

The Information Society
An International Journal

ISSN: 0197-2243 (Print) 1087-6537 (Online) Journal homepage: www.tandfonline.com/journals/utis20

Comparative privacy research: Literature review, framework, and research agenda

Philipp K. Masur, Dmitry Epstein, Kelly Quinn, Carsten Wilhelm, Lemi Baruh & Christoph Lutz

To cite this article: Philipp K. Masur, Dmitry Epstein, Kelly Quinn, Carsten Wilhelm, Lemi Baruh & Christoph Lutz (2025) Comparative privacy research: Literature review, framework, and research agenda, The Information Society, 41:2, 69-90, DOI: 10.1080/01972243.2025.2451863

To link to this article: https://doi.org/10.1080/01972243.2025.2451863

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 28 Jan 2025.

Submit your article to this journal

Article views: 2057

View related articles

View Crossmark data

Citing articles: 5 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=utis20

THE INFORMATION SOCIETY
2025, VOL. 41, NO. 2, 69–90
https://doi.org/10.1080/01972243.2025.2451863

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Comparative privacy research: Literature review, framework, and research agenda

Philipp K. Masur[a], Dmitry Epstein[b,c], Kelly Quinn[d], Carsten Wilhelm[e], Lemi Baruh[f], and Christoph Lutz[g]

[a]Department of Communication Science, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands; [b]Noah Mozes Department of Communication & Journalism, Hebrew University of Jerusalem, Jerusalem, Israel; [c]Federmann School of Public Policy & Governance, Hebrew University of Jerusalem, Jerusalem, Israel; [d]Department of Communication, University of Illinois, Chicago, IL, USA; [e]Center for Research on Economies, Societies, Arts and Techniques, Université de Haute-Alsace, Mulhouse, France; [f]Department of Media and Visual Arts, Koç University, Istanbul, Turkey; [g]Department of Communication and Culture, BI Norwegian Business School, Oslo, Norway

ABSTRACT

The ways in which privacy is understood, defined, perceived, and enacted are contingent on cultural, social, political, economic, and technological settings. Yet, privacy research is often criticized for not adequately accounting for these. A comparative perspective requires the contextualization of privacy through investigating similarities and differences across contexts. This article outlines the Comparative Privacy Research Framework, which involves (a) scrutinizing one's position (of power) and epistemological biases, (b) assessing the comparability of the object under study, (c) identifying and justifying meaningful units of comparison, and (d) reflecting on how these units of comparison interact in shaping privacy. We conclude by proposing a comparative privacy research agenda that informs efforts in privacy regulation, education, and research.

ARTICLE HISTORY
Received 10 December 2021
Accepted 6 January 2025

KEYWORDS
Comparative research; framework; literature review; privacy; research agenda

The ways in which people understand, perceive, and enact privacy may differ considerably across cultural, social, political, economic, and technological settings (Altman 1977; Arora 2019). Depending on context, individuals may appraise privacy threats differently, may understand the role of institutions in privacy protection or intrusion differently, and may engage differently with privacy protection strategies. For example, while US respondents were concerned about government use of dedicated mobile contact-tracing apps during the COVID-19 pandemic (Ioannou and Tussyadiah 2021), Israeli citizens showed notable apathy toward the state's use of intelligence surveillance capabilities for the same purpose (Duke 2021). Similarly, in societies with limited freedom of expression and surveillance-heavy policies, individuals tend to be more cautious about expressing dissenting opinions online or sharing information that could be deemed sensitive by the government (Dal and Nisbet 2022; Dal, Nisbet, and Kamenchuk 2023).

The majority of studies on privacy are mono-national and based on samples from Western, educated, industrialized, rich, and democratic (WEIRD) societies (Arora 2019; Henrich, Heine, and Norenzayan 2010; Wu, Vitak, and Zimmer 2020).[1] Findings from such studies are important in their own right and contribute to the understanding of privacy, but we need to be careful to not overgeneralize them beyond their socio-technical context as they rarely move beyond Western conceptualizations of privacy. Even in comparative studies, the role of specific cultural, social, political, economic, and technological differences in shaping privacy-related outcomes, or in determining the applicability of privacy-related concepts, is often insufficiently operationalized.

