IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 June 2022, accepted 7 July 2022, date of publication 13 July 2022, date of current version 19 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3190373

TOPICAL REVIEW

Organisational Privacy Culture and Climate: A Scoping Review

LEONARDO HORN IWAYA[1,2], **(Member, IEEE), GABRIEL HORN IWAYA**[1], **SIMONE FISCHER-HÜBNER**[2], **(Member, IEEE), AND ANDREA VALÉRIA STEIL**[1]

[1]Graduate Program in Psychology, Department of Psychology, Federal University of Santa Catarina—UFSC, Florianópolis 88040-900, Brazil
[2]Privacy and Security (PriSec) Research Group, Department of Mathematics and Computer Science, Karlstad University, 65188 Karlstad, Sweden

Corresponding author: Leonardo Horn Iwaya (leonardo.iwaya@kau.se)

This work was supported by the Swedish Knowledge Foundation (TRUEdig Project).

ABSTRACT New regulations worldwide are increasingly pressing organisations to review how they collect and process personal data to ensure the protection of individual privacy rights. This organisational transformation involves implementing several privacy practices (e.g., privacy policies, governance frameworks, and privacy-by-design methods) across multiple departments. The literature points to a strong influence of the organisations' culture and climate in implementing such privacy practices, depending on how leaders and employees perceive and address privacy concerns. However, this new hybrid topic referred to as Organisational Privacy Culture and Climate (OPCC), remains poorly demarcated and weakly defined. In this paper, we report a Scoping Review (ScR) on the topic of OPCC to systematically identify and map studies, contributing with a synthesis of the existing work, distinguishing core and adjacent publications, research gaps, and pathways of future research. This ScR includes 36 studies categorised according to their demographics, research types, contribution types, research designs, proposed definitions, and conceptualisations. Also, 18 studies categorised as primary research were critically appraised, assessing the studies' methodological quality and credibility of the evidence. Although published research has significantly advanced the topic of OPCC, more research is still needed. Our findings show that the topic is still in its embryonic stage. The theory behind OPCC has not yet been fully articulated, even though some definitions have been independently proposed. Only one measuring instrument for privacy culture was identified, but it needs to be further developed in terms of identifying and analysing its factors, and evaluating its validity and reliability. Initiatives of future research in OPCC will require interdisciplinary research efforts and close cooperation with industry to further propose and rigorously evaluate instruments. Only then OPCC would be considered an evidence-based research topic that can be reliably used to evaluate, measure, and embed privacy in organisations.

INDEX TERMS Privacy, data protection, organisational culture, organisational climate, privacy culture, privacy climate, reviews.

I. INTRODUCTION

In recent years, several countries and jurisdictions have enacted privacy and data protection regulations, e.g., the European General Data Protection Regulation (GDPR) [1], the California Consumer Privacy Act (CCPA) [2], the Brazilian General Data Protection Law (LGPD) [3], and the Chinese Data Privacy Framework, including China's Personal Information Privacy Law (PIPL) [4]. Considering the GDPR (Article 83) [1], non-compliance can lead to fines of up to 20 million euros or up to 4% of a company's worldwide annual turnover, whichever is higher. Studies also indicate an increasing number of fines based on the GDPR since its publication [5], [6], with the largest fine imposed by the Luxembourg's Data Protection Authority against Amazon (746 million euros) in July 2021 [7]. This scenario has forced many organisations to adapt and implement new *privacy practices* to achieve regulatory compliance and, most

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

importantly, to respect people's privacy when developing and applying new technology [3], [8], [9].

Here, we refer to privacy practices as a wide range of technical and organisational privacy controls inside the company. For instance, writing privacy policies, appointing data protection officers, performing privacy impact assessments, or adopting privacy-by-design methodologies. However, recent research proposes that the adoption of such privacy practices is strongly influenced by an organisation's culture and climate and how employees perceive and address privacy concerns in working systems [10]–[12]. These studies also stress the role of leaders and senior management in setting a culture of privacy in organisations [11]–[13]. Therefore, apart from the mere knowledge of privacy practices, organisations have also to tackle the challenge of creating a conducive environment that values and fosters information privacy across all departments involved with the collection and processing of personal data. This, in turn, also influences the adoption of organisation-wide privacy governance strategies and the successful implementation of a myriad of required privacy practices.

Given that, researchers are starting to use terms such as *information protection culture* [10], *organisational privacy climate* [11], [12], and *organisational privacy culture* [13] to refer to this hybrid emerging topic between areas of (a) Organisational Culture and Climate and (b) Information Privacy. However, the theory behind Organisational Privacy Culture and Climate (OPCC) remains poorly demarcated, pointing to a significant research gap for both scholars and practitioners. The topic still lacks established definitions, let alone rigorously validated instruments to assess and measure privacy-related factors in organisations reliably. Furthermore, the emerging evidence on OPCC has not yet been systematically assessed to examine the extent, range, and nature of available research, which would constitute the initial step in research development. Therefore, there is an urgent need to first map and summarise the existing work on the topic of OPCC, helping to inform future research efforts that can later ground evidence-based practices.

In this paper, our objective is to carry out a Scoping Review (ScR) [14] on the topic of OPCC to identify, map, and synthesise existing work. As an overarching research question, we ask: *What is "this thing" called Organisational Privacy Culture and Climate?* (a question that we further elaborate on in Section III-A2). We followed the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) as our methodology. Specifically, the PRISMA extension for Scoping Reviews (PRISMA-ScR) [15].

A total of 36 studies were systematically selected and classified according to various demographics, e.g., types of research, contributions, authors and affiliations, and publication venues. The main definitions and conceptualisations for OPCC are identified and discussed. We propose separating studies into two main groups, (1) adjacent/motivational research and (2) core research in the area. We also present a critical appraisal of the existing primary research (quantitative and qualitative) and discuss the current strength of evidence in the topic.

As a result, this work contributes by synthesising the body of knowledge on OPCC. This ScR offers academics a comprehensive overview, identifies main research gaps, and presents pathways for future research. It also informs practitioners (e.g., psychologists, leaders, and software professionals) about the current state-of-the-art on OPCC, emphasising that the topic ought to be fostered in organisations but still approached carefully due to the lack of scientific evidence. Overall, yet promising, the topic of OPCC is still at its embryonic stage. Therefore, a joint effort from multiple disciplines (e.g., computer science, organisational psychology, management, and law) is still warranted for building the theory and practical instruments on the topic. This and other research gaps are further examined in this paper.

II. LITERATURE REVIEW

A. INFORMATION SECURITY IS NOT INFORMATION PRIVACY

Although many researchers have used the term privacy within the scope of security, or even interchangeably, it is crucial to understand the differences. According to National Institute of Standards and Technology (NIST) guidelines [16], the term "information security" refers to the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. The concepts of confidentiality, integrity, and availability (CIA) are also defined by [16]:

- The term "confidentiality" means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- The term "integrity" means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- The term "availability" means ensuring timely and reliable access to and use of information.

Although these definitions point to an overlap between information security and information privacy, particularly on the confidentiality of personal data, there are still fundamental differences.

Privacy as a broad concept concerns to the rights and freedoms of natural persons and their data rather than just protecting information systems. Privacy can be framed as a fundamental human right, both in terms of physical privacy and "information privacy" [17]. In this work, we are particularly interested in the latter, i.e., in the context of organisations processing personal data in working systems. Although there is no absolute agreement on the definition of privacy, in this paper, we consider the proposition of Westin and Solove [18]: *"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"* [18].

Privacy is, therefore, subjected to the individuals' claims, self-determination, and choices in regards to their data.

Moreover, various laws and regulations add other concepts to the umbrella term of privacy. For instance, the GDPR [1], covering principles such as lawfulness, consent, purpose binding, data minimisation, and transparency which are disjointed or have little overlap with information security. Another example is the complement of the CIA triad with the three additional privacy protection goals of unlinkability, transparency and intervenability, as proposed in [9], [19]:

- The term "unlinkability" refers to separating data and processes, meaning that processes must be operated in such a way that the personal data are unlinkable to any other set of personal data outside of the domain.
- The term "transparency" refers to adequately and clearly describing the personal data processing activities so that the collection, processing and use of the information can be understood and reconstructed at any time.
- The term "intervenability" refers to the data subjects' ability to interfere with personal data that has been collected or is being processed.

Hence, it should be clear that whilst information privacy is protected through information security measures, privacy cannot be satisfied solely on the basis of managing security [20].

Apart from information security, the term "information protection" is also used, sometimes to refer specifically to information privacy. Even well-known privacy laws, such as the GDPR [1], use the term "data protection" in their titles, possibly encouraging researchers to use this narrower term instead of information privacy. However, as previously explained, information privacy is more than just protecting personal information.

B. PRIVACY AND ORGANISATIONS

Recent national privacy and data protection legislations have put new requirements on organisations. Especially the GDPR [1] had a major impact on privacy policies and routines for organisations in the EU but also for non-European organisations that according to Art. 3 GDPR have also to comply with the GDPR if they offer goods or services to data subjects in the EU or monitor the behaviour of users in the EU. Moreover, personal data transfer is in general restricted to third countries outside the EU that have an adequate level of data protection (Art 45). Meeting this adequacy principle of the GDPR for enabling data exchanges with European organisations has also motivated several non-European countries to revise or enact national data protection legislation that largely complies with GDPR principles. Due to the strong power that the GDPR has worldwide, we focus in this section on discussing the impact of the GDPR on organisations.

The GDPR mandates requirements for several data protection measures that organisations must implement. For this, a risk-based approach needs to be taken by the organisations tailoring data protection measures to the respective risks. This means that data controllers and processors have to implement protective measures that are appropriate, corresponding to the risk levels of their data processing activities. Several obligations, such as the obligation to implement an adequate level of data security or obligations for enforcing data subject's rights for data access, correction or deletion, were already part of the previous EU Data Protection Directive that was replaced by the GDPR. Specific new responsibilities that the GDPR has introduced include [1]:

- **The Data Protection by Design and Default principle** of Art. 25 GDPR: According to this principle, the data controllers are particularly required to implement appropriate technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start.
- **Data Breach notification** according to Art. 33 and 34: If a data breach occurs, and it is likely that the breach poses a risk to an individual's rights and freedoms, the data controller has to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach. If the data breach poses a high risk to the data subjects affected then they should all also be informed.
- Pursuant to Art 35, a **Data Protection Impact Assessment (DPIA)** is required in case that the processing is likely to result in a high risk to the rights and freedoms of the data subjects. This includes cases of systematic or extensive user profiling, processing of sensitive data on a large scale, or in the case of a systematic monitoring of public areas on a large scale.
- The obligation to respond to extended data subject controls and rights including the right to easily withdraw consent at any time (Art. 7), the right to be forgotten (Art. 17), or the right to data portability (Art. 20).

Art. 83 that allows the Supervisory Authority to impose administrative fines for infringement of the GDPR, has been a strong motivating factor for many organisations to strive for GDPR compliance. While with the earlier EU Data Protection Directive, fines were low and thus often not deterring non-compliance on purpose or by negligence, this situation is different with the GDPR that introduces fines that can really "hurt" an organisation, with possible fines of up to 4% of the global turnover or 20 million euros.

Especially the new obligations that were imposed by the GDPR in combination with the threat of high fines in cases of non-compliance, have urged organisations to implement new guidelines, routines and procedures for impacting relevant stakeholders in organisations to consider and think in terms of data protection by design and default, for implementing new effective procedures for rapid privacy breach handling and reporting, for conducting DPIAs, for consent management and effective (automated) handling of data subject rights request.

All these measures impose required changes in organisations, as addressed by several papers that are part of our scoping review, which will be further discussed in this paper.

In particular, the links between information privacy in relation to organisational culture and climate, and how it influences that ways that leaders and employees perceive and deal with privacy concerns.

C. ORGANISATIONAL CLIMATE AND CULTURE

Organisational climate and organisational culture are two important constructs for defining the way people perceive, experience and describe their work settings [21]–[23]. Research on organisational climate can be traced back to the 1960s and 1970s, while the interest in organisational culture spread in the 1980s.

Organisational climate can be defined as *"the shared perceptions of the meaning attached to the policies, practices, and procedures employees experience and the behaviors they observe getting rewarded and that are supported and expected"* [23] (p. 362). Earlier research on organisational climate operationalised it as a broad construct (i.e., the whole organisational functioning). More recently, there has been growing interest in an organisational climate with a specific focus. Examples include customer service climate [24], safety climate [25], initiative climate [26], learning climate [27], information security climate [28], and privacy climate [11].

Measures of climate with a specific focus on organisations have yielded better results than general climate metrics because they focus first on the outcome to be predicted and then proceed to the development of specific climate items. In doing so, it is possible to measure not only the specific climate but also its antecedents, consequences and potential moderators [23]. Besides, robust studies on a specific climate (i.e., privacy climate) could predict relevant organisational outcomes such as compliance with privacy regulations, ensuring transparency, avoiding data breaches, or empowering the data subjects to exercise their various privacy rights.

Organisational culture, on the other hand, has its conceptual and methodological basis in anthropology and was largely embraced by areas such as organisational studies and organisational psychology. In the early eighties, Smircich [29] distinguished competing definitional approaches to organisational culture as something an organisation **has** versus something an organisation **is**. Studies following the first approach (organisations have cultures) tend to describe what would be an effective organisational culture and how it could be managed in order that organisations succeed. Studies based on the second approach (organisations are cultures) focus on how organisational members develop shared meanings and basic assumptions about the organisation they work. This dilemma persists in today's studies on organisational culture.

Notwithstanding the lack of consensus if organisational culture is something an organisation has or something an organisation is, organisational culture may be broadly defined *"as the shared basic assumptions, values, and beliefs that characterize a setting and are taught to newcomers as the proper way to think and feel, communicated by the myths and stories people tell about how the organization came to be the way it is as it solved problems associated with external adaptation and internal integration"* [23] (p. 362).

The three most prevalent themes in the research on organisational culture focus on (1) leadership, (2) the relation between national culture and organisational culture, and (3) organisational culture as a moderator variable [23] (p. 362). Regarding the studies on leadership, the most prominent author is Schein [30] with his contributions on how organisational founders and leaders embed their values through multiple primary (i.e., resource allocation, rewarding systems and status, selection and promotion strategies) and secondary mechanisms (i.e., organisational systems, procedures, design and structure, rites and rituals, stories, organisational philosophy, creeds, and charters) in the organisation. The notion that organisational culture manifests itself in artefacts, espoused beliefs and values, and basic assumptions taken for granted is widely accepted and derived from Schein's approach. The second theme focuses on understanding how and to what extent national culture shapes organisations located in the respective nation, being Hofstede [31] its most influential scholar. Hofstede [32] developed a model of six dimensions of national cultures: power distance, uncertainty avoidance, individualism/collectivism, masculinity/femininity, long/short term orientation, and indulgence/restraint that influence the culture of organisations located in it. Recent studies on this theme compare the relationship between organisational culture and organisational effectiveness (i.e., Hartnell *et al.* [33]). The third most prevalent theme treats organisational culture as a moderator of the relationship between other constructs. An example of this theme is the study of Erdogan *et al.* [34] which found out that different dimensions of organisational culture strengthened or weakened the relationship between interactional justice and leader-member exchange in a sample of teachers from high schools in Turkey. Nonetheless, some studies also approach the topic differently, aiming to determine the association between explanatory factors of organisational culture and their correlations to performance variables. For instance, the work of [35] shows that organisational culture has a significant impact on employee's job performance, with employees' participation as the most critical factor for achieving organisational goals of software houses in Pakistan. Similarly, the study of Shahzad *et al.* [36] shows that organisational innovation performance is backed and affected by organisational culture, suggesting that factors such as flexibility/support to change and organisational climate have a comparable significant influence on creativity and innovation performance.

