INVESTIGATING THE MOTIVATIONAL FACTORS INFLUENCING MANAGERIAL DECISIONS TO ADOPT PRIVACY-ENHANCING TECHNOLOGIES

Completed Research Paper

Alexandra Klymenko, Technical University of Munich, TUM School of Computation, Information and Technology, Department of Computer Science, Garching, Germany, alexandra.klymenko@tum.de

Stephen Meisenbacher, Technical University of Munich, TUM School of Computation, Information and Technology, Department of Computer Science, Garching, Germany, stephen.meisenbacher@tum.de

Iva Lilova, Technical University of Munich, TUM School of Computation, Information and Technology, Department of Computer Science, Garching, Germany, iva.lilova@tum.de

Florian Matthes, Technical University of Munich, TUM School of Computation, Information and Technology, Department of Computer Science, Garching, Germany, matthes@tum.de

Abstract

Recent years have shown an increase in fervor in the discussion surrounding data privacy, in an age where data processing has become ubiquitous. Concurrently, the regulatory response to such practices has been realized in the form of wide-reaching data protection regulations, most notably the General Data Protection Regulation in the EU. In the adoption of Privacy-Enhancing Technologies (PETs) as data protection measures, the role of managers represents a crucial point in the decision-making process. As such, we place the point of investigation at the managerial level to explore the motivating factors that influence decisions to adopt PETs. Following a literature review that reveals the applicability of Corporate Social Responsibility as a basis for privacy protection, semi-structured interviews with managers responsible for privacy-related decisions are conducted, uncovering 47 motivational factors falling under three categories of incentives. These factors are taxonomized, validated, and analyzed in the remainder of our work.

Keywords: Data Privacy, Privacy-Enhancing Technologies, Corporate Social Responsibility

1 Introduction

The landscape of data privacy has been rapidly changing in the last decade, spearheaded by modern data protection regulations that threaten strict penalties for non-compliance. In particular, regulations such as the General Data Protection Regulation (GDPR) and its many successors, place a clear emphasis on the implementation of technical and organizational measures for data protection.

An immediate challenge becomes the translation of a legal mandate to protect data in processing activities to technical measures that realize such a requirement. As such, a clear understanding of *technical measures* is an active field of research, calling for a more unified understanding. As introduced by Klymenko et al. (2022), the implementation of Privacy-Enhancing Technologies (PETs) presents a promising solution, but the complexities lie in the lack of understanding of the relation between such novel technologies and the requirements set forth by regulations such as the GDPR.

Beyond the lack of clear relation between PETs and regulations, the technical details of PETs also contribute to potential obstacles in their adoption. PETs are generally complex in nature, requiring domain expertise to understand and implement in practice. Therefore, high complexity, lack of domain expertise, and mistakes in implementation have all been listed as persistent challenges when it comes to the adoption of PETs in practice (Information Commissioner's Office, 2022; Klymenko et al., 2023)

Looking behind the scenes, the challenges associated with adopting PETs in practice emerge before their actual implementation, where factors such as organizational culture and the influence of managers can directly impact the implementation of PETs as technical measures for privacy compliance (Klymenko et al., 2023). In this way, the implementation of PETs is far more complex than the technologies themselves, requiring not only domain expertise but also a clear organizational incentive to do so.

In considering the organizational incentives to protect privacy and specifically to implement PETs, we turn to the decision-makers within organizations. We seek to understand what may drive individuals in managerial roles, particularly those dealing with privacy-related decisions, to prioritize advanced privacy protection, as they shape the goals and objectives of the organization.

In exploring the motivational factors influencing managerial decisions to adopt PETs, one may first turn to the incentive of compliance, or rather, the demonstration of compliance to avoid fines. Beyond this financial aspect, however, the question remains as to what might motivate executives to surpass the bare minimum and invest in state-of-the-art technologies such as PETs. The underlying challenge presented in this question is highlighted by previous work (Klymenko et al., 2022), but no work has been performed to investigate its answer. To fill this gap, we employ the use of Corporate Social Responsibility, which promotes socially conscious action beyond what is strictly required.

As such, we aim to investigate the *motivational factors* (hereinafter also *incentives*) influencing managerial decisions to adopt PETs as a measure for data privacy protection. In particular, we focus on senior-level executives and decision-makers responsible for privacy-related decisions in their organizations. Guided by insights found in related literature, we interviewed six people serving in executive roles with the goal of validating factors found in the literature, as well as introducing new ones. All identified incentives are structured into a taxonomy and then evaluated in a survey study.

2 Background and Related Work

2.1 Privacy-enhancing technologies

Privacy-Enhancing Technologies (PETs) represent a technical approach to the preservation of privacy and are designed specifically for the safeguarding of personal information. More formally, these technologies "protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system" (Van Blarkom et al., 2003). Although PETs present concrete solutions for personal data protection, they remain predominantly in the academic sphere and are not widely adopted in practice (Hansen et al., 2015). Among the main reasons for this are the complexity of these technologies, little awareness and knowledge of them, as well as the lack of incentive to put resources into implementing state-of-the-art PETs, when the bare minimum technical measures can suffice to be compliant "on paper" (Klymenko et al., 2023). Acquisti et al. (2020) suggest that further research, integrating psychology, economics, computer science, and the law, is necessary to overcome such challenges.

While academics acknowledge that the decision to use PETs can be influenced by both subjective and societal factors, research so far has rarely taken such factors into account, and to the best of the authors' knowledge, no studies specifically investigate the managerial perspective in adopting PETs.

2.2 The role of management

There are numerous mentions in the past and recent literature of the role of managers as stakeholders for privacy protection. Greenaway and Chan (2005) emphasize the growing importance of data privacy

to managers and policymakers within the field of information management, declaring it a significant concern. In a conceptual design support guide developed in 2018 to assist managers in addressing the challenges associated with digital transformation, challenges related to privacy and security were among the factors identified as obstacles managers face in achieving successful digital transformation in business (Heavin and Power, 2018). Culnan and Williams (2009) emphasize managerial responsibility for organizational privacy behavior, drawing upon information ethics and "the moral responsibility of executives to do no harm." They claim that much of privacy research has not addressed broader organizational, managerial, and societal concerns, such as how businesses handle personally identifiable information, the specific actions managers must take, and the moral obligations they owe to various stakeholders involved in their organizations. In line with this, multiple recent works on responsible organizational practices and the role of privacy such as by Lobschat et al. (2021) and Martin et al. (2020) have placed the focus on the managerial perspective.

Previous research focused on the implementation of technical measures for data privacy compliance also showed that management plays an essential role in the privacy compliance structure of organizations (Klymenko et al., 2022), and that lack of awareness of the importance of data privacy on the management level can lead to challenges in implementing privacy protection measures (Klymenko et al., 2023). Furthermore, it was shown that "the decision to interpret PETs as appropriate technical measures is one left to upper management" and that it is practitioners in managerial roles that stand behind the decisions on whether or not to implement PETs (Klymenko et al., 2022). In these works, however, no detail was provided regarding managerial incentives for privacy, thus motivating our decision to focus on how people in these roles are incentivized to invest in the adoption of PETs.

