarism [Accessed 3 March 2020].

Magnusson, E. & Marecek, J. (2015). Doing Interview-Based Qualitative Research: A Learner's Guide: Cambridge University Press.

Mandal, A., Mitchell, J., Montgomery, H. & Roy, A. (2017). Privacy for Targeted Advertising. 2017 IEEE Conference on Communications and Network Security (CNS), IEEE, 438-443.

Myers, M. D. & Newman, M. (2007). The Qualitative Interview in Is Research: Examining the Craft, *Information and organization,* vol. 17, no. 1**,** pp 2-26.

Neuendorf, K. (2017). The content analysis guidebook, Thousand Oaks, CA: SAGE Publications.

Oates, B. J. (2006). Researching Information Systems and Computing, Sage Publications Ltd.

Oetzel, M. C. & Spiekermann, S. (2012). Privacy-by-Design through Systematic Privacy Impact Assessment-a Design Science Approach.

Patton, M. Q. (2015). Qualitative Research and Methods: Integrating Theory and Practice, Thousand Oaks, CA: SAGE Publications.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go?, *MIS Quarterly,* vol. 35, no. 4**,** pp 977-988.

Pender-Bey, G. (2016). The Parkerian Hexad, *Information Security Program at Lewis University.*

Portman, R. & Carper, T. (2017). How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach, Available online: https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf [Accessed 4 April 2020]

Potter, B. (2009). Microsoft Sdl Threat Modelling Tool, *Network Security,* vol. 2009, no. 1**,** pp 15-18.

Rao, R. V. & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing, *Procedia Computer Science,* vol. 48, no. 204-209.

Recker, J. (2013). Scientific Research in Information Systems. [Elektronisk Resurs] a Beginner's Guide: Springer Berlin Heidelberg.

Redman, T. C. & Waitman, R. M. (2020). Do You Care About Privacy as Much as Your Customers Do?, *Harvard Business Review Digital Articles,* vol. no. 2.

Rubens, P. (2019). How to Comply with CCPA, Available online: https://www.esecurityplanet.com/compliance/how-to-comply-with-ccpa.html?fbclid=IwAR2HrDKbY14cezX3IKvWbKwP2jv_Ir5KfcpWu21gl1Bqujbk5vSbPt7mNFc [Accessed 24 March 2020].

Saldaña, J. (2015). The Coding Manual for Qualitative Researchers: Sage.

Samonas, S. & Coss, D. (2014). The Cia Strikes Back: Redefining Confidentiality, Integrity and Availability in Security, *Journal of Information System Security,* vol. 10, no. 3**,** pp 21-45.

Saraiva, S. (2017). Data Protection through Privacy by Design, Available online: https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments.pdf [Accessed 13 March 2020].

Schaar, P. (2010). Privacy by Design, *Identity in the Information Society,* vol. 3, no. 2**,** pp 267-274.

Schrage, M. (2016). Why User Experience Always Has to Come First, *Harvard Business Review Digital Articles*, pp. 2–4. Available online: https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&db=bth&AN=118678988&site=eds-live&scope=site [Accessed 24 April 2020].

Schultze, U. & Avital, M. (2011). Designing Interviews to Generate Rich Data for Information Systems Research, *Information and organization,* vol. 21, no. 1**,** pp 1-16.

Seale, C. (1999). Quality in Qualitative Research, *Qualitative inquiry,* vol. 5, no. 4**,** pp 465-478.

Shuaifu, L. & Armstrong, D. J. (2019). Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites, *Journal of the Association for Information Systems,* vol. 20, no. 4**,** pp 434-475.

Silver, C., & Lewins, A. (2014). Using software in qualitative research: A step-by-step guide, London: Sage.

Smith, M. & Mulrain, G. (2017). Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, J. Nat'l Sec. L. & Pol'y,* vol. 9, no. 549.

Spiekermann, S. (2012). The Challenges of Privacy by Design, *Communications of the ACM,* vol. 55, no. 7**,** pp 38-40.

Stenbacka, C. (2001). Qualitative Research Requires Quality Concepts of Its Own, *Management decision,* vol. 39, no. 7, pp. 551-556.

Sullivan, P. (2012). Qualitative Data Analysis Using a Dialogical Approach. London: Sage.

Sun, Y., Song, H., Jara, A. J. & Bie, R. (2016). Internet of Things and Big Data Analytics for Smart and Connected Communities, *IEEE access*, vol. 4, no. 766-773.

Sutanto, J., Palme, E., Chuan-Hoo, T. & Chee Wei, P. (2013a). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users, *MIS Quarterly*, vol. 37, no. 4**,** pp 1141-A5.

Sutanto, J., Palme, E., Tan, C.-H. & Phang, C. W. (2013b). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users, *MIS quarterly*, vol. no. 1141-1164.

van Rest, J., Boonstra, D., Everts, M., van Rijn, M. & van Paassen, R. (2012). Designing Privacy-by-Design. Annual Privacy Forum, 2012. Springer, 55-72.

Verizon. (2019). Data Breach Investigations Report, Available online: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf [Accessed 2 March 2020].

Wang, F., Ko, R. & Mickens, J. (2019). Riverbed: Enforcing User-Defined Privacy Constraints in Distributed Web Services. 16th Symposium on Networked Systems Design and Implementation (19), pp. 615-630.

Wang, P. & Park, S.A. (2017). Communication in Cybersecurity: A Public Communication Model for Business Data Breach Incident Handling, *Issues in Information Systems*, vol. 18, no. 2.

Wolcott, H. F. (1994). Transforming Qualitative Data: Description, Analysis, and Interpretation: Sage.

Wunderlich, P., Veit, D. J. & Sarker, S. (2019). Adoption of Sustainable Technologies: A Mixed-Methods Study of German Households, *MIS Quarterly*, vol. 43, no. 2**,** pp 673-691.

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, *Journal of the Association for Information Systems*, vol. 12, no. 12**.**

Yang, H., Zheng, W., Zhou, T., Jin, X. & Wang, A. (2019). A Privacy-Protecting and Resource-Saving Scheme for Data Sharing in Smart Home, *Journal of Internet Technology*, vol. 20, no. 2**,** pp 607-615.