Organisational culture is associated with continuity since it embeds shared norms and values in the minds of workers as *"a pattern of recipes for handling situations, then very often with time and routine they become tacit and taken for granted and form the schemas which drive action"* [37] (p. 559). Organisational culture is understood as a broad construct, with general dimensions, comprising the whole organisation;

however, growing research has addressed what can be called specific components of organisational culture, such as security culture [38]. The focus on specific components of organisational culture brings the pragmatic possibility of integrating research on organisational culture and organisational climate.

For instance, a set of shared values, beliefs and assumptions concerning information privacy in an organisation (information privacy culture) can be compared with the shared perceptions and meanings employees attach to the policies, practices and procedures related to information privacy in the organisation (information privacy climate). In theoretical terms, one might expect an alignment between the information privacy culture and the information privacy climate so that positive outcomes regarding information privacy could be accomplished.

D. EXISTING SURVEYS AND SYSTEMATIC REVIEW

In this section, we review the identified survey-based studies that are closely related to the topics of privacy and organisational culture. Moreover, we justify the scope and contributions of the proposed ScR based on a systematic comparison of the existing survey-based studies in Table 1. As follows, we present the existing surveys, discuss their main findings, and highlight their limitations.

The work of [39] performed a comprehensive literature review to identify the variables that influence the cultivation of a security culture in organisations. In summary, they propose five potential variables: (1) information security behaviour; (2) top management support; (3) security education & awareness; (4) information security policy; and (5) information security acceptance. Based on that, the authors propose a conceptual framework for modelling information security culture, highlighting the importance of variables and their inter-relationships, as well as the relationship with other theories, such as Hofstede [44] national culture dimensions and Schein [45] organisational culture levels. Although this work does not explicitly address information privacy, the identified variables are potentially similar. The links to the existing theories on national cultures and organisational culture are also plausible in the context of information privacy. However, since information security and information privacy are not the same, further research is needed to validate such assumptions.

In [40], the authors performed a literature review to identify security and privacy issues in big data systems, aiming to categorise the issues into a classification framework. This study highlights that security and privacy issues fall under three distinct contexts: technological, organisational, and environmental. Although this study focuses on big data systems, the classification framework is likely relevant to other types of applications. However, the authors do not further elaborate on organisational culture *per se*. Instead, they just suggest that it influences the security and privacy issues, e.g., depending on the company's security culture, learning culture, competencies, and management support.

Another similar work is the literature review of [41] that identifies conceptual themes to foster information security policy compliance among employees. Based on 67 studies, the authors propose four overarching themes for information systems security [41]: (1) implementing different philosophies of countermeasures (i.e., deterrence and development); (2) applying procedural countermeasures; (3) applying technical countermeasures; and, (4) enhancing environmental countermeasures. Here we see some similarities to the work of [40], which also emphasises the technological, organisational and environmental contexts. This work, however, does not address key concepts such as information privacy and organisational culture in their paper and limits the scope to information security.

The work of [42] explores the organisational culture of healthcare institutions with regards to information security. This literature review organises the topic in four main components of information security programs: (1) technical controls; (2) management process controls, e.g., policies and sanctions designed to change user behaviour; (3) training programs; and (4) governance programs. The author argues that healthcare organisations should focus and improve practices on such fronts to protect personal health data and support continued operations of critical business functions. This work also borrows from Deal and Kennedy [46] definitions for the key characteristics of corporate cultures, such as shared values, heroes in the organisations, rituals and ceremonies, and cultural social networks. However, this research mainly focuses on information security, indirectly addressing privacy.

The work of [43] is the only *systematic* review identified that focuses on the attempts of organisations to maintain privacy and security while undertaking digital transformation. This work also stresses that the perceptions of multiple stakeholders will impact the adoption of new technologies and how privacy and security are maintained. Apart from purely technical measures, the authors emphasise that organisational culture, organisational structure, HR practices, privacy and security policies, and senior leaders' commitment and IT leadership are essential for maintaining privacy and security that support digital transformation [43]. Even though the authors in this study account for privacy and security as complementary concepts, the authors only mention the aspect of organisational culture as a key component without further exploring it.

The main topic of this ScR (i.e., OPCC), remains largely unaddressed by the existing surveys and systematic reviews. Most studies focus on information security culture [39], [41], [42]. Although these studies' findings are relevant to this ScR, it is critical to differentiate between information security and information privacy (as explained in Section II-A). An "information security culture" can contribute to creating a privacy culture inside organisations, but only in a complementary manner. Similarly, any instruments for measuring information security culture and climate also need to be re-considered and re-validated to include privacy

TABLE 1. Summary of existing surveys and systematic review.

Ref.	Year	SLR	Title	Limitations
[39]	2015	No	An identification of variables influencing the establishment of information security culture	**(i)** Focus on identifying variables that influence cultivating a Security Culture. **(ii)** It does not address Privacy, specifically.
[40]	2016	No	Technological, Organisational and Environmental Security and Privacy Issues of Big Data: A Literature Review	**(i)** Focus on Big Data. **(ii)** It does not address directly Organisational Culture but points to it as an influential factor.
[41]	2017	No	Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory	**(i)** Focus on security policy compliance for information systems. **(ii)** It does not address Privacy nor Organisational Culture.
[42]	2017	No	Exploring Organizational Culture for Information Security in Healthcare Organizations: A Literature Review	**(i)** Focus on Organisational Culture for information security in healthcare organisations. **(ii)** It does not address Privacy, specifically.
[43]	2020	Yes	Privacy and Security in the Digitalisation Era	**(i)** It does not directly address Organisational Culture but points to it as an essential component.
This ScR		Yes	**Main Topic:** Organisational Privacy Culture and Climate	**(i)** Focus on Information Privacy rather than information security, observing the fundamental differences between concepts. **(ii)** It does not explicitly address Security Culture, although we take into consideration the potential overlaps.

factors. Besides, existing research that addresses privacy is rather specific in scope (i.e., focus on digital transformation [43], or big data [40]), and they only indirectly point to the importance of organisational culture for maintaining privacy. Overall, the topic of OPCC remains poorly demarcated despite its presumed strong influence in the privacy practices of the software industry [11], [13].

III. METHODOLOGY

This paper performs a Scoping Review (ScR), which is a review methodology that can be used to map key concepts underpinning a research area, clarify working definitions, and understand the conceptual boundaries of a topic [14]. According to [47], the most common reasons for conducting an ScR are to explore the breadth or extent of the literature, to map and summarise the evidence, and inform future research. These reasons also provided the basis for us to employ the ScR methodology on the OPCC topic, given its emerging characteristics as a research area. As mentioned, this research follows the methodology proposed in the PRISMA, considering the extension for Scoping Reviews (PRISMA-ScR) [15]. For the ScR protocol, specifically, we also followed the PRISMA-P checklist [48] to ensure the completeness and transparency of the review process. Figure 1 presents an overview of this study's methodology, further described in the following subsections.

A. PHASE I - PLANNING THE SCR

As shown in Figure 1, Phase I of the ScR consists of first identifying the need for such a study and looking for existing reviews that may have already covered the topic. Once the need for the ScR is justified, the second step pertains to defining the Research Questions that will guide the entire study. Based on the research questions, the ScR Protocol is formulated by specifying all the methodology for the ScR. The ScR Protocol must also be piloted and refined by the research team before conducting the study. These three steps of Phase I are detailed as follows.

1) IDENTIFYING THE NEED FOR THE REVIEW

Before starting this ScR, the authors searched for existing reviews on the topic. A few databases (i.e., Google Scholar, Scopus, IEEE Xplore, ACM Digital Library and Web of Science) were searched using the keywords: `review`, `organi*ational culture`, `organi*ational climate`, and `privacy`. This preliminary search reassured us that there were no existing systematic reviews on the topic in the searched databases. None of the retrieved literature (in. Section II-D, Table 1) was related to the outlined research questions in Section III-A2, motivating the need for this ScR.

2) RESEARCH QUESTIONS

This ScR aims to explore the extent of the literature topic, map and summarise the evidence, and provide a framework to position new research activities appropriately. To this end, we defined three specific Research Questions (RQs):

- RQ1.1: *What is the nature of the evidence on OPCC?* **Objective:** To understand the types of published research (e.g., journal or conference papers), types of research designs (e.g., quantitative or qualitative), types of contributions (e.g., models, guidelines), prominent authors, and publications venues.
- RQ1.2: *What is known about the concept of OPCC?* **Objective:** To identify the existing definitions and conceptualisations (or the lack thereof) on the topic in the published research.
- RQ1.3: *What is the state of existing primary research studies on OPCC?* **Objective:** To further examine and critically appraise existing primary research, and identify the studies (or the lack thereof) that have proposed valid and reliable models for measuring OPCC.

3) WRITING THE SCR PROTOCOL

As a last step of the planning phase, a detailed version of the ScR protocol was written, and then discussed, piloted and refined by the authors prior to conducting the review. This ScR protocol describes in detail all the phases and steps of the

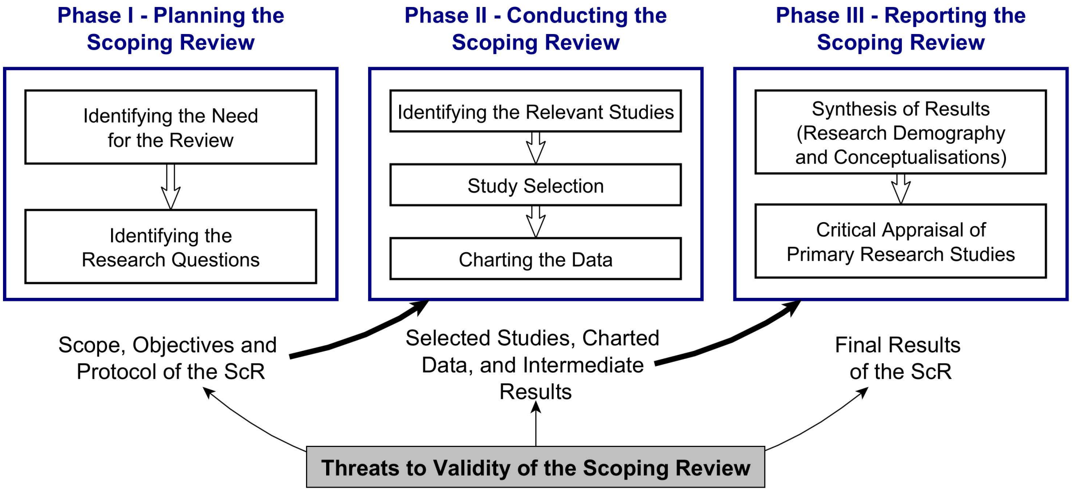
Phase I - Planning the Scoping Review
Identifying the Need for the Review
Identifying the Research Questions
Phase II - Conducting the Scoping Review
Identifying the Relevant Studies
Study Selection
Charting the Data
Phase III - Reporting the Scoping Review
Synthesis of Results (Research Demography and Conceptualisations)
Critical Appraisal of Primary Research Studies
Scope, Objectives and Protocol of the ScR
Selected Studies, Charted Data, and Intermediate Results
Final Results of the ScR
Threats to Validity of the Scoping Review

FIGURE 1. **Overview of the Scoping Review methodology.**

methodology, as shown in Figure 1. The ScR protocol [49] and replication package were made available in an online repository [50]. Hence, the full details are not provided in this paper.

B. PHASE II - CONDUCTING THE SCR

Once the ScR Protocol was finalised, the research team started the study *per se*. It is noteworthy, however, that if there were a need to change any aspects of the planning, the team would continually discuss and update the ScR protocol accordingly. As shown in Figure 1, the first step in Phase II refers to the systematic search of pre-specified databases. The eligibility criteria based on the RQs were also defined in the ScR Protocol. The second step, the selection of studies, is performed by the research team using these selection criteria to analyse all the studies retrieved from the various databases. The third step refers to the systematic extraction of data from the studies, taking place during the reviewers' full reading of the selected studies. All steps of Phase II are further explained as follows.

1) INFORMATION SOURCES AND SEARCH PROCESS

We searched four bibliographic and full-text databases: Scopus, Web of Science, IEEE Xplore, and ACM Digital Library. The databases Scopus and Web Science were chosen for their sizes and broad range of journals in multiple fields. Adding to that, we also chose the databases IEEE Xplore and ACM Digital Library for their relevancy in the areas of computer science and engineering. All databases were searched on the 16/Sep/2021 without setting any other restrictions (e.g., year limits, publication types, etc.). A structured search strategy was used based on keywords that reflect the RQs of this ScR, which included the terms: organisational culture, organisational climate, organisational values, and privacy. Hence, the following general search string was structured:

```
((``organi*ational culture'' OR
``organi*ational climate'' OR
``organi*ational values'') AND privacy)
```

We also performed backward snowballing searches (screening references cited in included studies) and forward snowballing searches (exploring studies that cite included studies using Google Scholar). In addition, we searched for relevant grey literature (e.g., unpublished works, reports, website information, journal articles) using the OpenGrey System for Information on Grey Literature in Europe. These searches using OpenGrey were done on 20/Oct/2021.

2) ELIGIBILITY CRITERIA

The selection of studies included in the review followed the general inclusion criteria of publications relating to both, (1) organisational culture, climate or values, in connection with (2) privacy and data protection. By organisations, the most diverse contexts and environments can be considered (e.g., companies, government agencies, non-profit organisations, etc.). The term privacy relates to "privacy of information" and "data protection" when organisations collect and process personal data of individuals (for example, system users, employees, civilians, etc.). Besides, various types of publications were considered, e.g., primary research papers, literature reviews, opinion papers, experience papers, and etc.

This review also established the following exclusion criteria: a) studies that focus on "organisational culture, climate or values" only for "information security"; b) studies that only address the key terms in isolation; c) studies published in foreign languages which the authors are not fluent (i.e., other than English, Spanish, Portuguese, German). We acknowledge that many publications addressed the topic of "Information Security Culture" in the context of Organisational Culture. In this study, however, we focus on Privacy rather than Security since the former has broader and independent dimensions (as discussed in Section II-A). We also disregarded papers that only propose security or privacy theories, methods, tools or techniques, without addressing ''organisational culture, climate, or values''; papers on people's or users' privacy that do not address ''organisational privacy''; and, papers that address privacy culture in populations (e.g., a country's culture) without addressing ''organisational culture, climate or values''.

3) SELECTION OF STUDIES

The search results were exported from each database and imported into RAYYAN software (www.rayyan.ai), which is a collaborative web-tool for systematic reviews that supports researchers in the screening process. RAYYAN automatically aggregates all the search results and flags duplicated entries facilitating their removal by the reviewers. The study selection phase was carried out by two independent reviewers (R1, R2). Before starting the selection, a calibration exercise was performed by the reviewers to ensure a common understanding and minimise any doubts on the eligibility criteria, defined in Section III-B2.

The selection of studies was systematised in two steps: Step 1) reading of titles and abstracts; and, Step 2) full reading of the studies. In Step 1, the reviewers used separate RAYYAN accounts to analyse the entire list of retrieved studies independently. Based on the eligibility criteria, the reviewers decided whether to ''exclude'' a study from the review or ''include'' it for further analysis in Step 2. In case of disagreements between R1 and R2, the third reviewer (R3) was called to establish the final decision. In Step 2, another round of full-text readings resulted in the set of studies initially included in the review. After downloading the full-texts, reviewers R1 and R2 read all papers to verify if they were within the scope of the review, i.e., following the eligibility criteria. If any reviewer deemed the study to be outside the scope, the study was then further discussed by the group together with R3 for a final decision.