A comparative approach holds promise for systematic understanding of how privacy is conceptualized, experienced, valued, and studied across contexts (cf. Capurro 2005), exploring both similarities and differences. Comparative privacy research (CPR) questions the generalizability of findings derived from a single context by inviting scholars to critically assess their own interpretations against structural inconsistencies, inequalities, and ethnocentrism (Livingstone 2013). CPR urges scholars to question whether theories of privacy developed in a specific culture can adequately explain the phenomenon in other communities, particularly those that are marginalized or non-Western.

CONTACT Philipp K. Masur p.k.masur@vu.nl Department of Communication Science, Vrije Universiteit Amsterdam, De Boelelaan 1081/1081 HV, Amsterdam, The Netherlands.
© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Furthermore, a comparative lens addresses pressing issues such as the applicability of regulatory approaches across regional or national borders, tensions between global and local power structures, identification of at-risk populations, and the customization of literacy interventions.

But CPR is not simply local methods applied in other contexts or international networking turned into a scholarly collaboration. Such motivations are insufficient and are not conducive to the added value of the comparative approach. Further, "containers" such as nation states have lost some of their heuristic weight (Beck 2007). They are criticized for overlooking both the internal diversity (Esser and Hanitzsch 2012) and the increasing cross-border flow of data and digital services (Aaronson 2019). CPR is particularly needed to address the ongoing tension between transnational communication technologies, their infrastructures and platforms, national or regional regulations, and hyper-local, intimate, and personal experiences. Yet, developing a systematic comparative framework for privacy research is also challenging due to the breadth and ambiguity of the core concepts. Capurro (2005), for example, warns against comparing concepts of privacy that are derived in different historical or cultural contexts because simple juxtaposition inherently oversimplifies.

With this article, we propose a conceptual framework that offers a roadmap to scholars interested in conducting systematic CPR across methodologies. The framework is meant to help scholars (a) to scrutinize their own position (of power), epistemological biases, and how these affect their theoretical and methodological lens in conducting research, (b) to consider the comparability of the object under study, (c) to identify and justify meaningful units of comparison, and (d) to reflect on how these units of comparison interact in shaping privacy, its dimensions, processes, and outcomes. We explicitly incorporate quantitatively, qualitatively oriented and mixed modes of investigation. This diversity enables previously unnoticed and underexplored concepts and relationships to come to light, revealing novel insights into privacy and its contextual dependency. At the same time, such methodological plurality is necessary to explore and test how established concepts manifest themselves in different units of comparison. Obviously, such an aspirational framework has inherent limitations, such as its breadth and complexity that may clash with the practical implementability or by focusing on specific units of comparisons that necessarily represent a form of methodological bracketing (Phipps 2001). While we discuss those in greater detail later, we believe these limitations do not fundamentally undermine the merit of the proposed framework as a basis for conceptual debate and empirical work.

In the following, we will first review existing research and problematize existing privacy theory and CPR to motivate the development of our framework. At the core of this article, we then describe and discuss the four elements of the Comparative Privacy Research Framework (CPRF). Finally, based on this framework, we lay out directions for an emerging CPR agenda to address privacy as a valued outcome through policy formation, education, and research trajectories.

Problematizing existing privacy theory

Privacy theories and conceptualizations continue to be developed and validated through work conducted mostly within WEIRD contexts and among their affluent populations (Li, Ghaiumy Anaraky, and Knijnenburg 2021; Wu, Vitak, and Zimmer 2020). However, as we discuss below, a growing body of situated work – primarily inductive, qualitative studies in specific socio-cultural settings – challenge the generalizability of those theories and conceptualizations. Although not comparative in their own right, thick descriptions of individual experiences, often going beyond the predominant positivist views on privacy and its underpinnings, offer surprising evidence for the inherent variation in privacy experiences across socio-technical contexts, cultures, and countries.