2.3 Corporate social responsibility and privacy

Corporate Social Responsibility (CSR) can be defined as a "firm's consideration of, and response to, issues beyond the narrow economic, technical, and legal requirements (...) in a manner that will accomplish social benefits along with the traditional economic gains which the firm seeks" (Davis, 1973). Davis argues that "social responsibility begins where the law ends", and a company "is not being socially responsible if it merely complies with the minimum requirements of the law", promoting the integration of social values into business decision-making processes.

Carroll (1979) classifies corporate social responsibilities into economic, legal, ethical, and discretionary categories. He acknowledges profit generation and legal compliance as some of the fundamental responsibilities of companies; however, he argues that society expects more. Mintzberg adds that CSR becomes relevant when organizations need to comply not only with the literal interpretation of existing legislation but also with its underlying principles (Mintzberg, 1983; Pollach, 2011). When it comes to privacy, the aspect of data protection calls for more attention than what is strictly needed to achieve compliance. Furthermore, it is important to distinguish between demonstrating compliance through technical measures and truly ensuring the protection of privacy (Klymenko et al., 2023). Therefore, Pollach (2011) suggests that privacy can be considered an ethical responsibility and a CSR initiative when the law is insufficient to govern corporate decision-making regarding data management. Similarly, Steele (2022) argues that "data protection needs to be considered as a primary CSR objective".

Allen and Peloza (2015) also explored the connection between privacy and CSR, suggesting that privacy concerns impact companies' relationships with stakeholders. To assess privacy-related activities as part of a CSR strategy, they develop a framework that distinguishes between company-focused and customer-focused privacy activities, as well as CSR activities related to business practices or goods/services. The authors argue that privacy protection when viewed from a CSR perspective can enhance a company's reputation and stakeholder relationships.

In this work, we suggest that the adoption of PETs can be viewed as a CSR initiative. Based on the work of Aguilera et al. (2007), who argued that there exist three main motives for engaging in CSR: moral, relational, and instrumental, we use these motives as foundational characteristics for the classification of factors influencing managerial decisions to adopt PETs.

3 Methodology

The conducted research follows a mixed methods approach, in which researchers employ both quantitative and qualitative research methods to enable a comprehensive understanding of a research topic (Creswell and Creswell, 2017). An effective application of the mixed method approach conducts the qualitative and quantitative investigations concurrently and independently (Greene et al., 1989). As such, we begin with a qualitative study: a systematic literature review followed by semi-structured interviews. After a thorough analysis of the qualitative findings, we develop a taxonomy and conduct a quantitative study (surveys) on a larger sample of the target audience not only to validate the relevance of the results, but also to explore their general acceptance among privacy managers.

3.1 Research questions

In order to address the goal of this work, we define the following research questions:

RQ1. What are the motivational factors for privacy protection in organizations?
RQ2. From a managerial perspective, what are the incentives for the adoption of PETs?

3.2 Systematic literature review

Our research begins with a systematic literature review (SLR), for which the methodology of Kitchenham et al. (2015) was applied. The SLR was conducted via Google Scholar by employing two separate search strings (*S1: "Organizational Privacy" OR "Organizational Motives"; S2: "Privacy" AND "Corporate Social Responsibility")* filtered for works from 1990-2022 with either of the queries appearing in the title. The publications were deduplicated and screened according to the three primary inclusion/exclusion criteria: (1) openly or institutionally accessible, (2) written in English, and (3) focused on privacy protection incentives for organizations or the link between privacy and CSR.

From this, the initial set of publications with the defined focus was selected, namely (Chan and Greenaway, 2005; Culnan and Williams, 2009; Parks et al., 2011; Pollach, 2011; Greenaway and Chan, 2013; Allen and Peloza, 2015; Pelteret and Ophoff, 2017; Senarath and Arachchilage, 2017; Bestman et al., 2022; Halder et al., 2022; Steele, 2022). In addition to the above, a forward and backward search was performed, which resulted in the identification of further relevant papers, specifically (Aguilera et al., 2007; Weitzner et al., 2008; Borking, 2009; Cavoukian et al., 2010; London Economics, 2010; Fairchild and Ribbers, 2011; Tsai et al., 2011; Jaatun et al., 2012; Pearson, 2012; Acquisti et al., 2020; Lobschat et al., 2021; Acquisti et al., 2022).

3.3 Interviews

Following the SLR, we conducted semi-structured interviews (SSIs), with the goal of gaining practical insights about managerial incentives for privacy protection and adopting PETs. In line with the goals of our study, we contacted potential interviewees only if they were currently serving in a management position responsible for privacy-related decisions in an organization. The relevant anonymized information about the six interviewees is presented in Table 1. Note that for Organization (size), the categories from the EU recommendation 2003/361 are used. *Exp.* denotes years of experience in the field of privacy. The interviews were conducted via Zoom with an average duration of 65 minutes.

ID	Role	Exp.	Organization	Industry Domain
IP1	Director of Engineering, Security and Privacy	16	Large-sized	International telehealth provider
IP2	Technical Co-founder	4	Micro-sized	German AI startup
IP3	Cybersecurity and Privacy Executive	15	Large-sized	American service company
IP4	Director of Privacy and Data Protection	7	Large-sized	American cryptocurrency company
IP5	Global Head of Privacy, Data Protection and Data Compliance	13	Large-sized	Multinational supply chain and logistics company
IP6	Director of Security and Privacy	10+	Large-sized	Online marketplace company

Table 1. Interview study participants.

Interviewees were all identified and initially contacted via Linkedin. All interviewees were presented with a prepared guide in a formal email invitation before the interview. The guide, developed based on Kallio et al. (2016), provides a structure for the interview but does not need to be strictly followed. This enables discussion during the interview (Whiting, 2008), changing the question order (Dearnley, 2005), and uncomplicated movement between questions (Åstedt-Kurki and Heikkinen, 1994).

The questions in the guide were divided into four main sections. First, after obtaining informed consent to conduct and record the interview, background information on the interviewee was collected. Next, participants were asked questions about the role of privacy in their organizations, as well as the incentives for privacy protection. The third part of the interview revolved around Privacy-Enhancing Technologies. After ensuring a mutual understanding of the term PETs, the interviewees' awareness and experience with these technologies, as well as the benefits and incentives for their adoption were discussed. Finally, the interviews were wrapped up with several forward-looking questions on the future of privacy protection, the practical adoption of PETs, and the role of privacy managers.