4) DATA EXTRACTION AND DATA CHARTING PROCESSES

The researchers first created a template form for the data extraction and charting process (available in the replication package [50]). The template form was then tested and discussed by the group with a couple of the studies. This pre-test enabled the resolution of conflicts between the reviewers' approaches for data extraction. Then, the relevant data were extracted from each publication by R1 and inserted in separate files. This data extraction step later facilitated the data charting process. This process of reading, extracting and charting data was carried out in an iterative fashion in which researchers were able to continually critique, agree and update the data extraction template form as needed. Finally, to ensure accuracy, only direct quotes were extracted from the studies. When needed, notes were added to justify the study's classifications made in the form. Various data items were extracted in this process, e.g., bibliographic metadata, publication type, contribution type, publication venues, main definitions, summary of results, etc.

For the data items 2) types of research and 3) types of contribution, we created a classification scheme based on existing prior work. To classify the ''types of research'' we combined categories proposed by Wieringa *et al.* [51] and Crewell and Creswell [52]. The work of Wieringa *et al.* [51] proposes six types of research that are relevant to the software engineering area (i.e., validation research, evaluation research, solution proposal, philosophical papers, opinion papers, experience papers). In addition, the work of Creswell and Creswell [52] helps us to better classify *Primary Research* according to their quantitative, qualitative, and mixed methods research designs (e.g., survey, experimental, grounded theory, ethnography, case studies). We also added a new research type for Literature Reviews (secondary research), since the classification in [51] accounts only for primary studies. Lastly, to classify the types of contribution, we used the classification proposed by Shaw [53] with the categories: model, theory, framework, guideline, lessons learned, advice, and tool.

C. PHASE III - REPORTING THE SCR

As shown in Figure 1, Phase III comprised the main steps that constituted the final report of findings. Starting with the synthesis of results, this step combines all the data collected from the studies into a coherent narrative, accompanied by the various tables, charts, and classifications. Based on the synthesis, we also identified the need to critically appraise primary research identified in this ScR, consisting of an additional step in the reporting phase. Lastly, we report the results and discuss the main findings as described in the remainder of this paper. These steps are detailed in the following subsections.

1) SYNTHESIS OF RESULTS

The data charting process was designed to provide two sets of structured data used to summarise the research results: quantitative data (e.g., year of publication, publications per author, citations) and qualitative data (e.g., type of publication, type of research, type of contribution). The synthesis of results was performed by R1 via spreadsheet and text software (Excel, Word), generating tables and figures, interpreting findings, and providing a descriptive mapping of the body of knowledge. Based on all the data, a whole coherent narrative was written by the research team, i.e, conveying all the results, our interpretation of the main findings, and the identification of research gaps.

2) CRITICAL APPRAISAL OF PRIMARY RESEARCH

All the studies classified as Primary Research were also further inspected by the reviewers. Two critical appraisal tools provided by the Center for Evidence-Based Management (CEBMa) were used to assess the methodological quality of the primary research studies: 1) *Checklist for Qualitative Studies* [54]; and, 2) the *Checklist for Cross-Sectional Studies (Surveys)* [55]. The evaluation process included a first calibration round and was subsequently conducted independently by R1 and R2. In case of a disagreement, R1 and R2 re-read and discussed the study to reach a consensus.

3) REPORTING RESULTS

As per Figure 1, this last phase of *Reporting the Scoping Review* is detailed in the following Section IV. The results are reported in line with the RQs (in Section III-A2), providing summaries and findings. That is, the *Synthesis of the Results* is presented in Sections IV-A and IV-B covering findings in terms of research demography and existing conceptualisations. Also, the *Critical Appraisal of Primary Research* is provided in Section IV-C further examining the methodological quality of primary research studies. As part of the reporting, threats to validity are reviewed in Section VI, describing the main limitations of this research.

IV. RESULTS

Figure 2 provides an overview of the selection process for this scoping review. Initially, 610 studies were identified through the search process, with 605 coming from the scientific databases and five PhD theses from OpenGrey. These five theses were screened by the authors and excluded as they did not meet the selection criteria. All the other entries from the scientific databases were imported into the Rayyan software. The Rayyan system also automatically generates a list of duplicated entries. The reviewers then examined this list and removed the duplications manually. A double-blind screening process using Rayyan resulted in the identification of 33 relevant studies. However, six studies were not accessible through the researchers' institutional libraries. In such cases, the corresponding authors were contacted, but we did not receive any answers. After the screening process, 20 papers were selected for this review. Using Google Scholar, we checked for all the papers that cited the selected studies (i.e., forward snowballing). This process revealed another nine studies that the authors deemed relevant. While reading the full texts, we further identified seven relevant studies mentioned and referenced by other studies (i.e., backward snowballing). In the end, a total of 36 studies were included in the scoping review (see the list in Appendix VII).

A. THE NATURE OF EVIDENCE ON OPCC

In this section, we answer RQ1.1 that focuses on the nature of evidence of studies on OPCC. This part of the analysis is based on the data charting step, in which we classify the studies under multiple demographic aspects. For example, the frequency of publications, the types of research and contributions, prominent authors, countries, and publication venues.

1) FREQUENCY AND TYPES OF PUBLISHED RESEARCH

Figure 3 shows the frequency of research published in the topic. More than 66% ($n = 24$) of the studies were published in the past seven years (i.e., 2015-2021). The authors interpret this trend as a growing academic interest in the intersection of ''Organisational Culture and Climate'' and ''Information Privacy''. This trend also follows the several privacy laws enacted in the past years, such as the EU GDPR, US CCPA, Brazilian LGPD, China's PIPL. However, the total number of research published remains small (i.e., only 36 studies), suggesting that OPCC as a research area is still in its embryonic stage.

The studies were also categorised according to their research type, using the classification schemes proposed by Wieringa *et al.* [51] and Creswell and Creswell [52]. Figure 4 shows the number of studies under each category. For instance, the studies [56] and [10] fall into multiple categories. These studies sketch a new way of looking at existing things by structuring the field in form of a taxonomy or conceptual framework (i.e., Philosophical Papers) and, more specifically, they propose new predictive models (i.e., Solution Proposal). Furthermore, they evaluate the models through surveys with real subjects (i.e., Primary Research, Evaluation Research) to validate the model and confirm or reject the studies' hypotheses. Notice that all the studies in the category Primary Research are further categorised using Creswell and Creswell [52] classification for research designs (e.g., qualitative, quantitative, mixed methods) in Section IV-C.

As shown in Figure 4, there is a higher prevalence of Philosophical Papers in the area. Various authors attempt to conceptualise and structure components in-between areas of Organisational Culture and Climate and Information Privacy. These studies are also mainly focused on Primary Research, e.g., qualitative and quantitative research that includes surveys, focus groups, questionnaires, and interviews. The topic of OPCC draws heavily from social sciences, such as industrial and organisational psychology. On the other hand, Information Privacy is strongly linked to the areas of law and computer science.

The studies were also categorised in terms of their contribution types, using the classification proposed by Shaw [53], as shown in Figure 5. Models related to various aspects of organisational culture and privacy perceptions are relatively common. For instance, the works of [57] and [58] offer two distinct types of models. In [57], the authors propose a multilevel model of information privacy concerns, illustrating that privacy concerns ought to be analysed at multiple levels (i.e., individuals, groups, organisations, government, society). In contrast, the work of [58] offers a predictive model to understand the drivers and impediments of ethical system development concerning privacy and security engineering. Similar to models, theoretical frameworks were also prevalent as a way of describing themes or structuring components. In such cases, we maintained the authors' nomenclature as ''framework'' for their contributions. For instance, some studies performed qualitative coding to describe interviews and focus groups data through thematic categories [59] or conceptual frameworks [60]. The authors interpreted such contributions as thematic frameworks. Also, some authors proposed conceptual frameworks, such as the conceptual

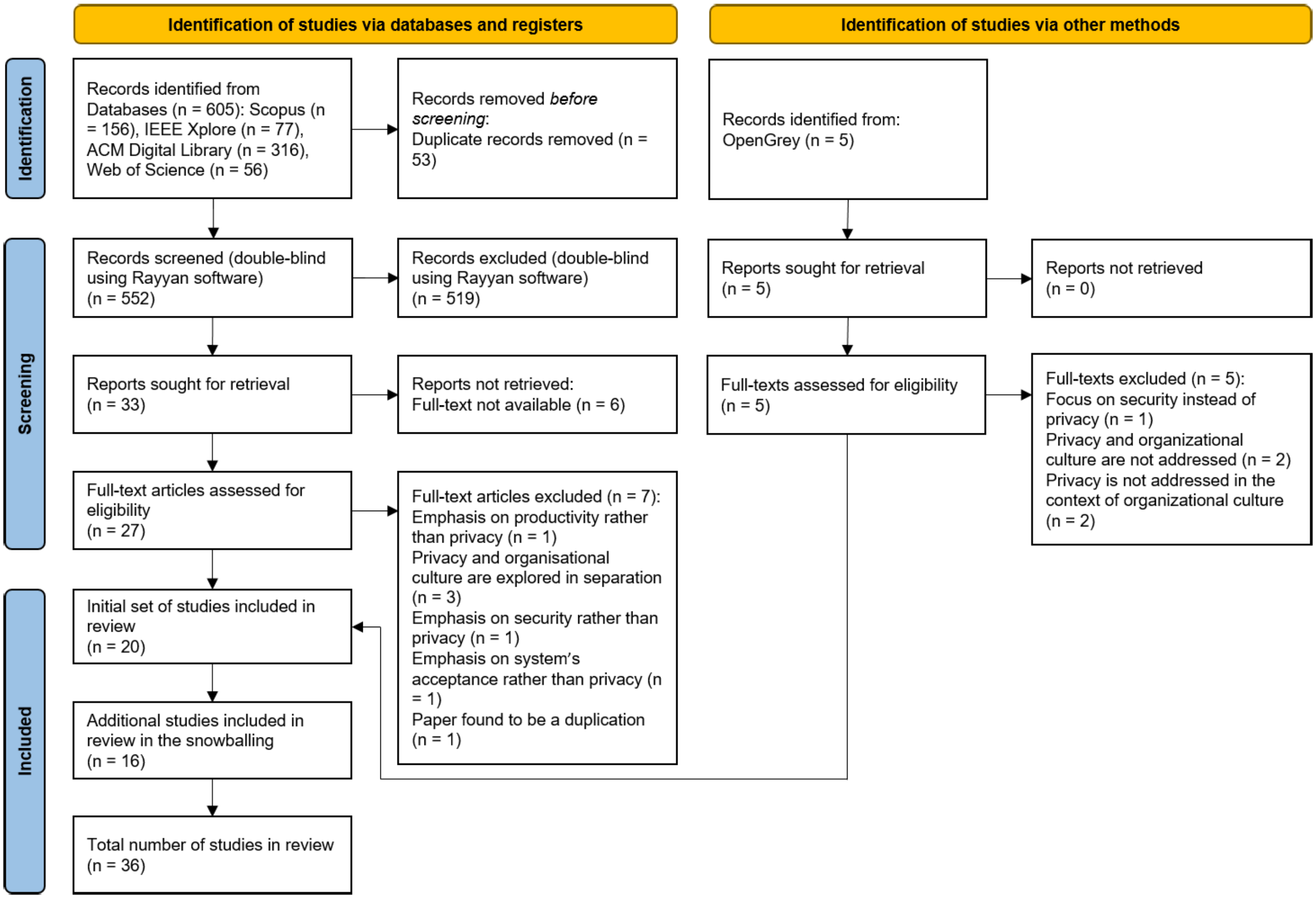
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Screening
Included
Records identified from Databases (n = 605): Scopus (n = 156), IEEE Xplore (n = 77), ACM Digital Library (n = 316), Web of Science (n = 56)
Records removed before screening: Duplicate records removed (n = 53)
Records identified from: OpenGrey (n = 5)
Records screened (double-blind using Rayyan software) (n = 552)
Records excluded (double-blind using Rayyan software) (n = 519)
Reports sought for retrieval (n = 5)
Reports not retrieved (n = 0)
Reports sought for retrieval (n = 33)
Reports not retrieved: Full-text not available (n = 6)
Full-texts assessed for eligibility (n = 5)
Full-texts excluded (n = 5): Focus on security instead of privacy (n = 1) Privacy and organizational culture are not addressed (n = 2) Privacy is not addressed in the context of organizational culture (n = 2)
Full-text articles assessed for eligibility (n = 27)
Full-text articles excluded (n = 7): Emphasis on productivity rather than privacy (n = 1) Privacy and organisational culture are explored in separation (n = 3) Emphasis on security rather than privacy (n = 1) Emphasis on system's acceptance rather than privacy (n = 1) Paper found to be a duplication (n = 1)
Initial set of studies included in review (n = 20)
Additional studies included in review in the snowballing (n = 16)
Total number of studies in review (n = 36)

FIGURE 2. PRISMA 2020 flow diagram for this Scoping Review.

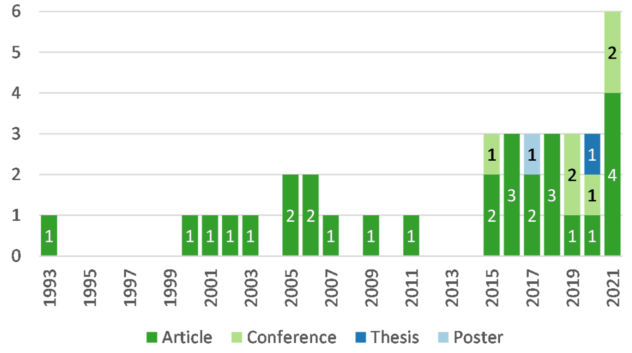

FIGURE 3. Papers published per year.

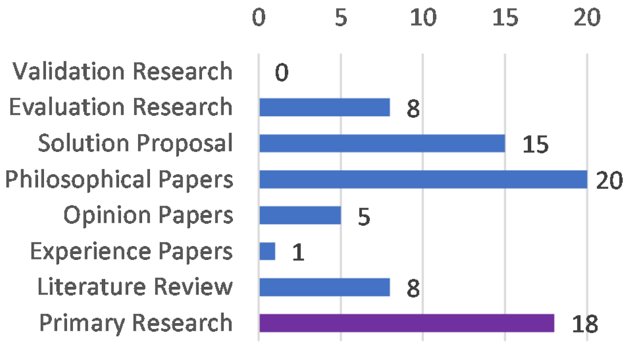

FIGURE 4. Research types in the area (classification sources: [51], [52]).

privacy governance framework in [61] and the conceptual framework on employee's electronic performance monitoring in [62]. Besides, many authors also proposed guidelines as a list of recommendations, e.g., for organisations [63] and researchers [57].

Current contributions associated to OPCC are primarily theoretical. In fact, there is only one Tool created in the area, which is the Da Veiga and Martins Information Protection Culture Assessment (IPCA) questionnaire. The proposed instrument can be used to assess the information privacy culture, and has been validated on a global financial institution. The authors highlighted that to further enhance the IPCA's content validity an "information protection culture framework" still needs to be defined. They also mentioned that a second validity and reliability assessment will be carried out to finalise the IPCA questionnaire.