Nonetheless, the majority of research on privacy – including our own – is based on theories, concepts, and definitions of privacy that (1) are based on the assumption that privacy constitutes a universal value, (2) are derived from specific situations in which privacy is assumed to be violated, (3) focus on individuals rather than collectives, (4) overlook diversity among privacy subjects, and (5) assume the existence of transparent and accountable privacy governance structures and institutions.

First, contemporary theories of privacy mostly assume that privacy is a universal value. Westin (1967), for example, argues that "needs for individual and group privacy and resulting social norms are present in virtually every society" (12). Similarly, Altman (1975) states that "while the mechanisms may differ across societies, there appears to be a 'cultural universal' that people in groups can shut off and open themselves to contact with others at different times" (17). The idea is further enshrined in the UN Universal Declaration of Human Rights (UN General Assembly 1948) which includes a protection against

"arbitrary interference with [one's] privacy" as one of the fundamental rights. Yet, while privacy may be highly valued in some cultures and contexts, it may be less valued in others. Some cultures may place greater emphasis on collectivism and community, while others focus more strongly on individual autonomy (Triandis 1988). Further, many privacy theories fail to acknowledge that, even within a single culture, individuals may have different privacy preferences (Masur and Scharkow 2016). Finally, the value of privacy is contingent on specific circumstances and socio-technological settings. For example, the theory of contextual integrity (Nissenbaum 2010), a notable exception in this regard, argues that claims to privacy are in fact claims to an appropriate flow of information in structured social settings with accompanying "canonical activities, roles, relationships, power structures, norms, and internal values" (132). Allen and Mack (1990) critique of origins of privacy norms, for example, highlights how the gendered roots of privacy torts in the U.S. reflect considerations of male privilege, resulting in "wrong kinds of privacy – too much modesty, seclusion" for women (470).

Second, the formulation of a definition of privacy is often the result of an inductive practice that entails examination of situations when individuals or groups think that their privacy has been violated (Solove 2008). For example, Warren and Brandeis (1890) seminal definition of privacy as the "right to be let alone" was a response to the growth of an overly intrusive US press. Similarly, networked approaches to privacy (e.g., Marwick and Boyd 2014) are mainly rooted in the experience of anticipated scaling of information sharing through extended social networks as well as other turbulences resulting from social interactions on social media. This is problematic for several reasons. First, what is considered a privacy violation, and the evaluation of its consequences, can differ depending on cultural and social settings. Second, privacy needs to be defined *independently* of violations. While the notion of privacy violation implies the existence of attendant norms and rules, the experience of privacy can exist even in the absence of such norms and rules. For instance, an individual living in a remote area experiences privacy not because of societal norms and rules but due to the sheer absence of others. Further, not all losses of privacy result necessarily from intentional or accidental violations of norms or rules. For instance, privacy can also be lost passively through unavoidable circumstances, such as living in a densely populated area where physical boundaries are minimal, or through voluntary actions, like sharing personal information in exchange for convenience or social interaction (Tavani 2007). Finally, while inductive approaches that focus on observable violations are valuable for capturing the specific privacy dynamics within a given context, they tend to operate in isolation, missing opportunities to connect with broader theoretical frameworks (cf. Bazarova and Masur 2020). By concentrating solely on violations, these approaches may fail to incorporate insights from established frameworks, such as contextual integrity (Nissenbaum 2010) or interpersonal boundary regulation (Altman 1975), which provide a more comprehensive understanding of privacy as a multifaceted and interdependent phenomenon rooted in social interaction.