To analyze the interview data, we employed thematic analysis (Braun and Clarke, 2006) to identify recurring themes appearing in the transcript data. The knowledge previously gained in the SLR became crucial to thematic analysis, as it was necessary to extract themes from the interviews to align them with SLR findings, as well as to discover novel incentives. The six-step process as proposed by Braun and Clarke was performed in parallel to the conduction of interviews. The initial step involved interactively reading the interview transcriptions, highlighting potentially important statements, and writing down initial impressions, an interpretative act by which the first meanings were created (Lapadat and Lindsay, 1999). Next, we divided the data set into individual chunks of data (data extracts). For each extract, we identified codes, which refer to "the most basic segment[s]... of the raw data or information that can be assessed in a meaningful way regarding the phenomenon" (Braun and Clarke, 2006). Step 3 involved the identification of themes in light of the *a priori* themes extracted from the SLR, resulting in a collection of intermediate themes. Following this (steps 4 and 5), we applied the intermediate (candidate) themes to the data set in order to determine if they tell a convincing story or if adjustments are necessary, and then verified the quality of the themes to ensure that they accurately depict the essence of the transcribed data. In the identification of themes as part of the analysis, the interview study was stopped once the analysis of an interview yielded no new themes.

3.4 The taxonomy

In order to classify all factors that influence managerial decisions to adopt PETs in their organizations, identified both from the SLR and SSIs, we created a taxonomy, following the method proposed by Nickerson et al. (2013). The particular choice for representation in a taxonomy structure was motivated by its ability to illustrate the hierarchical nature of our findings.

The first step in creating a taxonomy is to identify its *meta-characteristic (MC)*, which is the primary characteristic that serves as the foundation for selecting the remaining characteristics. The MC of our taxonomy was determined during the SLR, after identifying the link between privacy and CSR. Based on the results of our qualitative study findings, namely on the work of Aguilera et al. (2007), we adopt the moral, relational, and instrumental reasons for engaging in CSR as the foundation of our taxonomy.

According to Nickerson et al. (2013), the purpose of the taxonomy should be aligned with its intended application, and its design process can involve the participation of its target users. In line with this approach, we engaged our target audience, i.e., managers and decision-makers responsible for privacy-related decisions in their organizations, in the development of the taxonomy through SSIs and its validation through a survey. Specifically, the taxonomy creation process consisted of three iterations:

1. *Empirical-to-conceptual*: building upon the selected MC, the dimensions (subcategories) of the taxonomy were outlined using the motivational factors identified during the SLR. Subsequently, these factors were classified according to these subcategories.
2. *Empirical-to-conceptual*: analyzing the *interview findings* and determining possible new subcategories (themes) to characterize the identified motivational factors.

3. *Conceptual-to-empirical*: the survey findings validated the applicability of the motivational factors for privacy protection as incentives for the adoption of PETs. As no new incentives outside of the existing categories were identified, the defined categories and subcategories were validated, and the method's ending conditions were met.

3.5 Survey study

The final part of the designed research study represented the quantitative analysis of our findings in the form of surveys. Consistent with the sequential mixed methods approach, surveys were carried out only after the qualitative data analysis was finished *and* the resulting taxonomy was created. Thus, the overarching goal of conducting a survey study was to produce quantifiable results that give insight into the identified factors from the SLR and SSI studies as incentives for the adoption of PETs.

The target group of the survey study was set to be the same as in the SSI study, and all interviewees were invited to participate. However, not all interview participants contributed to the survey study.

The survey questions were divided into two sections: (1) relevant background (summarized in Table 2), and (2) agreement with each individual motivational factor from the three categories of our taxonomy. To craft the survey, each incentive was mapped to one or more statements, formulated as: *As a manager / decision-maker, I am motivated to adopt PETs as technical measures for privacy protection because…* In the case of five incentives, more than one statement was assigned, due to the multi-faceted nature of these incentives. The results for incentives with more than one statement were averaged for the final validation score. To ensure a common understanding of the term PETs, survey participants were provided with a definition of the term, presented in Section 2.1.

We employed a five-point symmetric Likert scale *{strongly agree, agree, neutral, disagree, strongly disagree}* for all survey questions in the second section of the survey. This format allows for quantitative analysis, in which composite scores for each subcategory can be produced.

ID	Role	Exp.	Organization	Industry Domain
SP1	Business Information Security Officer	10+	Large-sized	Retail and Wholesale Trade
SP2	Director of Privacy	10+	Large-sized	Transportation and Warehousing
SP3	Founder & Management Consultant	5-10	Micro-sized	Management Consulting
SP4	Data Protection Officer	10+	Large-sized	Electric Power
SP5	Senior Manager Data Privacy	10+	Large-sized	MedTech
SP6	Associate Director Global Compliance & Privacy	10+	Medium-sized	Biotech/Pharma
SP7	Senior Specialist Data Protection	0-3	Large-sized	Semiconductors
SP8	Head of Legal	3-5	Medium-sized	Software as a Service
SP9	IT Privacy Manager	0-3	Large-sized	Pharma/Life Sciences
SP10	Senior VP, Global Head of Security & Privacy	10+	Large-sized	HR, Payroll, Employer of Record
SP11	Director of Privacy and Data Protection	5-10	Large-sized	Finance and Insurance
SP12	Data Protection Officer	5-10	Medium-sized	Finance and Insurance
SP13	Chief Technology Officer	3-5	Micro-sized	Tech
SP14	Chief Data Analytics & Privacy Officer	10+	Large-sized	Finance and Insurance
SP15	Privacy Officer and Information Security & Compliance Principal	10+	Large-sized	Healthcare and Social Assistance

Table 2. Survey study participants.

4 Motivational Factors for Privacy Protection

Before analyzing the factors for adopting PETs, we first begin with a systematic investigation into the motivational factors for privacy protection in general. Viewing the decision to implement data protection measures as a prerequisite for adopting PETs, the goal is first to extract and structure the motivational factors for privacy protection, derived from the SLR and SSIs. While the aim was to investigate privacy protection, some identified factors are also explicitly relevant to the adoption of PETs. The results presented in the following represent a fusion of the identified findings from both the SLR and SSIs.

The link between privacy and CSR, identified during SLR, provides a foundation for the three overarching categories of motivational factors for privacy protection: moral, relational, and instrumental. In the following, these categories are introduced, along with their respective subcategories and motivational factors. All factors are represented visually in our taxonomy, found in Figure 1.

4.1 Moral factors

Moral factors, a concept taken from CSR, serve as important incentives for privacy protection in organizations. They are centered around the notion of companies having a duty to protect the privacy rights of individuals and to act in an ethical and responsible manner when handling personal information.

4.1.1 Subjective values (I1.1)

Some managers and companies recognize the importance of treating privacy as a fundamental human right and are committed to acting morally right. Decision-makers can be aware of the fact that not all customers or end users are familiar with the possible risks associated with privacy, suggesting a concern for justice and the wish to "do the right thing". Managers who are personally interested in privacy might be more likely to emphasize the importance of privacy protection in their organizations, as they see the value in protecting sensitive data. Doing so will set an example for employees to follow. Furthermore, managers who consider the personal implications of privacy protection might also be more inclined towards prioritizing it in their organizations. This is supported by existing literature illustrating privacy as inherently personal (Introna and Pouloudi, 1999; Solove, 2008).