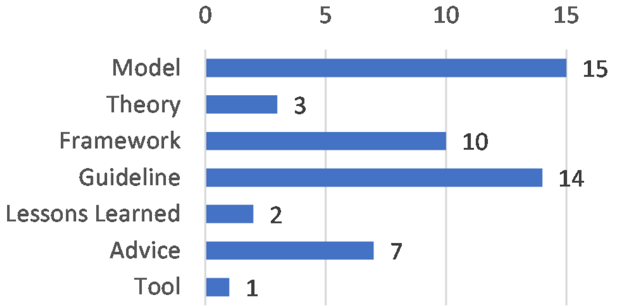

FIGURE 5. Types of contributions in the area (classification source: [51]).

2) AUTHORS, COUNTRIES AND AFFILIATIONS

Figure 6 shows the distribution of studies per country. Authors from the United States still dominate the published research. In total, there are 83 individual authors, but most authors ($n = 68$, 82%) published a single study. As shown in Table 2, there are 15 (18%) authors that published two or three studies and are involved in 14 studies (39%). These authors also influence Table 3 of affiliations in which nine academic institutions (from a total of 43) are featured in 16 (44%) studies. Our findings suggest that the academics from the USA, Israel, South Africa, India and Taiwan are leading the research efforts regarding OPCC. However, the scientific community is still small, and most studies come from individual authors and affiliations.

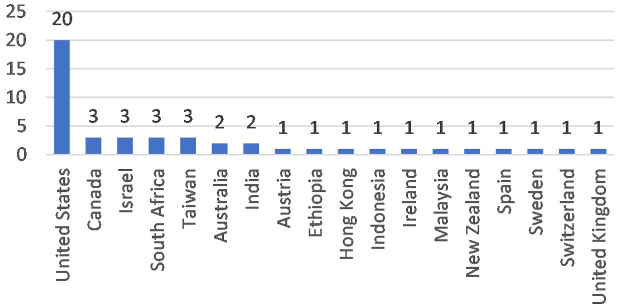

FIGURE 6. Publications per country.

TABLE 2. Authors with most publications.

Author	Ref.	Author	Ref.
A. Da Veiga (3)	[10], [61], [64]	A. Frik (2)	[13], [65]
I. Hadar (3)	[11], [12], [66]	A.Y. Liu (2)	[67], [68]
N. Martins (3)	[10], [61], [64]	S.K. Mathew (2)	[69], [70]
B.J. Alge (2)	[56], [71]	S. Sherman (2)	[11], [12]
V.S.P. Attili (2)	[69], [70]	V. Sugumaran (2)	[69], [70]
O. Ayalon (2)	[11], [66]	P. Swartz (2)	[61], [64]
M. Birnhack (2)	[11], [66]	E. Toch (2)	[11], [66]
S.E. Chang (2)	[67], [68]	-	-

3) PUBLICATION VENUES

Published research is sparsely distributed across 32 distinct journal and conference venues. Only three journals appear with two studies each, namely: Empirical Software Engineering, Journal of the Association for Information Systems, and Management Information Systems Quarterly. Nonetheless, we can sort the publication venues according to their broad research areas. Table 4 shows the six concentration areas, i.e., (1) Computer Science & Information Systems, (2) Management & Organisation, (3) Security & Privacy, (4) Healthcare, (5) Law, and (6) Psychology. For example, the journal Management Information Systems Quarterly would fall into the concentration areas (1) and (2). Most research is concentrated in computer science and information systems venues, with a significant decrease in other areas, such as management and organisational sciences.

TABLE 3. Institutions with most publications.

Institutions	Ref.
University of California, USA (3)	[13], [59], [65]
University of Haifa, Israel (3)	[11], [12], [66]
University of South Africa, South Africa (3)	[10], [61], [64]
Indian Institute of Technology Madras, India (2)	[69], [70]
National Chung Hsing University, Taiwan (2)	[67], [68]
Oakland University, USA (2)	[69], [70]
Purdue University, USA (2)	[56], [71]
Tel Aviv University, Israel (2)	[11], [66]
Virginia Tech, USA (2)	[57], [59]

TABLE 4. Main areas of the venues (i.e., journals and conferences).

Main areas	#	References
Computer Science & Information Systems	26	[72], [73], [74], [67], [68], [40], [75], [66], [11], [61], [58], [43], [13], [76], [70], [57], [77], [12], [65], [64], [78], [63], [10], [69], [79], [80]
Management & Organisation	8	[81], [67], [71], [57], [59], [62], [78], [63]
Security & Privacy	4	[73], [65], [64], [10]
Healthcare	3	[72], [82], [83]
Law	3	[84], [10], [85]
Psychology	2	[83], [56]

4) INDUSTRY SECTORS

Figure 7 shows that most studies did not focus on any specific industry sectors or research context. Examples are studies of [11]–[13], [58] that surveyed and/or interviewed software developers from a broad range on companies. However, some studies were focused on specific industrial contexts, such as the works of [64] and [10] with banks and other financial services, or the works of [72], [73], [82] in healthcare institutions. Only two studies addressed multiple industry sectors, i.e., the work of [75] covering healthcare, consumer, and financial services; and, the work of [79] based on health insurance, credit card, and banking institutions.

5) LAWS AND REGULATIONS

Figure 8 shows the most commonly mentioned privacy-related laws and regulations. The EU GDPR appears in almost a third of the studies, leading the rank of privacy regulations. Other well-know regulations such as the US HIPAA

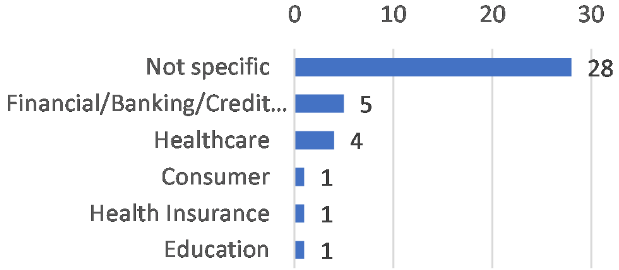

FIGURE 7. Most common industry sectors targeted by the studies.

and the US FIPPs are also mentioned by many studies. There was a total of 30 other regulations that were mentioned by just two or fewer studies, e.g., the EU Directive 95/46/EC (which was replaced by the GDPR in 2018), US Children's Online Privacy Protection Act, and AU Privacy Act.

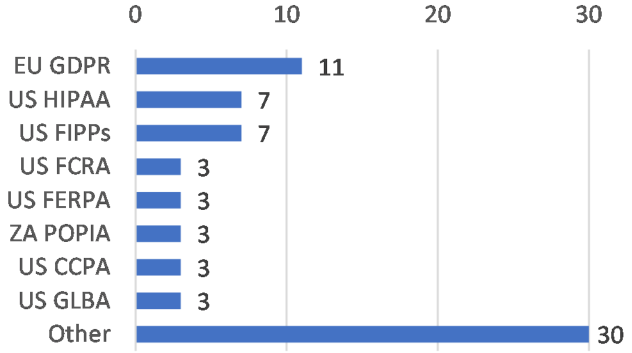

FIGURE 8. Laws and regulations most mentioned by the studies. Acronyms: General Data Protection Regulation (EU GDPR); Health Insurance Portability and Accountability Act (US HIPAA); Fair Information Privacy Principles (US FIPPs); Fair Credit Reporting Act (US FCRA); Family Educational Rights and Privacy Act (US FERPA); Protection of Personal Information Act (ZA POPIA); California Consumer Privacy Act (US CCPA); Gramm-Leach-Bliley Act (US GLBA).

B. THE CONCEPTUALISATION OF OPCC

In this section, we answer RQ1.2 concerning the conceptualisations of OPCC. As shown in Table 5, there are currently two explicit definitions for the terms of Information Protection Culture [10] and Organisational Privacy Climate [11]. Most studies mention other terms, such as "privacy climate" or "privacy culture", but lack precise definitions. The definitions proposed by Da Veiga and Martins [10] and Hadar *et al.* [11] are not commonly used by other researchers. Just the work of Arizon-Peretz *et al.* [12] uses the definition Hadar's definition for Organisational Privacy Climate. However, such conceptualisations did not happen in a vacuum. Most of the identified studies are neighbouring the central topic of OPCC. Given that, we propose that the studies can be separated into two main groups:

- **Adjacent Research** that identifies gaps, motivates or influences the topic of OPCC, even though this was not the main focus of the study; and,
- **Core Research** that explicitly tackles the concept of OPCC, proposing definitions, methods, and constructs in the area.

TABLE 5. Existing definitions on OPCC.

Ref.	Information Protection Culture
[10]	*"[...]* ***"information protection culture"*** *is defined by the researchers as, "a culture in which the protection of information and upholding of privacy are part of the way things are done in an organisation. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behaviour."* (p. 249)
Ref.	**Organisational Privacy Climate**
[11]	*"[...] we can refer to* ***organizational privacy climate*** *as a shared perception of the way behavior with regard to privacy is rewarded, supported and expected."* (p. 271)

1) ADJACENT RESEARCH

Table 6 shows a summary of five recurring topics presented in the adjacent research. This table is not meant to summarise the content of all studies but only to capture common themes linked to OPCC. Notice that this table of common topics contains studies classified in various research types (e.g., primary research, philosophical papers, opinion papers). In addition, even though some studies mention or discuss these topics, it does not mean that sufficient research and evidence was gathered to support them.

TABLE 6. Common topics from adjacent research.

Topics	#	References
(I) The significant influence of Organisational Culture and Climate on Information Privacy and the employee's perceptions, attitudes and behaviours	22	[13], [40], [43], [56], [58]–[60], [62], [65]–[70], [74]–[79], [81], [85]
(II) The role of leaders, seniors, and top management in the Organisational Privacy Culture and Climate	11	[40], [43], [60], [61], [63]–[65], [70], [79], [82], [84]
(III) Employees' monitoring and invasion of privacy - organisational culture may influence what employees deem to be fair and acceptable	11	[56], [59], [60], [62], [67], [68], [71], [74], [77], [78], [81]
(IV) Proposes creating and fostering a Culture of Privacy, Confidentiality, Privacy-by-Design in organisations	8	[13], [60], [61], [63], [64], [76], [82], [84]
(V) Recommends the topic of Organisational Privacy Culture and Climate as future research	4	[57], [60], [77], [80]

Most authors mentioned that organisational culture and climate strongly influence employees' perceptions, attitudes, and behaviours with regard to information privacy. For instance, organisational culture has an influence on privacy-related activities at the organisation [70], and employee's perception of information privacy [68]. Some studies also found that there are corporate climates that inhibit discussions of privacy concerns [79], as well as climates that can be hostile to nonfunctional requirements (e.g., privacy and security), making engineers ignore or do not feel responsible for implementing privacy [58]. Conversely, the employee's privacy attitudes and behaviours can also positively influence the organisational privacy climate, as discussed in the work of [13], on Privacy Champions in development teams.

Another factor mentioned by many authors refers to the role that leaders, senior employees and top management play in supporting the OPCC. Senior management is a crucial factor to mediate the implementation of privacy-related policies and procedures in an organisation [70]. Many authors refer to it as leadership commitment for privacy governance [61], organisation-wide, and top management support [40], or the leader's willingness to champion organisational awareness for privacy and adoption of best practices [43].

About a third of the studies focus on employees' privacy and its relation with the organisation's culture. For instance, some studies focus on Electronic Performance Monitoring (EPM) and how the organisational culture plays a role in the employees' acceptability, sense of fairness, perceived invasion of privacy, and reactions to such monitoring systems [62], [78], [81]. This interplay of organisational culture and privacy was also investigated in the context of employee's use of social media [60], and the organisational policies for Bring Your Own Device (BYOD) [74], [77].

Finally, various studies have proposed creating, fostering and improving a culture of privacy [13], [60], [61], [63], [64], a culture of confidentiality [82], a Privacy-by-Design culture [84], or embedding ethics (and privacy) in the organisation's culture [76]. Other studies have also suggested the intersection of Organisational Culture and Information Privacy as a future research area [57], [60], [77], [80]. In conclusion, although the adjacent studies motivate and suggest new research fronts, they only briefly approach central topics of OPCC without fully articulating the concepts.

2) CORE RESEARCH

Only five studies were found to be at the core of the OPCC research in this scoping review. In Table 7, we listed the studies and summarised the main reasons for classifying them as core research. As follows, we briefly discuss their main contributions and their impact on the conceptualisation of OPCC as an emerging theory.

In the first studies, proposed by [83] and [73], the authors share their experience and advice on how to change the organisational culture and develop a culture of privacy. Gibbons' (2003) [83] proposes a method of changing the culture of the Clinical Pastoral Education (CPE) to adapt to new privacy laws in Australia. In this work, the author proposes three major phases that the institution needs to go through (i.e., preliminary actions, transformations of structures and traditions, and implementing supportive structures of education). He also offers a series of recommendations for the CPE Centers to ensure compliance with Australian National Privacy principles, i.e., collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder data flows, sensitive information.

TABLE 7. Core research.

Reference	Summary
G.D. Gibbons (2003) [83]	**(I)** Proposes a "Method of Changing the Culture" to comply with new privacy laws in the context of the Clinical Pastoral Education.
E.M. Power (2007) [73]	**(I)** Describes a case study on how to develop a "Culture of Privacy" in the context of the Smart Systems for Health Agency.
A. Da Veiga and N. Martins (2015) [10]	**(I)** Defines Information Protection Culture. **(II)** Proposes the Information Protection Culture Assessment (IPCA) questionnaire.
I. Hadar *et. al.* (2018) [11]	**(I)** Defines Organisational Privacy Climate. **(II)** Discusses the influence of organisational privacy climate in the developers' practices of privacy.
R. Arizon-Peretz *et. al.* (2021) [12]	**(I)** Proposes the use of organisational climate theory to understand the developers' perceptions and behaviors and the underlying forces affecting them. **(II)** Identifies constructs that compose organisational privacy and security climates.

Similarly, the work of [73] shares experience acquired by the Smart Systems for Health Agency (SSHA, Ontario) in attempting to develop a culture of privacy. As a starting point, the author proposes that to build a culture of privacy an organisation must: (1) clearly articulate privacy as an organisational priority; (2) communicate key privacy and security messages; (3) educate across the organisation; (4) raise awareness of the importance of registering privacy incidents and breaches; (5) build privacy into the fabric of the organisation's activities; and, (6) make privacy information and guidance readily accessible. The author also stresses the importance of starting from the top (i.e., board of directors), creating a privacy awareness campaign, conducting training, and evaluating employees and contractors understandings.

These works from [83] and [73] represent individual efforts from institutions in changing and building a culture of privacy. However, these studies do not adequately address the concepts of Organisational Culture and Climate.

The first definition in the area, as shown in Table 5, appears only many years later in the work of [10]. In this paper, Da Veiga and Martins [10] define Information Protection Culture based on their previous research on Information Security Culture of organisations. Notice that the authors use the term ''information protection'' to refer to ''information privacy''. Apart from a definition for Information Protection Culture, the authors also proposed creating a Information Protection Culture Assessment (IPCA) instrument to assess/measure the information protection culture of organisations. This new construct is based on an existing Information Security Culture Assessment (ISCA) instrument [86], [87]. Although some of the privacy attributes added to the ISCA instrument have been found valid and reliable, this study only motivates the creation of an IPCA instrument. To create a final IPCA instrument, the authors mentioned that other privacy attributes ought to be determined and tested for the validity and reliability of the constructs. We consider that the proposed term Information

Protection Culture is equivalent to Organisational Privacy Culture, i.e., a hybrid of organisational culture and information privacy concepts.