When privacy is defined inductively through violations, the focus is primarily on specific instances of harm rather than on the underlying principles or values that privacy protects. This approach makes it challenging to establish a coherent framework that connects a violation to its broader consequences because each violation is treated as a standalone event. As Citron and Solove (2022) highlight, courts often struggle to address privacy violations due to the difficulty of proving tangible harm, which stems from the lack of a clear, overarching definition of privacy that links violations to specific harms. Their proposed solution—a taxonomy of privacy harms rooted in the values privacy safeguards—addresses this issue by shifting the focus from isolated violations to a structured understanding of the fundamental purposes of privacy.

Third, privacy theories are often individualistic, focusing on individual agency, needs, preferences, and behavior instead of acknowledging that privacy is often related to and managed by collectives and groups (Bazarova and Masur 2020, Marwick and Boyd 2014, Petro and Metzger 2023). Rennie, Yunkaporta, and Holcombe-James (2018), for example, show how social norms and obligations in an Australian Aboriginal community, rooted in the ideas of sharing and relatedness, collide with inherently individualistically designed privacy settings in mobile phones and social media platforms. Individualistic privacy management practices embedded in mainstream platforms and devices expose community members to "specific privacy-related ordeals, including identity violations and unauthorized access to financial accounts," and propagate conflict within the community, particularly when devices are shared, challenging established hierarchies and norms of conflict resolution (1305). Notable exemptions are approaches such as Communication Privacy Management Theory (Petronio 2002), networked privacy (Marwick and Boyd 2014),

and group privacy (Petro and Metzger 2023), which view privacy as inherently social, requiring coordination with others, often in a rule-based process that is managed both individually and collectively.

Further, as Regan (1995) has observed, privacy has a collective dimension because contemporary market dynamics make it difficult for any one individual to enjoy privacy without all others enjoying a comparable level of privacy. Even if one chooses to withdraw from disclosing personal information, privacy can be violated through derivatives of private information of others. In algorithmic targeting potential privacy harms arise from processes that assign individuals, without their knowledge, to fluid group memberships for behavioral modification cues, creating an asymmetry between who is rendered visible/actionable (i.e., the group), whose agency is pertinent, and who is given the onus of protection (i.e., the individual) (Helm 2016).

Fourth, privacy conceptualizations and operationalizations often tend to treat subjects uniformly, without regard to their different social, political, economic, and power positions even within a single context. For example, studies investigating the privacy calculus – the idea that people generally weigh the risks and benefits before disclosing (Dinev and Hart 2006) – tend to assume that people are aware of the same benefits and risks. However, perceptions of what constitutes benefits and risks are contingent on individuals' privacy literacy, past experiences, as well as other individual- and group-level characteristics (Dienlin and Metzger 2016; Masur and Trepte 2021). But acknowledging heterogeneity in how people perceive and enact privacy is not just a matter of including relevant control variables. Structurally marginalized groups (e.g., LGBTQ communities, people of color, immigrants, people with disabilities, youth and elders, religious minorities) experience privacy differently from privileged individuals (Marwick and Boyd 2018). Further, non-adaptive conceptualizations of privacy can harm minorities. For example, Fullenwieder and Molnar (2018) show how a liberal approach to privacy was used as a pretext for erasure, whereby the Canadian government utilized existing privacy regulation to obscure the historical record of violence and dispossession in the process of reconciliation with Indigenous populations. Minorities or marginalized communities are also rarely represented in empirical studies, thus obscuring their unique privacy practices. For example, De Wolf and De Leyn (2023) revealed that the group identity of Muslim children in Belgium actively shapes their nonstandard privacy protection and information sharing behavior online. With a clear awareness of how Islam is represented, they actively manage self-presentation online by hiding Islam-related information in some online spaces or negotiating the appropriateness of certain information with other Muslim children.