4.1.2 Feeling of social responsibility (I1.2)

Managers can feel morally obligated not to harm customers in handling sensitive data (Marcoux, 2003; Velasquez, 2003; De George, 2008), which becomes the focal point when balancing commercial objectives with protecting consumer privacy. A responsibility arises out of situations "where one party in a relationship is at a disadvantage with regard to the other" (Culnan and Williams, 2009), e.g., where data collection provides an advantage to data controllers over data subjects. This may also be reflected by a manager's responsibility for a firm's ethical behavior toward privacy rights in terms of safeguarding customer data, or the responsibility of a manager to care for a company's impact on society at large.

> "*I treat privacy not only as a compliance matter, but as a human right.*" (IP6)

4.2 Relational factors

CSR enables the strengthening of social relationships, as well as the alleviation of perceived negative feelings between an organization and its community (Clary and Snyder, 1999). Accordingly, relational incentives stem from an organization's desire to maintain positive relationships with its stakeholders by promoting their interests, thereby increasing trust and acquiring social legitimacy (Aguilera et al., 2007).

4.2.1 Trust building with stakeholders (I2.1)

In some cases, managers are willing to accept responsibility for appropriately protecting privacy and protecting individuals from the negative consequences of privacy protection failures, in line with the argument that accountability should become a "primary means by which society addresses issues of appropriate information usage" (Weitzner et al., 2008). In turn, an accountability-based approach can help organizations ease their operations and achieve trust with stakeholders (Pearson, 2012). Customers are more likely to trust organizations that are transparent about how they collect, store, and use personal data and that take measures to protect it. This notion, therefore, reflects a crucial factor in privacy protection, which is to gain trust through openness and transparency (Cavoukian et al., 2010). As a result, caring for customer data also enhances relationships with stakeholders.

The interviews also shed light on three aspects of stakeholder relations that can properly motivate the pursuit of privacy protection. Some "companies think about [privacy] as trust, where they really think

about customers' long-term trust that they want to retain" (IP4). In turn, "long-term trust" becomes crucial to gaining customer loyalty. Beyond this, increasing stakeholder satisfaction with a company's management of personal data can be viewed as an important motivational factor for privacy protection. Similarly, continuous cooperation with secondary stakeholders becomes important for ensuring the long-term success of the company. Chan and Greenaway (2005) argue that organizations choose the type of legitimacy they seek to obtain through their privacy practices. In line with this, firms that acknowledge their moral responsibilities are more likely to earn legitimacy among key internal stakeholders (Culnan and Williams, 2009). As such, managers who value trustworthiness may be well-served to place emphasis on their organization's privacy practices.

4.2.2 Provision of a good product or service (I2.2)

Allen and Peloza (2015) show that consumers and employees appreciate social responsibility efforts that prioritize their needs, which can be expanded to include privacy as an important factor in the provision of a product or service. By understanding privacy's value for customers and using it as a product or service differentiator, managers are thinking about the privacy needs of customers, which in turn can lead to enhanced customer relationships in meeting customer privacy expectations. For companies to provide a good product or service in terms of privacy protection, viewing privacy protection as a feature extends the value of privacy beyond reducing business risk to ensuring that data "gives your business proper value for money" (IP3).

> *"If the goal is to protect the customer and behave ethically, you have to think of privacy as a product and a feature rather than just a cause.*" (IP3)

4.3 Instrumental factors

According to CSR research (Pollach, 2011; Aguilera et al., 2007), firms engage in CSR activities for instrumental reasons that serve their corporate self-interest. Thus, companies can use CSR initiatives to gain a competitive advantage, enhance reputation, or avoid costly fines.

4.3.1 Legal and regulatory compliance (I3.1)

Amongst all factors, compliance can often be the most immediate incentive, as the legal mandate put forth is non-negotiable. Especially highlighted were the existential implications of privacy protection, or rather the lack thereof, and the fact that these consequences can be particularly harmful in the case of startups, as well as for larger, more established organizations. Therefore, managers want to avoid non-compliance incidents or breaches, which can threaten the loss of revenue or personal data.

4.3.2 Competitive advantage (I3.2)

Companies try to gain a competitive advantage through strategic differentiation (Chan and Greenaway, 2005). In this context, managers may adopt privacy protection measures to differentiate themselves from direct competitors without such a privacy focus and, as such, gain a competitive edge (Cavoukian et al., 2010). Such value of privacy has been supported by previous research that showed that customers tend to choose companies that offer more privacy protection and are even willing to pay a premium for privacy (Tsai et al., 2011). In the particular case of PETs, promoting privacy protection via the use of PETs can serve as a unique selling point with which a product or service is marketed. Moreover, by becoming a "first-mover" for privacy protection, an organization can become a leader in the market from a privacy perspective. Following the lead of competitors who already focus on privacy, some managers can also be motivated for privacy protection due to herd or mimicry behavior.

4.3.3 Reputation and brand image (I3.3)

Among the benefits of being a first mover is an enhanced reputation as "someone who is leading the way when it comes to privacy" (Jaatun et al., 2012) in the eyes of important stakeholders. The level of

privacy protection an organization follows can strengthen its reputation, helping to gain a reputational advantage. There may also exist an expectation of organizations to demonstrate CSR, including privacy (Jaatun et al., 2012). Borking (2009) asserts that "organizations take leadership roles even though there may not be immediate financial compensation, because of the value of the organization's reputation."

4.3.4 Risk mitigation (I3.4)

Privacy protection measures serve to prevent breaches, which in turn enable an organization to become a better "custodian" of data. In this way, not only is risk mitigated, but data processing practices are also optimized, thereby "minimizing the impacts when something bad happens" (IP5). In a study by London Economics (2010), the role of PETs in the prevention of economic damage is highlighted. Hence, the implementation of sound technical measures can mitigate the financial harm imposed by a privacy breach, since such technologies are designed to protect individuals even if data is leaked.

Existing literature suggests that both the disclosure of privacy-invasive practices (Jaatun et al., 2012; Allen and Peloza, 2015; Bestman et al., 2022) and privacy breaches can lead to reputational damage for organizations (Borking, 2009; Culnan and Williams, 2009; Greenaway and Chan, 2013; London Economics, 2010; Parks et al., 2011). As such, privacy-protective practices and prevention of privacy breaches can serve to safeguard an organization's reputation.

In a similar vein, previous research (Borking, 2009; Culnan and Williams, 2009; Fairchild and Ribbers, 2011; Greenaway and Chan, 2013) shows that companies can face business losses as a result of insufficient privacy practices. These losses can include the loss of customers (Borking, 2009) or sensitive corporate data, such as trade secrets and intellectual property (Culnan and Williams, 2009). As an additional factor, Culnan and Williams (2009) argue that privacy incidents encountered by one organization can lead to spillover effects for the entire industry, causing "firms in the same industry to incur substantial new costs even though they were uninvolved in the original crisis."