The second definition, now for Organisational Privacy Climate (see Table 5) comes from the work of Hadar *et al.*. This study gives insights into the software architects' mindsets through a series of in-depth interviews about information privacy, privacy engineering, organisational and technical privacy strategies. Based on a grounded theory methodology, authors defined Organisational Privacy Climate was one of the main categories in their theoretical model. Therefore, Organisational Privacy Climate is considered a central force, referring to the influence of the environment on developers' cognitive factors and behaviour related to privacy. The study also articulates about positive and negative privacy climates in the organisation (e.g., (+) having clear guidelines, (-) low sense of responsibility). The authors also point to a misalignment between the organisations' privacy policies and the actual privacy climate among employees. For instance, there is little to no concern for privacy when designing and developing systems despite normative privacy policies, or there are mismatches between the norms and employees' moral values.

Based on Hadar's study [11], the work of Arizon-Peretz *et al.* [12] proposes using organisational climate theory for attaining a better understanding of developers' privacy perceptions and behaviours and the underlying forces. Another research aim is to discover the constructs that compose organisational privacy and security climates. A similar process of in-depth interviews and grounded theory was used in this study. Their findings reveal that software developers receive inconsistent and confusing cues conveyed by management and other parties in their work environment. Privacy is seen as a low priority, leading to perceptions and behaviours that would not comply with existing regulations. As a result, this study provides part of the groundwork for developing climate measures to quantify organisational privacy and security climates.

It is worth mentioning that the work of Da Veiga and Martins [10] and the ones of Hadar *et al.* and Arizon-Peretz *et al.* [12] seem to emerge in isolation. The studies nonetheless propose new definitions for Information Protection Culture and Organisational Privacy Climate, complementing each other. However, it is worth emphasising that organisational culture and organisational climate are different concepts and should not be used interchangeably.

All in all, core publications approach the topic and provide contributions in rather distinct ways. Whilst Gibbons [83] and Power [73] are the first identified proponents for creating an organisational privacy culture, their work is based on their personal experiences. On the other hand, the works of Da Veiga and Martins [10], Hadar *et al.* [11] and Arizon-Peretz *et al.* are supported by evidence-based quantitative and qualitative research.

Core publications also share some common ingredients that guide research on OPCC. First, they start from a series of privacy principles that have been embedded in guidelines and regulations and that organisations should embrace. Some clear examples are:

- The ten Australian national privacy principles mentioned in [83], i.e., data collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, trans-border data flows, sensitive information;
- The Organisation for Economic Co-operation and Development (OECD) guidelines mentioned in [10], i.e., collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability; and,
- The Fair Information Practice Principles (FIPPs) mentioned in [11], [12], i.e., notice, consent, data minimisation, purpose specification, confidentiality, data security, access, rectification.

Second, core publications also rely on established theories in organisational culture and climate. The work of Da Veiga and Martins [10] adopts the definitions of organisational culture proposed by Schein [88] as *"a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration – that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems"*. The works of Hadar *et al.* [11] and Arizon-Peretz *et al.* [12] are based on the aforementioned definition of organisational climate proposed by Schneider *et al.* [23] (i.e., see Section II-C). Nonetheless, the works of [11] and [12] also borrow from other organisational climate theorists, specially on safety climate, such as in [89]–[92].

A significant distinction among core publications pertains to acknowledging privacy-by-design and privacy engineering, such as the privacy- and security-by-design definitions from [93], and engineering ideas of privacy-by-architecture and privacy-by-policy from [94]. These system engineering approaches for dealing with privacy concerns appear only in the works of Hadar *et al.* [11] and Arizon-Peretz *et al.* [12]. This is likely due to the studies' focus on software engineers' perceptions and behaviours on privacy in the industry. Such qualitative research on privacy could be considered for other departments in organisations, e.g., to understand how marketing, finances, or human resources deals with privacy concerns and the influence of organisational culture and climate.

C. THE STATE OF EXISTING PRIMARY RESEARCH

In this section, we answer RQ 1.3, focusing on the existing primary research that has been published on the topic. Primary research accounted for half of the studies, as previously shown in Figure 4. These 18 studies were further classified using the sub-categories of primary research proposed by Creswell and Creswell [52]. Two authors also critically appraised all studies using the checklists for qualitative studies and cross-sectional studies (surveys) from the Center for Evidence-Based Management (CEBMa). Results are presented on Tables 8 and 9 summarising the main aspects of the quality of the studies' methodological process and credibility of the evidence.

1) TYPES OF PRIMARY RESEARCH

As shown in Figure 9, nine studies used quantitative surveys for collecting data from employees in multiple organisations. For instance, the work of Alge *et al.* [56] that presents two survey studies to support their proposed predictive model in which information privacy predicts psychological empowerment, which in turn predicts discretionary behaviours on the job, including creative performance and organisational citizenship behaviour. Another example is the work of Chang *et al.* [67] that evaluates the privacy boundaries and explores employees' reactions in employee monitoring based on their proposed research model. The other nine studies used various qualitative research approaches, collecting data through interviews and open-ended questionnaires. An example is the work of Smith [79] with findings based on 105 semi-structured interviews with executives and managers in seven organisations that handled sensitive personal data. The only exception is the study of Spiekermann *et al.* [58] that uses (primarily) a quantitative survey methodology but also provides a broader qualitative background based on six interviews. This study was classified as Survey (quantitative) and Other (qualitative), but it was appraised only for its quantitative survey because the qualitative data analysis was not explained in the paper.

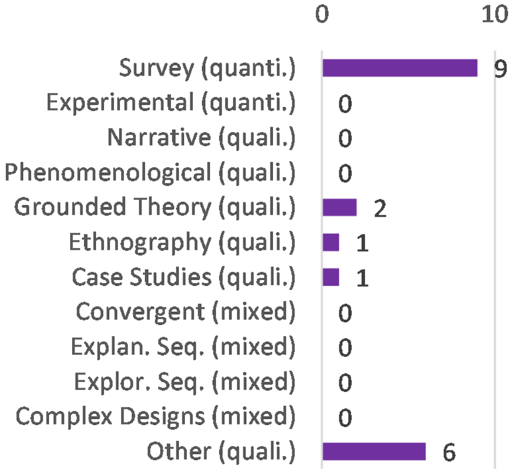

FIGURE 9. **Sub-types of primary research (classification source: [52]).**

2) CRITICAL APPRAISAL OF QUALITATIVE STUDIES

As shown in Table 8, the critical appraisal of the qualitative studies reveals that most of them have clearly established research questions and used appropriate research methodologies. All the studies have also clearly explained the context of the research and the data collection processes. Some typical issues prevalent in most studies refer to the reliability of the qualitative coding process and the generation of categories or themes based on the collected data. Only a few studies discuss reliability measures (e.g., inter-coder reliability) in the qualitative coding process during the data analysis [12], [13], [59], [69]. Thus, most studies lack sufficient methodological appropriateness to ensure reliable and reproducible findings. Also, these studies usually investigate the employee's perceptions, making the interview transcripts confidential, preventing other researchers from inspecting them. Overall, the qualitative studies still offer credible results and justified conclusions. These results and conclusions cannot be generalised to other organisational contexts, but this is often the case for most qualitative research.

Qualitative studies offer deeper insights into individuals' perceptions, attitudes and behaviours concerning information privacy within real organisational contexts. These studies, in turn, support the research community to formulate better theories and hypotheses that can be investigated through quantitative research. Currently, most identified studies have addressed the topic of OPCC adjacently, and only two studies investigated it more explicitly. Due to the small number of studies, it is reasonable to expect that more qualitative research is still needed on the topic to corroborate findings and make new inquiries on the field. For instance, both the core qualitative studies of [11] and [12] come from interrelated research groups in Israeli universities. Each study is based on semi-structured interviews of 27 participants each, and the participants' cultural backgrounds are not explicitly described. The studies also focused on software engineers, but further studies could also investigate the privacy perspectives of employees in other departments in the organisations. Besides, other types of qualitative research strategies are advisable, such as ethnography, relying on collecting organisational documentation, internal policies, and field observations, so that researchers are not based only on interviews and individual perceptions.

3) CRITICAL APPRAISAL OF QUANTITATIVE STUDIES

Based on the critical appraisal in Table 9, we consider that the methodological appropriateness of the quantitative studies still lacks sufficient rigour. On a positive note, all studies have clearly stated research questions and used appropriate methodologies for carrying out the studies. The selection of participants was also clearly described in all studies. Most studies present valid and reliable models with statistical significance assessed. However, the vast majority of the studies still rely on convenience sampling without estimating appropriate sample sizes, which also affects the statistical power. Most studies also do not present confidence intervals in their data analysis and do not account for (or not even mention) possible confounding factors. The results of the existing quantitative studies are still not generalisable, deterring their application in other organisational contexts. Nonetheless, the work of Da Veiga and Martins [10] clearly stands out in terms of methodological rigour, setting a high bar for future studies. However, similar to the qualitative studies, their study was conducted within a global financial institution, so that further studies in other industry sectors are needed.

TABLE 8. Qualitative research – critical appraisal using the checklist for qualitative studies from the CEBMa [54] (Answer: Yes, No, Can't tell).

Author, year and reference	Group	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
I. Hadar *et. al.* (2018) [11]	Core	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No
M. Tahaei *et. al.* (2021) [13]	Adjacent	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
J.C. Ibáñez and M.V. Olmeda (2021) [76]	Adjacent	No	No	Yes	Yes	No	No	No	Yes	No	No
S.A. Smith and S.R. Brunner (2017) [59]	Adjacent	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
J. Henry (2020) [60]	Adjacent	Yes	No	Yes	Yes	No	No	No	Yes	Yes	No
R. Arizon-Peretz *et. al.* (2021) [12]	Core	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
V.S.P. Attili *et. al.* (2018) [69]	Adjacent	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
H.J. Smith (1993) [79]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No
A.E. Waldman (2018) [85]	Adjacent	No	No	No	No	No	No	No	No	Yes	No

CEBMa Checklist Questions - **Q1.** Did the study address a clearly focused question/issue? **Q2.** Is the research method (study design) appropriate for answering the research question? **Q3.** Was the context clearly described? **Q4.** How was the fieldwork undertaken? Was it described in detail? Are the methods for collecting data clearly described? **Q5.** Could the evidence (fieldwork notes, interview transcripts, recordings, documentary analysis, etc.) be inspected independently by others? **Q6.** Are the procedures for data analysis reliable and theoretically justified? Are quality control measures used? **Q7.** Was the analysis repeated by more than one researcher to ensure reliability? **Q8.** Are the results credible, and if so, are they relevant for practice? **Q9.** Are the conclusions drawn justified by the results? **Q10.** Are the findings of the study transferable to other settings?

TABLE 9. Quantitative research – critical appraisal using the checklist for cross-sectional studies (surveys) from the CEBMa [55] (Answer: Yes, No, Can't tell).

Author, year and reference	Group	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
B.J. Alge *et. al.* (2006) [56]	Adjacent	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No
S.E. Chang *et. al.* (2015) [67]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No
S.E. Chang and A.Y. Liu (2016) [68]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No
O. Ayalon *et. al.* (2017) [66]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes	No
S. Spiekermann *et. al.* (2019) [58]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No
V.S.P. Attili *et. al.* (2021) [70]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No
K. Degirmenci *et. al.* (2019) [77]	Adjacent	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	No
P. Swartz *et. al.* (2021) [64]	Adjacent	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
A. Da Veiga and N. Martins (2015) [10]	Core	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No

CEBMa Checklist Questions - **Q1.** Did the study address a clearly focused question/issue? **Q2.** Is the research method (study design) appropriate for answering the research question? **Q3.** Is the method of selection of the subjects (employees, teams, divisions, organizations) clearly described? **Q4.** Could the way the sample was obtained introduce (selection)bias? **Q5.** Was the sample of subjects representative with regard to the population to which the findings will be referred? **Q6.** Was the sample size based on pre-study considerations of statistical power? **Q7.** Was a satisfactory response rate achieved? **Q8.** Are the measurements (questionnaires) likely to be valid and reliable? **Q9.** Was the statistical significance assessed? **Q10.** Are confidence intervals given for the main results? **Q11.** Could there be confounding factors that haven't been accounted for? **Q12.** Can the results be applied to your organization?

The current evidence on OPCC remains incipient. Considering the six levels of appropriateness from the Center for Evidence-Based Management [95] (see Table 10), the nature of the evidence that comes from cross-sectional studies (surveys) is often limited, ranked at a D level. Nonetheless, existing quantitative studies are pointing to new directions on OPCC. More cross-sectional studies are still needed in the area, perhaps leading to more robust controlled studies in the future. Also, due to the small number of studies, comprehensive systematic reviews with meta-analysis are not possible. In summary, to gather solid evidence on the topic, there is still a need for more studies in general as well as more sophisticated levels of research design.

TABLE 10. CEBMa's six levels of appropriateness [95].

Research Design	Level
(a) Systematic review or meta-analysis of randomized controlled studies	AA
(b) Systematic review or meta-analysis of non-randomized controlled and/or before-after studies	A
(c) Randomized controlled study	A
(d) Systematic review or meta-analysis of controlled studies without a pretest or uncontrolled study with a pretest	B
(e) Non-randomized controlled before-after study	B
(f) Interrupted time series	B
(g) Systematic review or meta-analysis of cross-sectional studies	C
(h) Controlled study without a pretest or uncontrolled study with a pretest	C
(i) Cross-sectional study (survey)	D
(j) Case studies, case reports, traditional literature reviews, theoretical papers	E

V. DISCUSSION

This ScR shows that there is a significant number of studies composing the literature on the topic of OPCC. The research area has grown significantly since 2015, with researchers in the USA leading with respect to publication numbers. Studies are mostly not specific in terms of context or industry sectors, but the most commonly mentioned privacy regulations have been the EU GDPR, US HIPAA and US FIPPs. Based on this ScR, we can interpret that the topic of OPCC has still a small core of published research, yet a significant number of adjacent research supports it. However, the topic lacks established definitions, and its conceptual boundaries are not demarcated. Overall, a lack of theoretical and primary research correlates to the lack of valid and reliable instruments for assessing and measuring privacy factors in organisational contexts.

Nevertheless, such findings inform various fruitful pathways for future interdisciplinary research.

Based on our main findings, we composed a graphical summary on the topic of OPCC as shown in Figure 10. First, at the top, potential *research gaps* are identified, suggesting some pathways for future work. Second, *core research* studies are highlighted, evidencing the limited number of primary research, practical constructs, and instruments. Third, the *adjacent research* is acknowledged, providing insights on recurring themes that support and motivate the topic. Lastly, *main supporting areas* are emphasised, underlining the inherent multifaceted nature of the research topic.

In the following subsections, we begin by discussing the research gaps identified by the research team based on the ScR findings, in Section V-A. Next, we discuss the study's implications and propose potential venues for future work towards building an evidence-based OPCC research area, in Section V-B.

A. RESEARCH GAPS

As shown in Figure 10, we argue that the topic still lacks significant research on two fronts: (1) *theory building*, meaning that the theory of OPCC has to be further substantiated, given the lack of fully articulated constructs, limited definitions, and supporting primary research; and, (2) *instruments evaluation*, implying that once evidence-based theories are built, novel instruments can be proposed and evaluated for measuring/assessing different aspects of OPCC. These research gaps are decomposed and further elaborated as follows.

1) OPCC AS AN EMERGING THEORY

As shown in Section IV-A1, the topic is in its embryonic stage in terms of theory, with only 36 studies identified by the authors, of which 24 (66.7%) were published after the year 2015. In addition, most of the studies were considered as adjacent research that motivates the topic but is not aimed at the developing its core ideas and components. Currently, only five of the identified studies were categorised as core research that explicitly focus on investigating and conceptualising organisational privacy culture and/or climate.