Fifth, most privacy research assumes the existence of transparent and accountable privacy governance structures or institutions. The responsibility for solving the wicked problem of privacy is placed either with public (government regulation) or private (self-regulation) institutions (e.g., Ginosar and Ariel 2017; Marchant 2020), or with individuals assumed to know how their private data is collected, processed, and shared (Hagendorff 2018; Matzner et al. 2015). While some studies acknowledge the decentralized, polycentric arrangements of privacy governance, they still assume that mechanisms of transparency and accountability allow them to work (e.g., Bennett and Raab 2020). This may not be the case outside liberal democracies, where such mechanisms are lacking or do not exist. For example, the study of social media visibility management practices in an authoritarian regime has revealed the importance of "slow visibility" privacy strategies, where dissidents carefully stage the revelation of their political beliefs and activities to balance the very tangible risks and less tangible benefits of such exposure (Pearce, Vitak, and Barta 2018).

While not an exhaustive list, these five assumptions are the focus of the criticism of much privacy research today. It is criticized for enacting an ethnocentric approach (Arora 2019; Keulen and Kroeze 2018) and for reifying power structures that are rooted in deterministic, techno-centric, capitalistic worldviews (Fuchs 2011). As such, it preserves existing forms of marginalization and enables new ones, which give rise to the "privacy rich" and "privacy poor" (Marwick and Boyd 2018). Engaging with each of the aforementioned five criticisms is necessary to outline the value proposition of CPR. A comparative lens allows both testing of established theories in new contexts and discovering or developing new conceptualizations of privacy that address some of the critiques outlined above. Before we outline the major tenets of the proposed CPRF, we discuss existing comparative and situated privacy studies.

Problematizing existing comparative privacy research

While limited in volume, CPR has highlighted important structures along which privacy can be meaningfully studied. The largest part of this literature utilizes quantitative-descriptive methods to study differences

between countries. Some of these studies rely on large-scale surveys in multiple countries (e.g., Bellman et al. 2004; European Commission 2019), while others use dedicated, smaller samples focused on specific countries (e.g., Cho, Knijnenburg, and Li 2018; Cho, Rivera-Sánchez, and Lim 2009; Cho et al. 2023; Dinev et al. 2006; Krasnova, Veltri, and Günther 2012; Li, Rho, and Kobsa 2022; Miltgen and Peyrat-Guillard 2014; Trepte et al. 2017).

The European Commission regularly conducts large-scale surveys across all EU member states that include questions related to privacy and data protection (2011, 2015, 2019). Even with their relatively simple design and measurements, these studies provide evidence of striking differences across countries. For example, in 2015, there was substantial variation in public awareness of the Snowden revelations among EU member states, with awareness levels surpassing 70% in some countries (e.g., Germany, Austria) while remaining around 30% in others (e.g., Croatia, Cyprus) (European Commission 2015).

Studies utilizing country-specific samples highlight similar differences, albeit in a more nuanced fashion. For example, Dinev et al. (2006) investigated the privacy calculus regarding online purchases in Italy and the US using a more elaborate measurement of privacy than the European Commission surveys, considering risk, trust, and privacy concerns. Among other things, they found that trust in an online business and general privacy concerns were stronger predictors of the willingness to engage in online purchases in the US compared to Italy.

Despite their benefits, cross-country comparison studies have several limitations. First, they typically do not offer potential explanations for the differences they report. Second, political geography is often, and somewhat imprecisely, interpreted as offering a cultural lens (Livingstone 2013). Third, the selection of countries is often opaque and not sufficiently justified. Finally, while methodologically convenient, country-level comparisons may overlook the true source of variation within or across the country-units.

Other, more culturally aligned studies (e.g., Cho et al. 2023; Li, Rho, and Kobsa 2022; Miltgen and Peyrat-Guillard 2014) call attention to underlying dimensions such as Hofstede's (1984) cultural difference dimensions (i.e., individualism, indulgence, power distance, masculinity, long-term orientation, and uncertainty avoidance). These differences are used to justify country selection for comparison, as country-level predictors (Trepte et al. 2017), or moderators of privacy outcomes (Baruh, Secinti, and Cemalcilar 2017). For example, comparing countries with low (South Korea and Singapore) and high (Australia and US) individualism scores, Cho, Rivera-Sánchez, and Lim (2009) found that higher individualism positively predicted privacy concerns, suggesting that cultural orientations can meaningfully explain cross-country differences.