4.3.5 Long-term success (I3.5)

Adopting sound privacy practices can demonstrate to potential employees that privacy protection is a core value, helping to retain employees in the long run, in the way that a culture of privacy is created.

In line with such culture, Senarath and Arachchilage (2017) argue that some organizations take a proactive, user-centered approach toward privacy that goes beyond "merely complying with government regulations on data breach prevention." By demonstrating a strong privacy commitment in their privacy practices, organizations can attract customer segments with similar values. Additionally, adopting good privacy practices can lead to the long-term sustainability of an organization, and, in some cases, even add to business value, a topic closely related to organizational sustainability (Bestman et al., 2022).

When privacy is closely linked to the business model and is not just a compliance matter, privacy protection becomes a "must," especially in industries where "you can't sell if you are not compliant" (IP2). This relates to the desire of managers to demonstrate and improve *business efficiency*. In particular, adopting technologies that safeguard user data leads to enhanced data processing, where more comprehensive data (Jaatun et al., 2012) can be handled in an efficient way (London Economics, 2010). Moreover, users may be more willing to share information with such practices in place. Improved data quality may also be observed since data collection is more "meaningful, contextually sensitive, and proper, and in a way that gives your business proper value for money" (IP3).

4.3.6 Future readiness (I3.6)

Responding to the changing global regulatory landscape with a firm establishment of company vision can solidify privacy as a primary objective. Integrating privacy as part of an organization's vision can help managers motivate the pursuit of privacy protection, and by going beyond the minimum and adopting state-of-the-art practices, managers can ensure that they stay ahead. The adoption of privacy protection measures proactively by managers supports the idea that "privacy concerns can vary

dramatically for the same individual, and for societies, over time" (Acquisti et al., 2022), and companies can benefit "from being ready when the shift occurs" (Jaatun et al., 2012).

As data privacy continues to rise in importance, future regulations will require the use of more complex technologies, such as PETs, that can serve as effective technical solutions to ensure privacy protection. This is also true from the user perspective. According to Jaatun et al. (2012), while "today's users' privacy behavior is best described by the privacy paradox," their privacy expectations for companies could increase as they gain a better understanding of the risks associated with sharing personal information. Likewise, consumers indeed have a fundamental concern for their privacy and frequently take action to safeguard it (Acquisti et al., 2020). Insights like these can influence managerial decisions to pursue privacy protection, in anticipation of rising expectations from end-users.

> "*I think it is extremely critical that a company at least starts making investments and making changes in its culture... the more you do in this domain, the more you realize that you are not just improving privacy, but you are improving your maturity as a business, your efficiency as a business.*" (IP3)

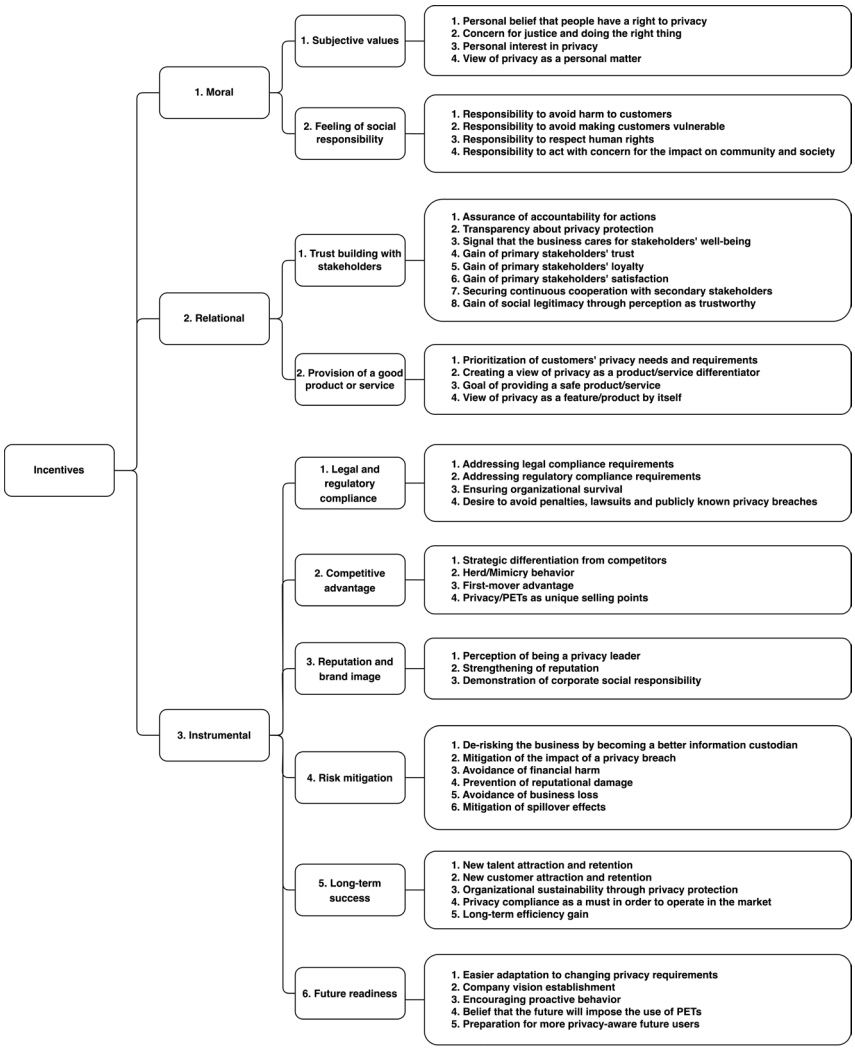

Figure 1. The final taxonomy.

5 Factors Influencing Managerial Decisions to Adopt PETs

In this section, we present the results of our survey, conducted to evaluate the relevance of the factors described in Section 4 as incentives for the adoption of PETs, as seen by the surveyed decision-makers. In the survey, each individual incentive I1.1.1-I3.6.5, presented in Figure 1 was mapped to one or two

survey statements as described in Section 3.5, with response options on the five-point Likert scale. We focus the ensuing discussion on the category and subcategory levels of incentives.

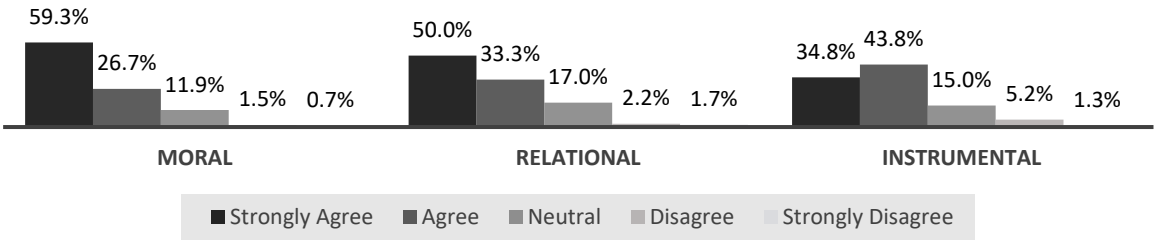

Figure 2. Survey responses, separated by incentive category.