However, the core research publications still lack fully articulated definitions. That is, currently we have two independently formulated definitions, one for ''information protection culture'' [10] and another for ''organisational privacy climate'' [11]. These definitions could be jointly articulated in order to differentiate aspects of a privacy culture and privacy climate more clearly. Besides, we also believe that this topic can be significantly influenced by the existing research on Information Security Culture, as already suggested by [10]. Nevertheless, the fundamental differences between security and privacy have to be carefully considered when articulating constructs.

2) UNCLEAR LINKS WITH ESTABLISHED THEORIES

There are also still open questions concerning how information privacy in organisations relates to established theories in national and organisational cultures, such as the ones introduced in Section II-C. Earlier research has analysed and discussed the impact of Hofstede's cultural dimensions on the privacy attitudes of individuals in different national cultures. For instance, the work of [96] revealed that individuals from countries ranking high in Hofstede's uncertainty avoidance dimension specifically emphasise the need to avoid privacy-related risks associated with online disclosures. The work of [97] also shows that uncertainty avoidance correlated with a stronger interest in transparency and control over personal data. Although these studies do not address organisational culture and climate *per se*, we perceive that national cultures will significantly influence the OPCC. Nonetheless, this link between the dimensions of national cultures and information privacy still needs further investigation.

There are also established theories on organisational culture that could be leveraged on the OPCC topic. For example, Schein [30] three levels of culture, i.e., (1) artefacts, (2) espoused beliefs and values, and (3) basic underlying assumptions. Also, Hofstede [98] six dimensions of organisational cultures, i.e., (1) process-oriented vs. results-oriented, (2) employee-oriented vs. job-oriented, (3) parochial vs. professional, (4) open system vs. closed system, (5) loose vs. tight control, and (6) normative vs. pragmatic. Currently, the work of Da Veiga and Martins [10] only bases their definition of ''information protection culture'' on Schein's definition of culture [88]. The work of Hadar *et al.* [11] also bases their definition of ''organisational privacy climate'' on Schneider's *et al.* definition of organisational climate [23]. However, it is still not clear how these new constructs in the topic relate in regards to the three levels of culture [23] or six dimensions of organisational culture [98].

3) OVERALL LACK OF PRIMARY RESEARCH

Another gap refers to the overall lack of primary research on the topic's core ideas. Only two qualitative studies [11], [12] and one quantitative study [10] were identified. Although these studies provide significant original contributions to the topic, important limitations should be considered. The interview studies from Hadar *et al.* [11] and Arizon-Peretz *et al.* [12] are limited to software engineers' self-reported perceptions and privacy practices. Even though the software engineers may have a direct impact on how information systems are designed and deployed, many other departments also deal with privacy concerns on a daily basis (e.g., HR and marketing). Also, leaders and top managers may not be directly connected to the software engineering teams, but still strongly influence how things are done in the organisation. Apart from that, we found only one quantitative study conducted by Da Veiga and Martins [10] that is also limited to participants in a global financial institution.

Moreover, in terms of the research populations, the two qualitative studies of [11] and [12] are not clear about the participants' demography – most likely from Israel, North America and Europe. Thus, it is also worth stressing concerns on misrepresentations due to an over-reliance on Western

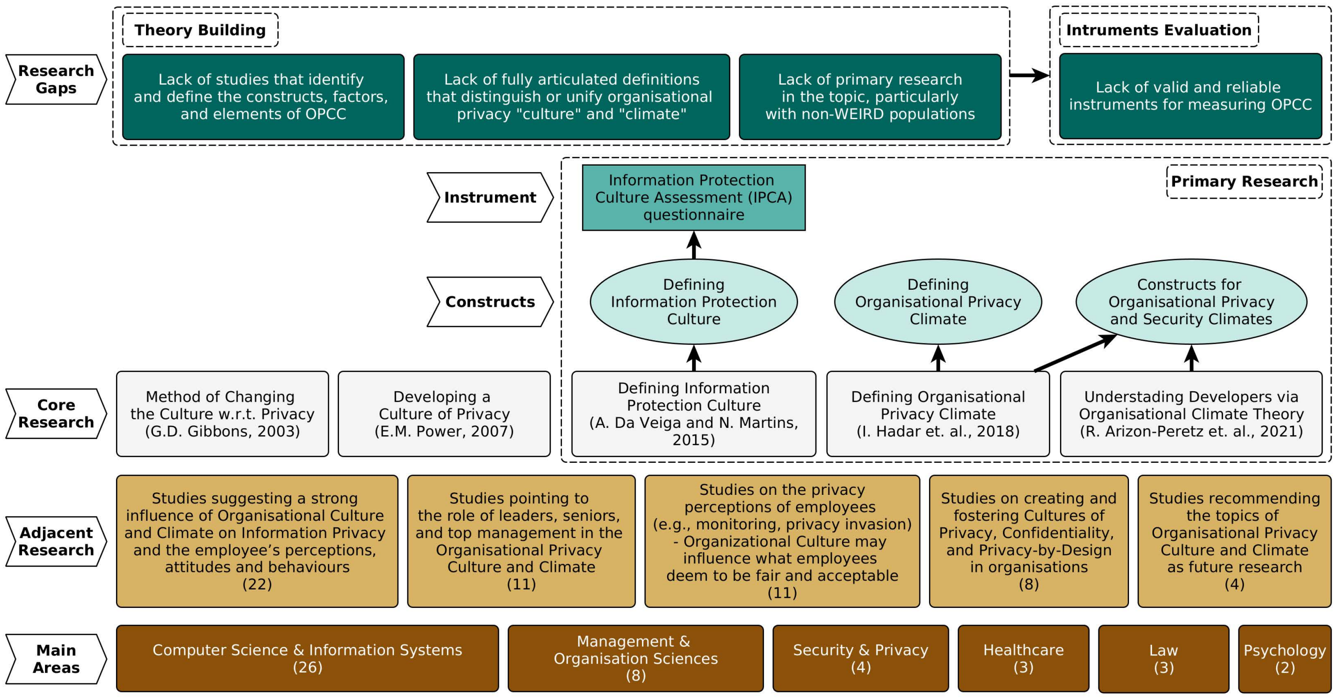
Theory Building
Intruments Evaluation
Research Gaps
Lack of studies that identify and define the constructs, factors, and elements of OPCC
Lack of fully articulated definitions that distinguish or unify organisational privacy "culture" and "climate"
Lack of primary research in the topic, particularly with non-WEIRD populations
Lack of valid and reliable instruments for measuring OPCC
Instrument
Information Protection Culture Assessment (IPCA) questionnaire
Primary Research
Constructs
Defining Information Protection Culture
Defining Organisational Privacy Climate
Constructs for Organisational Privacy and Security Climates
Core Research
Method of Changing the Culture w.r.t. Privacy (G.D. Gibbons, 2003)
Developing a Culture of Privacy (E.M. Power, 2007)
Defining Information Protection Culture (A. Da Veiga and N. Martins, 2015)
Defining Organisational Privacy Climate (I. Hadar et. al., 2018)
Understading Developers via Organisational Climate Theory (R. Arizon-Peretz et. al., 2021)
Adjacent Research
Studies suggesting a strong influence of Organisational Culture and Climate on Information Privacy and the employee's perceptions, attitudes and behaviours (22)
Studies pointing to the role of leaders, seniors, and top management in the Organisational Privacy Culture and Climate (11)
Studies on the privacy perceptions of employees (e.g., monitoring, privacy invasion) - Organizational Culture may influence what employees deem to be fair and acceptable (11)
Studies on creating and fostering Cultures of Privacy, Confidentiality, and Privacy-by-Design in organisations (8)
Studies recommending the topics of Organisational Privacy Culture and Climate as future research (4)
Main Areas
Computer Science & Information Systems (26)
Management & Organisation Sciences (8)
Security & Privacy (4)
Healthcare (3)
Law (3)
Psychology (2)

FIGURE 10. Graphical summary of the area of Organisational Privacy Culture and Climate (OPCC) based on the ScR studies.

Educated Industrialized Rich Democratic (WEIRD) populations. In terms of primary research, we believe that existing studies still need to be replicated and also adapted to investigate different industry contexts, professional roles, countries and nationalities.

4) LACK OF INSTRUMENTS

Another research gap refers to the lack of instruments for measuring OPCC, corresponding to the overall lack of primary research in the area. We identified only one study that proposes a novel instrument for assessing privacy culture, the Information Protection Culture Assessment (IPCA) questionnaire, proposed in [10]. However, this instrument has not been fully developed and evaluated, as mentioned in IV-B2. Apart from completing this instrument, further research is needed to ensure its validity and reliability.

B. IMPLICATIONS AND TOWARDS AN EVIDENCE-BASED OPCC

Looking back at the overarching research question, *What is "this thing" called Organisational Privacy Culture and Climate?* It is fair to say that this question cannot be answered yet with enough depth, precision and sophistication based on the available evidence. OPCC is an emerging topic that comes from the need of organisations to keep pace with a set of privacy values of today's societies, as enshrined in various privacy laws and regulations throughout the world. This pressure for compliance, as well as the raised awareness among practitioners, impacts the practices, values and underlying assumptions of organisations. However, in order to assess, measure and incorporate privacy in organisations reliably, the topic has to evolve into more rigorously built theories, methods, techniques and methodologies.

This theorisation gap, as evidenced in this ScR, has, in turn, multiple implications for varying organisations (e.g., companies, government agencies, non-profits). However, this is most critical for the organisations in which the data collection and processing are likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1)) [1]. We believe that such organisations have a lot to learn by adequately conducting Data Protection Impact Assessments (DPIAs)(Article 35) [1], also known as Privacy Impact Assessments (PIAs) [99]. PIAs generate cross-departmental interactions within the organisation and proactive engagement of external stakeholders (e.g., customers, 3rd-party service providers). Furthermore, incorporating PIAs as an organisational process shows employees that privacy is valued in the organisation and demonstrates compliance with supervisory authorities. For such reasons, we perceive PIAs as a substantial component of creating a privacy culture.

Several companies today fall into the category of "high risk" for data processing, especially the ones dealing with highly innovative technologies, of which privacy impacts are still not fully understood. Examples are companies that perform systematic and extensive evaluations of personal aspects, such as online social networks that enable comprehensive user profiling and capturing links between people [100]. External attackers can also employ automated social network analysis to gather user interactions from various open groups to create social interaction graphs, i.e., public information harvesting attacks [101].

Companies involved in large-scale processing of sensitive data (e.g., health, biometric, genetic religious, political, or financial data) are also likely to result in high privacy risks. For instance, companies that rely on advanced technology in machine learning, artificial intelligence, and deep learning. Many companies are pushing the legal and ethical boundaries in order to collect more data, create better models, and make better predictions, and then share this information with government agencies and private actors [102], which in itself can be a privacy violation of information disclosure. Companies also have to account for privacy attacks against such models trained on sensitive information, such as membership inference attacks [103]. Another example is companies that perform systematic monitoring of publicly accessible areas, which are the cases of autonomous vehicles [104], smart cities and IoT-enabled solutions [105], that may directly or indirectly monitor individuals, their location, and behavioural patterns.

Strengthening aspects of OPCC in organisations working with cutting-edge technology would be particularly important for the responsible development of new software solutions. In such cases, starting with PIAs would be highly recommended, if not mandatory depending on the organisation's jurisdiction. However, when it comes to assessing and measuring OPCC in the companies, practitioners (e.g., leaders, managers, and privacy officers) should still approach the topic carefully, given the current lack of scientific evidence.

Apart from the implications to organisations, this ScR also suggests different pathways for future research in academia. One aspect that has been under-investigated is the influence of national cultures on organisations and the effects on how privacy is handled. For instance, large IT companies are often composed of multi-cultural and diverse teams sometimes deployed worldwide. Privacy perceptions, attitudes, and behaviours in such companies might differ significantly from culturally homogeneous organisations. Besides the underlying national cultures, the company's size and sector may also play a role in how privacy is handled inside the organisation. For example, large enterprises are more likely to have more sophisticated processes in place to deal with privacy concerns (e.g., dedicated teams and departments), while smaller companies may lack such resources. Some sectors are also more sensitive and heavily regulated, e.g., healthcare and financial services, so companies may already have a long tradition of addressing privacy in their activities. More research is needed not only to link the topic to established theories in national and organisational cultures but also to acknowledge the diversity of companies that deal with privacy in their working systems.

In addition, many studies also pointed to the role of leaders in creating and supporting a culture of privacy. As advocated by Barrett [106], organisational transformation begins with the transformation of the leaders. In fact, organisations do not ''transform'', but actually, the people in the organisation do. The values and behaviours of the leaders set the tone and the culture for the whole organisation [106], and this likely applies to the leaders' privacy values as well. More research on the role of leadership in OPCC is still warranted, as well as studies on best privacy strategies and practices to support leaders and top management (e.g., using a privacy governance framework [61], [64]).

Finally, in terms of practical instruments, the IPCA questionnaire proposed by [10] suggests a straightforward avenue for future research on assessing organisational privacy culture. Instruments such as the IPCA need to be further developed, encompassing all privacy principles derived from legal frameworks (e.g., GDPR) and validated across multiple industry sectors in different countries. Nonetheless, quantitative research based on cross-sectional studies and surveys, which is the case for the IPCA questionnaire, still has limited ''strength of evidence'' in terms of scientific appropriateness (see Table 10). However, if the IPCA is further developed and the study is replicated, it would be possible to gather more robust evidence or perform a systematic meta-analysis of multiple studies. Alternatively, more research is also expected on different approaches of research design (e.g., controlled studies) for measuring OPCC.

Interdisciplinary cooperation of different scientific areas, such as computer science, psychology, management and law, will be needed for closing this theorisation gap on the topic of OPCC. Furthermore, OPCC inherently requires close interaction between practitioners in various organisations and academic research communities. We perceive such aspects of interdisciplinary and industry-led research as significantly promising, making the emerging research area of OPCC a fruitful target for collaborative research in the following years.

VI. THREATS TO VALIDITY

A. THREAT I – LIMITATIONS OF THE SCR PLAN

The first threat relates to the planning of the ScR in terms of identifying the need and justification for this study. Considering the existing surveys and systematic reviews (as in Table 1), during the planning phase, we were careful to set the scope of the ScR that does not overlap the existing research contributions. To avoid the risk of an overlapping scope, we executed an initial search to ensure that there were no other secondary studies on a similar topic. The results of the search string (Section III-A1) did not return any relevant secondary study on OPCC. Another important aspect of planning an ScR is to outline the research questions that provide the basis for an objective investigation of the studies that are being reviewed. If the RQs are not explicitly stated or omit the key topics, the scoping review results can be flawed, overlooking the key information. To avoid this threat, we outlined a number of RQs and objectives for each of the RQ (Section III-A2) that aim to find answers about the frequency, types of research, existing conceptualisations, the strength of primary research, and research gaps. In summary, we attempted our best to minimise any bias or limitations

TABLE 11. Complete list of papers included in the scoping review.