That said, such work generally hinges on the premise that nations have a distinctive national culture perpetuated through institutions such as family, education, media, and law, and assign aggregated, country-specific values to all participants. In doing so, such studies assume an unrealistic homogeneity within a country and are reductive of the complexity of culture. Such studies would benefit from approaches that investigate sources and consequences of variation within national cultures.

We want to stress that in addition to countries, meaningful units of comparison can be found in a variety of cultural, societal, political, economic, and technological structures and manifestations. For example, some privacy research may qualify as comparative work because it uncovers differences and similarities attributable to political systems, ideologies or regulatory regimes (Bennett 1992; Bignami 2007; Koops et al. 2017; Mendez and Mendez 2010). For example, Bennett's (2013) comparative analysis of voter management databases, commercial data brokerage firms, micro-targeting practices and social media, highlights how regulations and cultural norms were more likely to facilitate voter surveillance in the US than in the EU. Similarly, in a qualitative comparative analysis of how privacy issues are placed on the political agenda, how centralized solutions are justified, and which policy instruments are available in the US and the EU, Mendez and Mendez (2010) show how the design of privacy regulations reflects the underlying governance structures.

Examining individual behavior from a lens that takes into account these units of comparison is equally important. Pearce and Vitak (2016) demonstrated this in their study of Azerbaijani adolescents, revealing how the pervasive "honor culture," with its repercussions for deviating from behavioral codes, influences distinct privacy and impression management strategies in online settings. Particularly in relation to the role of political context, comparative research that analyzes one regulatory regime against another remains scarce. When it does exist, comparative work disproportionately focuses on democratic countries (e.g., US vs. European Union) that also tend to be contexts where governance structures are more transparent and relevant data is more accessible (cf. Van Eeten and Mueller 2013). This, however, limits the diversity and representativeness of compared political contexts.

Finally, existing CPR has also drawn attention to the affordances that various technologies offer for privacy enactment. Studies in this area have highlighted similarities and differences in privacy threats and protections across different online spaces (Han et al. 2013; Pekárek and Pötzsch 2009) and also that technological architectures influence behavioral norms (Lee and Yuan 2020; Papacharissi 2009). Han et al. (2013), for example, compared how differences between Android and iOS platforms may affect privacy protections built into third-party applications deployed on those platforms. They reported that iOS apps collected more sensitive user information, attributing this to higher accountability to the platform rather than the end users. In a study focusing on the relationship between affordances and privacy behavior, Choi and Sung (2018) found that users on Snapchat tend to be more candid, while Instagram users, exhibiting higher privacy concerns, present a rather idealized version of themselves.

In sum, comparative studies have focused on important intersections between privacy and culture, structural inequities, and political ideology. Likewise, they have emphasized the economic and socio-technical dimensions of privacy behavior and decision-making. Yet, comparative studies of privacy remain scarce, largely descriptive, and limited in their explanatory power. The future of privacy research requires challenging simplistic conceptual and empirical transferability, thereby deepening the understanding of privacy.

Comparative Privacy Research Framework

In proposing the CPRF, we aspire to build on the existing work discussed above, while addressing its limitations. Our goal is to offer a framework that balances rigor and openness, thus allowing for incorporation of different modes of empirical investigation, including both confirmatory and exploratory, as well as quantitative, qualitative, and mixed-methods designs. Such a framework should inspire scrutinizing privacy from multiple angles, including the examination of established conceptualizations of privacy across acknowledged units of comparison as well as evaluating the comparability of privacy-related concepts and exploring new units of comparison.

To reiterate, using the framework means (a) scrutinizing one's own position (of power), epistemological biases, and how these affect the theoretical and methodological lens in conducting research, (b) identifying and justifying meaningful units of comparison, (c) assessing the comparability of the object under study, and (d) explaining how these units of comparison may interact with privacy, its dimensions, processes, and outcomes.