Figure 2 illustrates the distribution of agreement among the three identified categories of motivational factors for the adoption of PETs. As depicted, the moral category obtained the highest number of *"strongly agree"* responses (59.3%), which is almost double the amount received by the instrumental category (34.8%). The moral category also had the highest overall agreement (86%), followed closely by relational (83.3%) and instrumental (78.6%). Although disagreement was quite low, it is worth noting that the instrumental category received the highest number of *disagree* responses. The results suggest that surveyed managers are most motivated by moral reasons to adopt PETs. This mindset demonstrates a morally-driven commitment to responsible business practices and a willingness to safeguard privacy.

5.1 Moral incentives to adopt PETs

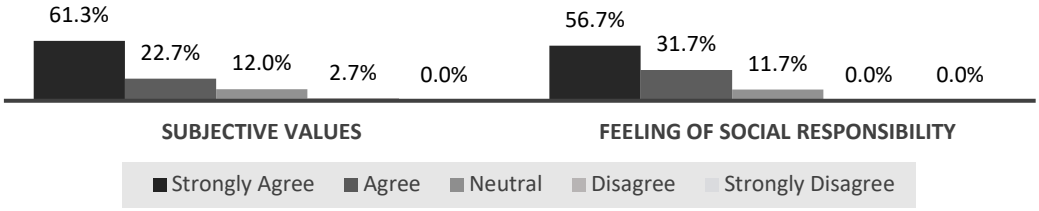

Figure 3. Survey responses from the Moral incentives category.

As illustrated in Figure 3, both moral subcategories received a high level of agreement. *Subjective values (I1.1)* obtained an agreement level of 84% and *Feeling of social responsibility (I1.2)* received 89.4% agreement. While the first subcategory had low disagreement at 2.7%, the second subcategory received no negative responses at all. I1.2 distinguishes itself from I1.1 in that it is motivated by a sense of responsibility or even obligation towards privacy protection. The observed results, therefore, suggest that although survey participants consider their strong personal values to be important incentives for adopting PETs, the feeling of social responsibility may be an even more compelling driver.

Overall, our quantitative data findings confirm the general acceptance of all individual factors from both moral subcategories as incentives for the adoption of PETs. This highlights the perceived importance of ethical considerations in the decision-making process of companies regarding privacy protection measures. Specifically, our findings indicate that surveyed managers prioritize the personal implications of privacy protection, acknowledge the responsibility to prevent harm to customers, recognize the vulnerability of customers when their sensitive data is collected, and regard fulfilling their obligation to respect human rights and act with concern for the community as important motivators for adopting PETs.

5.2 Relational incentives to adopt PETs

Figure 4 illustrates that both relational subcategories of incentives to adopt PETs received a high level of agreement. The first relational subcategory, *Trust building with stakeholders (I2.1)*, received positive

responses from 80.9% of the participants, while the second subcategory, *Provision of a good product or service (I2.2)*, was positively endorsed by 86.7%. Both subcategories received 1.7% *strongly disagree* responses, and in addition, I2.1 also received 3.3% *disagree* responses. The provision of a good product or service regarding privacy is perceived by managers as a stronger incentive for adopting PETs compared to developing social legitimacy among stakeholders. It should be noted, though, that on the individual factor level, survey respondents unanimously agreed on the importance of gaining primary stakeholders' *trust (I2.1.4)*. At the same time, factors related to gaining stakeholders' *loyalty (I2.1.5)* and *satisfaction (2.1.6)* gained notably lower agreement rates, 73.3% and 80%, respectively.

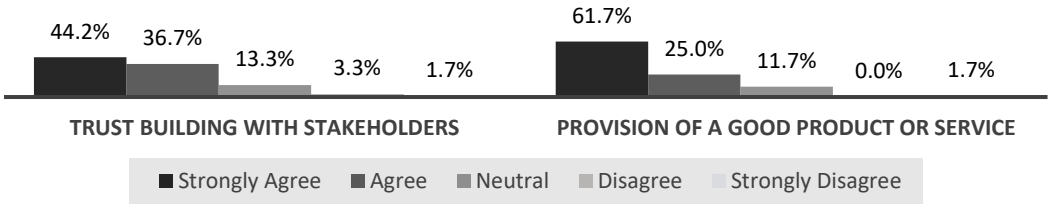

Figure 4. Survey responses from the Relational incentives category.

The results indicate that surveyed managers understand the potential impact of privacy breaches on stakeholders. Furthermore, our findings show that meeting customers' privacy expectations, particularly when privacy is considered a distinct product or feature, strongly motivates managerial decisions to adopt PETs. Therefore, we argue that organizations committed to delivering safe products or services and satisfying customers' privacy expectations are more likely to invest in PETs.

5.3 Instrumental incentives to adopt PETs

Figure 5 provides an overview of the survey agreement levels with the instrumental subcategories. Overall, all subcategories related to the company's self-serving interests obtained an agreement level exceeding 51%. The highest number of *strongly agree* responses (57%) was received by *Legal and regulatory compliance (I3.1)*, while *Long-term success (I3.5)* received the most *agree* replies (53%). In terms of agreement level, *Risk mitigation (I3.4)*, obtained the highest score (92.4%), closely followed by *Legal and regulatory compliance (I3.1)* (91.7%). This highlights the significance of achieving regulatory compliance and mitigating risks as incentives for adopting PETs, perceived equally by survey respondents from highly regulated industries (pharmaceuticals, finance, electronics) as well as those in other industries. It is also worth noting that both subcategories are related to perceiving privacy as a risk rather than an opportunity, which may strongly resonate with the survey participants.

The analysis of the individual factors showed that the surveyed managers consider PETs as technical measures for mitigating risk and achieving regulatory compliance, see the implementation of PETs as a possible means for strategic differentiation from competitors, and express a strong belief that customers and users will become more privacy-aware in the future. Interestingly, although none of the factors in the instrumental category were disproved, this category contained some of the least agreed-upon factors.

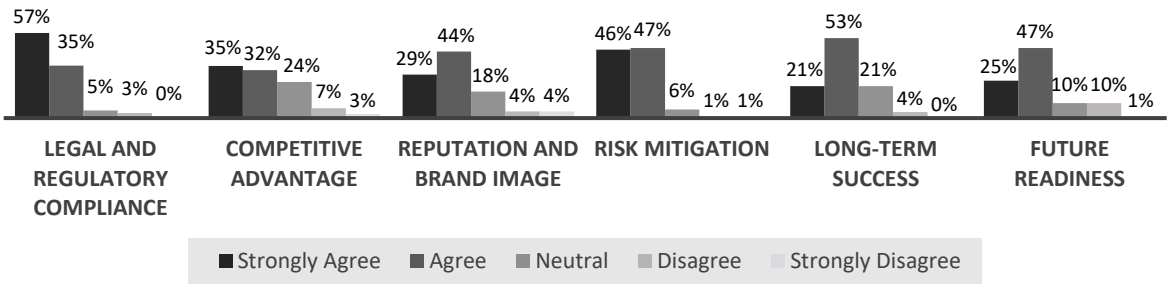

Figure 5. Survey responses from the Instrumental incentives category.