Ref.	Title	Year	Included in
[72]	Cognitive models in training health professionals to protect patients' confidential information	2000	Initial Search
[82]	The new HIPAA law on privacy and confidentiality	2002	Initial Search
[83]	Clinical pastoral education and post privacy legislation: an Australian perspective.	2003	Initial Search
[81]	The managerial decision to implement electronic surveillance at work: A research framework	2005	Initial Search
[56]	Information privacy in organizations: Empowering creative and extrarole performance	2006	Initial Search
[73]	Developing a Culture of Privacy: A Case Study	2007	Initial Search
[74]	Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control	2015	Initial Search
[67]	Exploring privacy and trust for employee monitoring	2015	Initial Search
[68]	Information security in practices: Exploring privacy and trust in computer and internet surveillance	2016	Initial Search
[40]	Technological, Organizational and Environmental Security and Privacy Issues of Big Data: A Literature Review	2016	Initial Search
[75]	Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess	2016	Initial Search
[66]	How developers make design decisions about Users' Privacy: The place of professional communities and organizational climate	2017	Initial Search
[84]	Privacy by design: Taking CTRL of big data	2017	Initial Search
[11]	Privacy by designers: software developers privacy mindset	2018	Initial Search
[61]	A conceptual privacy governance framework	2019	Initial Search
[58]	Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers	2019	Initial Search
[43]	Privacy and Security in the Digitalisation Era	2020	Initial Search
[13]	Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges	2021	Initial Search
[76]	Operationalising AI ethics: how are companies bridging the gap between practice and principles? An exploratory study	2021	Initial Search
[70]	Information Privacy Assimilation in IT Organizations	2021	Initial Search
[71]	An Identity-Based Model of Organizational Monitoring: Integrating Information Privacy and Organizational Justice	2006	FW Snowb
[57]	Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems	2011	FW Snowb
[59]	To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace	2017	FW Snowb
[77]	Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection	2019	FW Snowb
[60]	Management Ethics: How Social Media Affects Employees' Privacy and Organizational Climate?	2020	FW Snowb
[62]	EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring	2020	FW Snowb
[12]	Understanding developers' privacy and security mindsets via climate theory	2021	FW Snowb
[65]	WiP: Factors Affecting the Implementation of Privacy and Security Practices in Software Development: a Narrative Review	2021	FW Snowb
[64]	Validating an information privacy governance questionnaire to measure the perception of employees	2021	FW Snowb
[78]	Employee reactions to electronic performance monitoring: A consequence of organizational culture	2001	BW Snowb
[63]	How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches	2009	BW Snowb
[10]	Information security culture and information protection culture: A validated assessment instrument	2015	BW Snowb
[69]	Understanding information privacy assimilation in IT organizations using multi-site case studies	2018	BW Snowb
[79]	Privacy policies and practices: Inside the organizational maze	1993	BW Snowb
[85]	Designing without privacy	2018	BW Snowb
[80]	Theoretical Explanations for Firms' Information Privacy Behaviors	2005	BW Snowb

Initial Search: studies selected from the initial database searches. **FW Snowb** (*forward snowballing*): studies that cited the initially selected papers. **BW Snowb** (*backward snowballing*): studies selected in full-text readings (i.e., in references).

during the planning phase when defining the scope and objectives of this ScR. As a last step in the planning phase, the study protocol was finalised and cross-checked by the team to minimise the limitations of the ScR plan before proceeding to the subsequent phases.

B. THREAT II – CREDIBILITY OF THE LITERATURE SEARCH PROCESS

Another threat relates to the identification and selection of the studies that are reviewed in the ScR. Selecting studies is a critical step as if any relevant papers are missed, the results of the ScR may be flawed. Therefore, we followed a two-step process (Section III-B3), referred to as (i) literature screening and (ii) complete reading of papers. This selection process was carried out by two reviewers independently. We also performed forward and backward snowballing, looking for references to other potentially relevant studies. Also, this ScR restricts the selection of publications to four scientific databases, i.e., Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, and the OpenGrey database for grey literature. Only these databases were used due to their high relevancy to computer science, psychology, and management, as well as to maintain a feasible search space. We also noted that the term "data protection" could have been used in our search string as a similar term to "privacy". This was observed in internal reviews at a stage of the writing of the manuscript. Even though data protection is a narrower term than privacy, we still performed another search using this term, but we did not identify any other studies that were not already included. We therefore decided for not modifying the research protocol at this stage since adding an extra term would not contribute to the research results. Nonetheless, systematic reviews are inherently extendable, and other researchers are encouraged to consider additional databases, terms and search strategies, provided that they have enough resources to do so. Based on our step-wise search process, we are confident that we minimised limitations related to (i) excluding or overlooking relevant studies or (ii) including irrelevant studies that could impact the results and their reporting in the ScR.

C. THREAT III – POTENTIAL BIAS IN SCR REPORTING

The last threat relates to the potential bias in synthesising the data from the review and documenting the results. This means that if there are some limitations in the data synthesis, they directly impact the results of this ScR. Typical examples of such limitations could be a flawed research taxonomy, incorrect identification of research themes (e.g., adjacent and core research) and a mismatch of potential research gaps. To minimise the bias in synthesising and reporting the results, we have created the data extraction form that uses well-known classification schemes, such as the ones proposed by [51] and [52]. Two researchers were involved in synthesising the results, and an independent researcher cross-checked the extracted data and synthesis to ensure consistency. Apart from that, this ScR also offers a complete replication package [50] that conveniently enables other researchers to reproduce or extend this review (described in Section III-A3).

VII. CONCLUSION

Organisational privacy culture and climate (OPCC) is an emerging topic that combines various disciplines such as computer science, information systems, organisational sciences, management, healthcare, law, and psychology. The topic is motivated by the intrinsic need of organisations to adapt and implement privacy practices, which requires the engagement of leaders and employees dealing with working systems that process personal data. However, the understanding of OPCC as a research topic is still incipient, with existing contributions scattered across different fields. In this scoping review, we contribute to synthesising the existing research on OPCC, composing an overall picture of the topic.

As the main conclusion, we argue that the theory on the topic of OPCC still needs to be substantiated to support further development of new and existing instruments. Instruments also need to be rigorously evaluated so that there is strong evidence of their validity and reliability for applying them in practice. Notwithstanding, since the topic is in its embryonic stage, multiple research fronts are possible, which will require interdisciplinary efforts and close cooperation with the industry.

We expect to see future work in the area of OPCC in terms of theory building, i.e., identifying key elements and factors and defining workable constructs. Qualitative and quantitative primary research can be pursued (e.g., field studies, interviews, focus groups, surveys) in order to further define OPCC and articulate it in terms of a theoretical framework. Subsequently, based on the OPCC theory, new instruments can be proposed for measuring and assessing aspects of OPCC in specific organisations. The links between OPCC and other related theories can also be further investigated, such as the influence of the privacy cultures of the broader human societies in which organisations operate. On all fronts, practitioners will play an essential role as facilitators of such future studies by cooperating with researchers and sharing experiences. Ultimately, this increased understanding will support the industry with evidence-based practices for measuring and assessing OPCC. It can also establish strategies for cultivating privacy cultures shared by everyone in the organisation, helping to develop a privacy-conscious workforce and to promote desired privacy behaviours.

APPENDIX A
LIST OF PAPERS IN THE REVIEW

Table 11 provides a summary of all the studies included in the ScR.

REFERENCES

[1] European Commission, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation)," *Off. J. Eur. Union*, vol. 119, pp. 1–88, Apr. 2016.

[2] California State Legislature, "The California consumer privacy act of 2018," *AB, Chau. Privacy, Pers. Inf., Bus.*, Nov. 2018.

[3] E. D. Canedo, A. T. S. Calazans, E. T. S. Masson, P. H. T. Costa, and F. Lima, "Perceptions of ICT practitioners regarding software privacy," *Entropy*, vol. 22, no. 4, p. 429, Apr. 2020.

[4] M. D. Magalhaes, "Data protection regulation: A comparative law approach: Proteção de dados: Estudo comparado de normas nacionais," *Int. J. Digit. Law*, vol. 2, no. 2, pp. 33–53, Aug. 2021.

[5] W. Presthus and K. F. Sønslien, "An analysis of violations and sanctions following the GDPR," *Int. J. Inf. Syst. Project Manage.*, vol. 9, no. 1, pp. 38–53, Sep. 2021.

[6] J. Wolff and N. Atallah, "Early GDPR penalties: Analysis of implementation and fines through May 2020," *J. Inf. Policy*, vol. 11, pp. 63–103, Dec. 2021.

[7] M. N. Lintvedt, "Putting a price on data protection infringement," *Int. Data Privacy Law*, vol. 12, no. 1, pp. 1–15, Mar. 2022.

[8] A. Cavoukian, "Privacy by design in law, policy and practice—A white paper for regulators, decision-makers and policy-makers," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, Tech. Rep., 2011. [Online]. Available: https://gpsbydesigncentre.com/wp-content/uploads/2022/02/312239.pdf

[9] M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 159–166.

[10] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 243–256, Apr. 2015.

[11] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, and A. Balissa, "Privacy by designers: Software developers' privacy mindset," *Empirical Softw. Eng.*, vol. 23, no. 1, pp. 259–289, 2018.

[12] R. Arizon-Peretz, I. Hadar, G. Luria, and S. Sherman, "Understanding developers' privacy and security mindsets via climate theory," *Empirical Softw. Eng.*, vol. 26, no. 6, pp. 1–43, Nov. 2021.

[13] M. Tahaei, A. Frik, and K. Vaniea, "Privacy champions in software teams: Understanding their motivations, strategies, and challenges," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2021, pp. 1–15.

[14] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *Int. J. Social Res. Methodol.*, vol. 8, no. 1, pp. 19–32, Feb. 2005.

[15] A. C. Tricco, E. Lillie, W. Zarin, K. K. O'Brien, H. Colquhoun, D. Levac, D. Moher, M. D. Peters, T. Horsley, L. Weeks, and S. Hempel, "PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation," *Ann. Internal Med.*, vol. 169, no. 7, pp. 467–473, Oct. 2018.

[16] W. C. Barker, "Guideline for identifying an information system as a national security system," Nat. Inst. Standards Technol., Gaithersburg, MA, USA, Tech. Rep. NIST SP 800-59, 2003, doi: 10.6028/NIST.SP.800-59.

[17] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Hum. Rights Law Rev.*, vol. 14, no. 3, pp. 441–458, Sep. 2014.

[18] A. Westin and D. Solove, *Privacy and Freedom*. New York, NY, USA: IG Publishing, 2015.

[19] M. Hansen, "Top 10 mistakes in system design from a privacy perspective and privacy protection goals," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (IFIP Advances in Information and Communication Technology). Berlin, Germany: Springer, 2011, pp. 14–31.

[20] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, "An introduction to privacy engineering and risk management in federal systems," Nat. Inst. Standards Technol., Gaithersburg, MA, USA, Tech. Rep. NISTIR 8062, 2017. [Online]. Available: https://doi.org/10.6028/NIST.IR.8062

[21] S. P. Brown and T. W. Leigh, "A new look at psychological climate and its relationship to job involvement, effort, and performance," *J. Appl. Psychol.*, vol. 81, no. 4, p. 358, 1996.

[22] B. Schneider and A. E. Reichers, "On the etiology of climates," *Personnel Psychol.*, vol. 36, no. 1, pp. 19–39, Mar. 1983.

[23] B. Schneider, M. G. Ehrhart, and W. H. Macey, "Organizational climate and culture," *Annu. Rev. Psychol.*, vol. 64, no. 1, pp. 361–388, Jan. 2013.

[24] T. J. Bacile, "Digital customer service and customer-to-customer interactions: Investigating the effect of online incivility on customer perceived service climate," *J. Service Manage.*, vol. 31, no. 3, pp. 441–464, Jun. 2020.

[25] S. Bhandari and M. R. Hallowell, "Influence of safety climate on risk tolerance and risk-taking behavior: A cross-cultural examination," *Saf. Sci.*, vol. 146, Feb. 2022, Art. no. 105559.

[26] N. S. Vihari, M. Yadav, and T. K. Panda, "Impact of soft TQM practices on employee work role performance: Role of innovative work behaviour and initiative climate," *TQM J.*, vol. 34, no. 1, pp. 160–177, Jan. 2022.

[27] J.-C. Peng and S.-W. Chen, "Learning climate and innovative creative performance: Exploring the multi-level mediating mechanism of team psychological capital and work engagement," *Current Psychol.*, pp. 1–19, Jan. 2022.

[28] K. Dong, R. F. Ali, P. D. D. Dominic, and S. E. A. Ali, "The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses," *Sustainability*, vol. 13, no. 5, p. 2800, Mar. 2021.

[29] L. Smircich, "Concepts of culture and organizational analysis," *Administ. Sci. Quart.*, vol. 28, no. 3, pp. 339–358, 1983.

[30] E. Schein, *Organizational Culture and Leadership* (The Jossey-Bass Business & Management Series). Hoboken, NJ, USA: Wiley, 2010.

[31] G. Hofstede, *Culture's Consequences: International Differences in Work-Related Values* (Cross Cultural Research and Methodology). Newbury Park, CA, USA: Sage, 1980.

[32] G. Hofstede, "Dimensionalizing cultures: The Hofstede model in context," *Online Readings Psychol. Culture*, vol. 2, no. 1, pp. 919–2307, Dec. 2011.

[33] C. A. Hartnell, A. Y. Ou, and A. Kinicki, "Organizational culture and organizational effectiveness: A meta-analytic investigation of the competing values framework's theoretical suppositions," *J. Appl. Psychol.*, vol. 96, no. 4, p. 677, 2011.

[34] B. Erdogan, R. C. Liden, and M. L. Kraimer, "Justice and leader-member exchange: The moderating role of organizational culture," *Acad. Manage. J.*, vol. 49, no. 2, pp. 395–406, Apr. 2006.

[35] F. Shahzad, Z. Iqbal, and M. Gulzar, "Impact of organizational culture on employees job performance: An empirical study of software houses in Pakistan," *J. Bus. Stud. Quart.*, vol. 5, no. 2, p. 56, 2013.

[36] F. Shahzad, G. Xiu, and M. Shahbaz, "Organizational culture and innovation performance in Pakistan's software industry," *Technol. Soc.*, vol. 51, pp. 66–73, Nov. 2017.

[37] I. Colville, K. Dalton, and C. Tomkins, "Developing and understanding cultural change in HM customs and excise: There is more to dancing than knowing the next steps," *Public Admin.*, vol. 71, no. 4, pp. 549–565, Dec. 1993.

[38] D. Asamoah, D. Nuertey, B. Agyei-Owusu, and I. N. Acquah, "Antecedents and outcomes of supply chain security practices: The role of organizational security culture and supply chain disruption occurrence," *Int. J. Quality Rel. Manage.*, vol. 39, no. 4, pp. 1059–1082, Mar. 2022.

[39] E. Sherif, S. Furnell, and N. Clarke, "An identification of variables influencing the establishment of information security culture," in *Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust*. Cham, Switzerland: Springer, 2015, pp. 436–448.

[40] K. A. Salleh and L. Janczewski, "Technological, organizational and environmental security and privacy issues of big data: A literature review," *Proc. Comput. Sci.*, vol. 100, pp. 19–28, Jun. 2016.

[41] P. Balozian and D. Leidner, "Review of IS security policy compliance: Toward the building blocks of an IS security theory," *ACM SIGMIS Database Adv. Inf. Syst.*, vol. 48, no. 3, pp. 11–43, Aug. 2017.

[42] B. B. Page, "Exploring organizational culture for information security in healthcare organizations: A literature review," in *Proc. Portland Int. Conf. Manage. Eng. Technol. (PICMET)*, Jul. 2017, pp. 1–8.

[43] G. M. Jonathan, B. K. Gebremeskel, and S. D. Yalew, "Privacy and security in the digitalisation era," in *Proc. 11th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2020, pp. 0837–0844.

[44] G. Hofstede, "National cultures in four dimensions: A research-based theory of cultural differences among nations," *Int. Stud. Manage. Org.*, vol. 13, nos. 1–2, pp. 46–74, Mar. 1983.

[45] E. H. Schein, *The Corporate Culture Survival Guide*, vol. 158. Hoboken, NJ, USA: Wiley, 2009.

[46] T. Deal and A. Kennedy, *Corporate Cultures: The Rites and Rituals of Corporate Life*. Reading, MA, USA: Addison-Wesley, 1982.

[47] A. C. Tricco, E. Lillie, W. Zarin, K. O'Brien, H. Colquhoun, M. Kastner, D. Levac, C. Ng, J. P. Sharpe, K. Wilson, M. Kenny, R. Warren, C. Wilson, H. T. Stelfox, and S. E. Straus, "A scoping review on the conduct and reporting of scoping reviews," *BMC Med. Res. Methodol.*, vol. 16, no. 1, pp. 1–10, Dec. 2016.

[48] D. Moher, L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, and L. A. Stewart, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement," *Systematic Rev.*, vol. 4, no. 1, pp. 1–9, Dec. 2015.

[49] L. H. Iwaya, G. H. Iwaya, A. V. Steil, and S. Fischer-Hübner. (2022). *Organisational Privacy Culture And Climate: A Scoping Review Protocol*. [Online]. Available: https://github.com/lhiwaya/OPCC-ScR/blob/73f96e12a3e1fd44be94444916fa3533b7ab2a7e/Organizational%20Privacy%20Culture%20and%20Climate%20-%20ScR%20Protocol%20v1.0.pdf

[50] L. H. Iwaya. (2022). *OPCC Scoping Review—Replication Package*. [Online]. Available: https://github.com/lhiwaya/OPCC-ScR

[51] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requir. Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006.

[52] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Newbury Park, CA, USA: Sage, 2017.

[53] M. Shaw, "Writing good software engineering research papers," in *Proc. 25th Int. Conf. Softw. Eng.*, 2003, pp. 726–736.

[54] CEBMa. (2014). *Critical Appraisal Checklist for a Qualitative Study*. [Online]. Available: https://cebma.org/wp-content/uploads/Critical-Appraisal-Questions-for-a -Qualitative-Study-July-2014-1.pdf

[55] CEBMa. (2014). *Critical Appraisal Checklist For Cross-Sectional Study*. [Online]. Available: https://cebma.org/wp-content/uploads/Critical-Appraisal-Questions-for-a -Cross-Sectional-Study-July-2014-1.pdf

[56] B. J. Alge, G. A. Ballinger, S. Tangirala, and J. L. Oakley, "Information privacy in organizations: Empowering creative and extrarole performance," *J. Appl. Psychol.*, vol. 91, no. 1, p. 221, 2006.

[57] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quart.*, vol. 35, no. 4, pp. 1017–1041, 2011.

[58] S. Spiekermann, J. Korunovska, and M. Langheinrich, "Inside the organization: Why privacy and security engineering is a challenge for engineers," *Proc. IEEE*, vol. 107, no. 3, pp. 600–615, Mar. 2019.

[59] S. A. Smith and S. R. Brunner, "To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace," *Manage. Commun. Quart.*, vol. 31, no. 3, pp. 429–446, Aug. 2017.

[60] J. C. Henry, "Management ethics: How social media affects employees' privacy and organizational climate?" Ph.D. dissertation, School Bus., Northcentral Univ., San Diego, CA, USA, 2020.

[61] P. Swartz, A. Da Veiga, and N. Martins, "A conceptual privacy governance framework," in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, Mar. 2019, pp. 1–6.

[62] D. M. Ravid, D. L. Tomczak, J. C. White, and T. S. Behrend, "EPM 20/20: A review, framework, and research agenda for electronic performance monitoring," *J. Manage.*, vol. 46, no. 1, pp. 100–126, Jan. 2020.

[63] M. J. Culnan and C. C. Williams, "How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches," *MIS Quart.*, vo. 33, no. 4, pp. 673–687, 2009.

[64] P. Swartz, A. Da Veiga, and N. Martins, "Validating an information privacy governance questionnaire to measure the perception of employees," *Inf. Comput. Secur.*, vol. 29, no. 5, pp. 761–786, Nov. 2021.

[65] L. Nurgalieva, A. Frik, and G. Doherty, "WiP: Factors affecting the implementation of privacy and security practices in software development: A narrative review," in *Proc. 8th Annu. Hot Topics Sci. Secur. Symp. (HoTSoS)*, 2021, pp. 1–15.

[66] O. Ayalon, E. Toch, I. Hadar, and M. Birnhack, "How developers make design decisions about users' privacy: The place of professional communities and organizational climate," in *Proc. Companion ACM Conf. Comput. Supported Cooperat. Work Social Comput.*, Feb. 2017, pp. 135–138.

[67] S. E. Chang, A. Y. Liu, and S. Lin, "Exploring privacy and trust for employee monitoring," *Ind. Manage. Data Syst.*, vol. 115, no. 1, pp. 88–106, Feb. 2015.

[68] S. E. Chang and A. Y. Liu, "Information security in practices: Exploring privacy and trust in computer and internet surveillance," *Comput. Syst. Sci. Eng.*, vol. 31, no. 2, pp. 147–155, 2016.

[69] V. S. P. Attili, S. K. Mathew, and V. Sugumaran, "Understanding information privacy assimilation in IT organizations using multi-site case studies," *Commun. Assoc. Inf. Syst.*, vol. 42, 2018.

[70] V. S. P. Attili, S. K. Mathew, and V. Sugumaran, "Information privacy assimilation in IT organizations," *Inf. Syst. Frontiers*, pp. 1–17, Jun. 2021.

[71] B. J. Alge, J. Greenberg, and C. T. Brinsfield, "An identity-based model of organizational monitoring: Integrating information privacy and organizational justice," in *Research in Personnel and Human Resources Management*. Bingley, U.K.: Emerald Group, 2006.

[72] V. L. Patel, J. F. Arocha, and E. H. Shortliffe, "Cognitive models in training health professionals to protect patients' confidential information," *Int. J. Med. Informat.*, vol. 60, no. 2, pp. 143–150, Nov. 2000.

[73] E. M. Power, "Developing a culture of privacy: A case study," *IEEE Secur. Privacy Mag.*, vol. 5, no. 6, pp. 58–60, Nov. 2007.

[74] N. Selviandro, G. Wisudiawan, S. Puspitasari, and M. Adrian, "Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control," in *Proc. 3rd Int. Conf. Inf. Commun. Technol. (ICoICT)*, May 2015, pp. 113–118.

[75] J. Wall, P. B. Lowry, and J. B. Barlow, "Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess," *J. Assoc. Inf. Syst.*, vol. 17, no. 1, pp. 39–76, Feb. 2016.

[76] J. C. Ibáñez and M. V. Olmeda, "Operationalising AI ethics: How are companies bridging the gap between practice and principles? An exploratory study," *AI Soc.*, pp. 1–25, Aug. 2021.

[77] K. Degirmenci, J. Shim, M. Breitner, F. Nolte, and J. Passlick, "Future of flexible work in the digital age: Bring your own device challenges of privacy protection," in *Proc. 40th Int. Conf. Inf. Syst. (ICIS)*. Atlanta, GA, USA: Association for Information Systems, 2019, pp. 1–17.

[78] G. S. Alder, "Employee reactions to electronic performance monitoring: A consequence of organizational culture," *J. High Technol. Manage. Res.*, vol. 12, no. 2, pp. 323–342, Sep. 2001.

[79] H. J. Smith, "Privacy policies and practices: Inside the organizational maze," *Commun. ACM*, vol. 36, no. 12, pp. 104–122, Dec. 1993.

[80] K. Greenaway and Y. Chan, "Theoretical explanations for firms' information privacy behaviors," *J. Assoc. Inf. Syst.*, vol. 6, no. 6, pp. 171–198, Jun. 2005.

[81] J. V. Chen and W. H. Ross, "The managerial decision to implement electronic surveillance at work: A research framework," *Int. J. Org. Anal.*, vol. 13, no. 3, pp. 244–268, Mar. 2005.

[82] S. D. Calloway and L. M. Venegas, "The new HIPAA law on privacy and confidentiality," *Nursing Admin. Quart.*, vol. 26, no. 4, pp. 40–54, 2002.

[83] G. D. Gibbons, "Clinical pastoral education and post privacy legislation: An Australian perspective," *J. Pastoral Care Counseling, Advancing Theory Prof. Pract. Through Scholarly Reflective Publications*, vol. 57, no. 3, pp. 319–328, Sep. 2003.

[84] E. Everson, "Privacy by design: Taking CTRL of big data," *Cleveland State Law Rev.*, vol. 65, no. 1, p. 27, 2016.

[85] A. E. Waldman, "Designing without privacy," *Houston Law Rev.*, vol. 55, no. 659, p. 71, 2018.

[86] A. Da Veiga, N. Martins, and J. H. Eloff, "Information security culture-validation of an assessment instrument," *Southern Afr. Bus. Rev.*, vol. 11, no. 1, pp. 147–166, 2007.

[87] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[88] E. H. Schein, *Organizational Culture and Leadership*. San Francisco, CA, USA: Jossey-Basss, 1985.

[89] D. Zohar, "Safety climate in industrial organizations: Theoretical and applied implications," *J. Appl. Psychol.*, vol. 65, no. 1, p. 96, 1980.

[90] D. Zohar and G. Luria, "A multilevel model of safety climate: Cross-level relationships between organization and group-level climates," *J. Appl. Psychol.*, vol. 90, no. 4, p. 616, 2005.

[91] G. Luria, "Controlling for quality: Climate, leadership, and behavior," *Qual. Manage. J.*, vol. 15, no. 1, pp. 27–40, Jan. 2008.

[92] G. Luria, "Climate as a group level phenomenon: Theoretical assumptions and methodological considerations," *J. Org. Behav.*, vol. 40, nos. 9–10, pp. 1055–1066, Dec. 2019.

[93] A. Cavoukian and M. Dixon, "Privacy and security by design: An enterprise architecture approach," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, Tech. Rep., 2013. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-secu rity-by-design-oracle.pdf

[94] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, Jan. 2008.

[95] CEBMa. (2017). *CEBMa Guideline for Critically Appraised Topics in Management and Organizations*. [Online]. Available: https://cebma.org/wp-content/uploads/CEBMa-CAT-Guidelines-vs-2.0.pdf

[96] S. Trepte, L. Reinecke, N. B. Ellison, O. Quiring, M. Z. Yao, and M. Ziegele, "A cross-cultural perspective on the privacy calculus," *Social Media Soc.*, vol. 3, no. 1, 2017, Art. no. 2056305116688035.

[97] P. Murmann, M. Beckerle, S. Fischer-Hübner, and D. Reinhardt, "Reconciling the what, when and how of privacy notifications in fitness tracking scenarios," *Pervas. Mobile Comput.*, vol. 77, Oct. 2021, Art. no. 101480.

[98] G. Hofstede, B. Neuijen, D. D. Ohayv, and G. Sanders, "Measuring organizational cultures: A qualitative and quantitative study across twenty cases," *Administ. Sci. Quart.*, vol. 35, no. 2, pp. 286–316, 1990.

[99] D. Wright and P. D. Hert, "Introduction to privacy impact assessment," in *Privacy Impact Assessment* (Law, Governance and Technology). Dordrecht, The Netherlands: Springer, 2012, pp. 3–32.

[100] B. Hogan, "Online social networks: Concepts for data collection," *The SAGE Handbook of Online Research Methods*. Thousand Oaks, CA, USA: Sage, 2016, p. 241.

[101] F. Erlandsson, M. Boldt, and H. Johnson, "Privacy threats related to user profiling in online social networks," in *Proc. Int. Conf. Privacy, Secur., Risk Trust Int. Conf. Social Comput.*, Sep. 2012, pp. 838–842.

[102] K. Manheim and L. Kaplan, "Artificial intelligence: Risks to privacy and democracy," *Yale JL Technol.*, vol. 21, no. 1, p. 106, 2019.

[103] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, and A. V. Vasilakos, "Privacy and security issues in deep learning: A survey," *IEEE Access*, vol. 9, pp. 4566–4593, 2020.

[104] S. Karnouskos and F. Kerschbaum, "Privacy and integrity considerations in hyperconnected autonomous vehicles," *Proc. IEEE*, vol. 106, no. 1, pp. 160–170, Jan. 2017.

[105] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[106] R. Barrett, *Building a Values-Driven Organization: A Whole System Approach to Cultural Transformation*. London, U.K.: Butterworth-Heinemann, 2006.

LEONARDO HORN IWAYA (Member, IEEE) was born in Joinville, Santa Catarina, Brazil. He received the B.S. degree in computer science from Santa Catarina State University, the M.S. degree in electrical engineering from the University of São Paulo, and the Ph.D. degree in computer science from Karlstad University, Sweden, in 2019. From 2011 to 2014, he was a Research Assistant with the Laboratory of Computer Networks and Architecture (LARC), PCS-EPUSP. From 2019 to 2021, he worked as a Postdoctoral Researcher with the School of Computer Science, The University of Adelaide, Australia, as part of the Cyber Security Cooperative Research Centre (CSCRC). During 2021 and 2022, he worked as a Postdoctoral Researcher with the Interdisciplinary Research Group on Knowledge, Learning and Organizational Memory (KLOM), Federal University of Santa Catarina. Since 2022, he has been a Postdoctoral Research Fellow with the Privacy & Security (PriSec) Research Group, Karlstad University, contributing to the projects CyberSecurity4Europe, SURPRISE, and TRUEdig. His research interests include privacy engineering, information security, human factors, mobile and ubiquitous health systems, and the privacy impacts of new technologies.

GABRIEL HORN IWAYA received the degree in interdisciplinarity from the University of the Region of Joinville (UNIVILLE), in 2012, and the master's degree in psychology from the Federal University of Santa Catarina (UFSC), in 2020, where he is currently pursuing the Ph.D. degree in psychology. He is also a member of the CNPq Research Group of Organizational Knowledge, Learning and Memory (KLOM).

SIMONE FISCHER-HÜBNER (Member, IEEE) received the Diploma degree in computer science (law), in 1988, and the Ph.D. and Habilitation degrees in computer science from the University of Hamburg, Germany, in 1992 and 1999, respectively. In 2021, she became an Honorary Doctor and an Affiliated Professor with the Chalmers University of Technology, Sweden. She has been a Full Professor with Karlstad University, Sweden, since 2000, where she is currently the Head of the Privacy and Security Research Group. She has been the Scientific Coordinator with the EU H2020 Marie Skłodowska-Curie ITN Privacy & Us and contributed as a partner with security and privacy research to several other EU H2020 projects, including the CyberSec4Europe, PAPAYA, CREDENTIAL, and PRISMACLOUD projects. Her research interests include cyber security, privacy-enhancing technologies, and usable privacy and security. She is a Swedish IFIP TC 11 Representative, the Vice Chair of IFIP TC11, and a member of the Advisory Board Swedish Civil Contingency Agency's Cyber Security Council. She also serves as the Vice Chair for the IEEE Sweden Computer/Software Engineering Chapter and as a Board Member of the Swedish Data Protection Forum.

ANDREA VALÉRIA STEIL is currently pursuing the master's degree in business administration (psychologist) and the Ph.D. degree in production engineering. She is also a Professor at the Graduate Program in Engineering and Knowledge Management and the Graduate Program in Psychology, Federal University of Santa Catarina (UFSC), Brazil. She is a member of the Brazilian Association of Organizational and Work Psychology. Prior to joining academia, she spent ten years in profit and not for profit organizations in human resource management and executive roles.