5.4 Most endorsed incentives

The results of our quantitative evaluation showed that at the category level, the surveyed decision-makers are more strongly driven by moral reasons than by relational or instrumental reasons to adopt PETs as technical measures for privacy protection. This demonstrates that these managers are primarily motivated by the ethical implications of privacy rather than by enhancing key stakeholder relationships or solely serving the company's self-interest. At the taxonomy's subcategory level, the following six subcategories received the most *strongly agree (SA)* and *agree (A)* responses:

- I3.4 Risk mitigation, **92.4%** (SA: 45.7%, A: 46.7%)
- I3.1 Legal and regulatory compliance, **91.7%** (SA: 56.7%, A: 35.0%)
- I1.2 Feeling of social responsibility, **88.4%** (SA: 56.7%, A: 31.7%)
- I2.2 Provision of a good product or service, **86.7%** (SA: 61.7%, A: 25.0%)
- I1.1 Subjective values, **84.0%** (SA: 61.3%, A: 22.7%)
- I2.1 Trust building with stakeholders, **81.7%** (SA: 44.2%, A: 37.5%)

A closer analysis of the top-endorsed incentives reveals that when a distinction between *strongly agree* and *agree* responses is made, namely when these are weighted accordingly, the order of the top incentives changes. Using the Likert scale's five distinct values, we map all response options to a score: {*strongly agree*: 2, *agree*: 1, *neutral*: 0, *disagree*: -1, *strongly disagree*: -2}. Each survey statement can then be represented by the average score of all responses; likewise, each incentive category can be represented by the aggregate (mean) of all corresponding survey statements. The mean and standard deviation (SD) results of this scoring scheme for the top six incentives are as follows:

- I2.2 Provision of a good product or service, (Mean: 1.45, SD: 0.68)
- I3.1 Legal and regulatory compliance, (Mean: 1.45, SD: 0.84)
- I1.2 Feeling of social responsibility, (Mean: 1.45, SD: 0.86)
- I1.1 Subjective values, (Mean: 1.40, SD: 0.78)
- I3.4 Risk mitigation, (Mean: 1.35, SD: 0.67)
- I2.1 Trust building with stakeholders, (Mean: 1.19, SD: 1.00)

These findings highlight that compliance is not the sole determinant influencing the adoption of PETs in the industry. Notably, there are exactly two moral, two relational, and two instrumental subcategories among the six most agreed-upon subcategories. This further supports the inclusion of moral, relational, and instrumental reasons for engaging in CSR as foundational characteristics of the taxonomy, providing further evidence for the link between CSR and the adoption of PETs.

Among individual motivational factors for the adoption of PETs, four were met with unanimous agreement by *all* survey participants. The order in which these factors are presented is based on the number of *strongly agree* responses they elicited (highest first):

- I2.1.4 Gain of primary stakeholders' trust (SA: 73.3%, A: 26.7%)
- I3.1.4 Avoid penalties, lawsuits, and publicly known privacy breaches (SA: 66.7%, A: 33.3%)
- I3.1.2 Addressing regulatory compliance requirements (SA: 53.3%, A: 46.7%)
- I3.5.4 Privacy compliance as a must to operate in the market (SA: 33.3%, A: 66.7%)

One may take away from these results that managers are indeed highly incentivized by certain instrumental factors. Nevertheless, the high scores in the moral category would imply that managers are also strongly motivated by more subjective reasons, contrary to the possible assumption that organizational decision-making is purely instrumental. Our findings show that this is in fact not always the case, as the instrumental category also contains some of the most disagreed with incentives.

Overall, surveyed managers recognized the relevance of all motivational factors presented in Figure 1 as incentives for the adoption of PETs, with our quantitative results yielding a majority of agreement for all incentives. As such, no further changes to the taxonomy presented in Figure 1 were made.

6 Conclusion

In this work, we investigate the motivational factors influencing managerial decisions to adopt PETs. We first focus on privacy protection, looking to existing literature and insights from industry leaders to derive the primary motives in meeting the decision to invest in privacy. We structure the 47 identified incentives in categories relating to the moral, relational, and instrumental factors influencing privacy-related decisions. These incentives are taxonomized and presented in a survey to validate their relevance, specifically for the adoption of PETs. Having observed a large majority of agreement in the survey, we are confident that our contributions not only have practical relevance but also accurately represent the perspective of privacy decision-makers.

6.1 Limitations

The limitations of our work lie mainly in the relative niche target group, namely managers and decision-makers in privacy. Limitations arising from this include the bias towards interviewees from large-sized organizations, the relatively smaller sample sizes, and the lack of regional diversity (only European and American respondents). The authors are confident in the generalizability of the findings due to (1) the rigorous approach of the thematic analysis, and (2) an observed saturation of themes. Nevertheless, follow-up studies are recommended to verify our presented findings, particularly across larger samples in more geographically diverse settings.

6.2 Implications and future work

Our findings provide motivation for future work on the research and development of PETs, as well as their adoption in practice. Using CSR as a basis for structuring these motivating factors makes a tangible connection between the core tenets of CSR, that is "going *beyond* the narrow economic, technical, and legal requirements" (Davis, 1973), and the practical reasons for implementing PETs as technical measures for privacy protection that go *above* the "bare minimum." To the best of our knowledge, our work is the first to view PETs and CSR in the same light, thereby bridging the two fields.

The theoretical implications of our work include adding to the body of knowledge and study regarding the managerial role in privacy protection. In particular, we introduce the novel aspect of incentives for PET adoption, an aspect previously not covered in the literature. At the same time, our work possesses clear practical implications, setting the foundations for clearly outlined incentives for data protection programs. Provided with a broad range of possible incentives for privacy protection and PETs, practitioners may be better equipped to define clear strategies motivating the use of PETs in practice.

As paths for future work, firstly, the connection between Corporate Digital Responsibility (Lobschat et al., 2021) and PETs presents a logical next point of investigation. This may give way to a new concept of corporate responsibility specifically aimed at privacy practices. Focusing on the organizational side, viewing our identified factors in the context of the information privacy assimilation framework (Halder et al., 2022) may be of interest to researchers. Finally, in-depth investigations into any of the CSR subcategories or individual factors, as well as determining the corresponding strategies to motivate and enhance the adoption of PETs in practice, represent clear ways forward for future research.

Together, our findings and proposed artifact give credence to the benefit of PETs in the ongoing debate on data privacy in the age of big data. Our research highlights the many possible motivators for privacy protection, as well as the complexity with which such a decision comes. In the discussion surrounding the benefits and challenges of PETs, we hope that this work serves as a motivational foundation not only for managers, but for researchers and practitioners alike, to tread forth in the pursuit of data privacy.

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4):736–758.

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2022). Privacy and behavioral economics. In Modern Socio-Technical Perspectives on Privacy, pages 61–77. Springer, Cham.

Aguilera, R. V., Rupp, D. E., Williams, C. A., and Ganapathi, J. (2007). Putting the S back in corporate social responsibility: A multilevel theory of social change in organizations. Academy of management review, 32(3):836–863.

Allen, A. M. and Peloza, J. (2015). Someone to watch over me: The integration of privacy and corporate social responsibility. Business Horizons, 58(6):635–642.

Åstedt-Kurki, P. and Heikkinen, R.-L. (1994). Two approaches to the study of experiences of health and old age: the thematic interview and the narrative method. Journal of advanced nursing, 20(3):418–421.

Bestman, A., Chinyere, J., and Adebayo, A. (2022). Strategic use of information privacy for organizational sustainability. The Strategic Journal of Business & Change Management, 9(3):517–527.

Borking, J. (2009). Organizational motives for adopting privacy enhancing technologies (PETs). In D 7.3 PRISE Conference Proceedings: "Towards privacy enhancing security technologies–the next steps" Vienna, April 28th and 29th 2008, page 43. Citeseer.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2):77–101.

Carroll, A. B. (1979). A three-dimensional conceptual model of corporate performance. Academy of management review, 4(4):497–505.

Cavoukian, A., Taylor, S., and Abrams, M. E. (2010). Privacy by design: essential for organizational accountability and strong business practices. Identity in the Information Society, 3(2):405–413.

Chan, Y. E. and Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. Journal of the Association for Information Systems, 6(6):7.

Clary, E. G. and Snyder, M. (1999). The motivations to volunteer: Theoretical and practical considerations. Current directions in psychological science, 8(5):156–159.

Creswell, J. W. and Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Culnan, M. J. and Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS Quarterly, pages 673–687.

Davis, K. (1973). The case for and against business assumption of social responsibilities. Academy of Management journal, 16(2):312–322.

De George, R. T. (2008). The ethics of information technology and business. John Wiley & Sons.

Dearnley, C. (2005). A reflection on the use of semi-structured interviews. Nurse researcher, 13(1).

Fairchild, A. and Ribbers, P. (2011). Privacy-enhancing identity management in business. Digital Privacy: PRIME-Privacy and Identity Management for Europe, pages 107–129.

Greenaway, K. E. and Chan, Y. E. (2013). Designing a customer information privacy program aligned with organizational priorities. MIS Quarterly Executive, 12(3).

Greene, J. C., Caracelli, V. J., and Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. Educational evaluation and policy analysis, 11(3):255–274.

Halder, S., Attili, V. P., and Gupta, V. (2022). Information privacy assimilation: An organizational framework. International Journal of Digital Strategy, Governance, and Business Transformation (IJDSGBT), 12(1):1–17.

Hansen, M., Hoepman, J.-H., Jensen, M., and Schiffner, S. (2015). Readiness analysis for the adoption and evolution of privacy enhancing technologies: methodology, pilot assessment, and continuity plan. Technical report: ENISA.

Heavin, C. and Power, D. J. (2018). Challenges for digital transformation–towards a conceptual decision support guide for managers. Journal of Decision Systems, 27(sup1):38–45.

Information Commissioner's Office (2022). Chapter 5: Privacy-enhancing technologies (PETs) | draft anonymisation, pseudonymisation and privacy enhancing technologies guidance.

Introna, L. and Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. Journal of Business Ethics, 22:27–38.

Jaatun, M. G., Tøndel, I. A., Bernsmed, K., and Nyre, Å. A. (2012). Privacy enhancing technologies for information control. In Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, pages 1–31. IGI Global.

Kallio, H., Pietilä, A.-M., Johnson, M., and Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of advanced nursing, 72(12):2954–2965.

Kitchenham, B. A., Budgen, D., and Brereton, P. (2015). Evidence-based software engineering and systematic reviews, volume 4. CRC press.

Klymenko, O., Kosenkov, O., Meisenbacher, S., Elahidoost, P., Mendez, D., and Matthes, F. (2022). Understanding the implementation of technical measures in the process of data privacy compliance: A qualitative study. In Proceedings of the 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, pages 261–271.

Klymenko, O., Meisenbacher, S., and Matthes, F. (2023). Identifying practical challenges in the implementation of technical measures for data privacy compliance. AMCIS 2023 Proceedings. 2

Lapadat, J. C. and Lindsay, A. C. (1999). Transcription in research and practice: From standardization of technique to interpretive positionings. Qualitative inquiry, 5(1):64–86

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., and Wirtz, J. (2021). Corporate digital responsibility. Journal of Business Research, 122:875–888.

London Economics (2010). Study on the economic benefits of privacy-enhancing technologies (PETs).

Marcoux, A. M. (2003). A fiduciary argument against stakeholder theory. Business Ethics Quarterly, 13(1):1–24.

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., and Weaven, S. K. (2020). Data privacy in retail. Journal of Retailing, 96(4):474–489

Mintzberg, H. (1983). The case for corporate social responsibility. Journal of Business Strategy.

Nickerson, R. C., Varshney, U., and Muntermann, J. (2013). A method for taxonomy development and its application in information systems. European Journal of Information Systems, 22(3):336–359.

Parks, R., Chu, C., Xu, H., and Adams, L. (2011). Understanding the drivers and outcomes of healthcare organizational privacy responses.

Pearson, S. (2012). Privacy management in global organisations. In IFIP International Conference on Communications and Multimedia Security, pages 217–237. Springer.

Pelteret, M. and Ophoff, J. (2017). Organizational information privacy strategy and the impact of the popi act. In 2017 Information Security for South Africa (ISSA), pages 56–65. IEEE.

Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. Business Ethics: A European Review, 20(1):88–102.

Senarath, A. R. and Arachchilage, N. A. G. (2017). Understanding organizational approach towards end user privacy. arXiv preprint arXiv:1710.03890.

Solove, D. J. (2008). The new vulnerability: Data security and personal information.

Steele, V. (2022). Corporate social responsibility, data protection and the right to privacy. LJMU Student Law Journal, 2.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information systems research, 22(2):254–268

Van Blarkom, G., Borking, J. J., and Olk, J. E. (2003). Handbook of privacy and privacy-enhancing technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 198:14.

Velasquez, M. (2003). Debunking corporate moral responsibility. Business ethics quarterly, 13(4):531–562.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G. J. (2008). Information accountability. Communications of the ACM, 51(6):82–87.

Whiting, L. S. (2008). Semi-structured interviews: guidance for novice researchers. Nursing Standard (through 2013), 22(23):35.