While we present those elements in a particular order, they do not represent a sequential procedure. Rather, a comparativist will have to engage with all of them simultaneously and in an iterative fashion. For example, the meaningfulness of units of comparison is to a large degree dependent on how they interact with the object under study, and whether it is even comparable across those units. Furthermore, only the full picture of the planned investigation will allow a researcher to fully assess their own positionality. In the following, we will introduce each of these elements of the CPRF in more depth and discuss how those principles can be applied in designing and carrying out empirical research.

Identifying biases and scrutinizing one's position of power

In any research, we need to acknowledge that researchers' identity, personal characteristics and histories, as well as institutional incentives and constraints, shape their perspectives and subsequently their scholarship (Jafar 2018). Acknowledging and thinking through our own positions of power and associated biases is the first step in making research more rigorous and its findings more valid (Jafar 2018). This is particularly true for CPR.

As discussed above, when studying privacy, the fuzziness of the concept itself makes it amenable to framing from contesting positions (Arora 2019). These affect the choice of a study's focus, theoretical frameworks, design, and interpretation, ultimately resulting in a presentation of the research that may be representative of a certain perspective, but not necessarily generalizable beyond. Conducting CPR necessarily involves venturing beyond one's own boundaries of experience. A particular challenge is to adapt design and measurement to all studied settings and truly represent experiences different than one's own. In many cases, working together with local experts and extending the research team to cover relevant areas and expertises is often a logical and necessary step.

We suggest that comparative researchers should first acknowledge their positionality, embrace reflexivity throughout the design, analysis, and interpretation stages of their research, and aim to increase the validity and credibility of the entire research process, to produce a more transparent, and honest account of the research (Corlett and Mavin 2018).

Positionality

Acknowledging positionality means opening up one's self, rather than only one's scholarly ideas and products, to criticism (Massoud 2022). Wilson, Janes, and Williams (2022) describe positionality as locating the researcher in relation to "the topic under investigation; the research participants; and the research design, context and process" (46). However they acknowledge that positionality is not always a conscious choice, but also determined by how they are viewed by other actors such as study participants and gatekeepers. Incorporating a positionality statement in research outcomes (e.g., publications, reports) gives greater attention to, and a traceable account of, how identity and personal characteristics, experiences of marginalization or personal and professional privileges have influenced and shaped the formulation of research questions, the type of data collection, and analysis, and – perhaps most importantly – the interpretation of findings (Massoud 2022). Writing such a statement necessitates the researcher to consciously examine their own identity and biases to allow the reader to assess the effect of their personal perspectives (Wilson, Janes, and Williams 2022). Together with reflexivity in writing and interpretation, acknowledging positionality contributes to a more honest and trustworthy presentation of one's work.

To provide a tangible example of this practice, we provide our own positionality statement for this project:

> As comparative privacy scholars, we understand that our personal backgrounds, histories, and experiences play an integral role in shaping our approach to comparative privacy research. On the one hand, we recognize that our multicultural diversity, with authors from Germany, Switzerland, Russia, the USA, and Turkey, in part residing in additional countries such as the Netherlands, Israel, Norway, and France, allows us to understand the unique privacy concerns of a range of different groups and communities worldwide. On the other hand, we recognize a lack of diversity in areas like gender, race, socio-demographic status, and geography. These gaps may make it challenging to identify and understand privacy concerns of underrepresented and marginalized communities. With our expertise in both qualitative and quantitative research traditions, we also bring a necessarily wide, but not exhaustive range of theoretical and methodological lenses. Yet, we are cognizant of our Western academic training, the predominantly WEIRD contexts of our prior research, and the WEIRD theories and methods we use. To counter potential biases resulting from our backgrounds, we commit to self-reflection and to scrutinizing how our perspectives influence our research questions, methodologies, analyses, and interpretations.

In other words, it is crucial to address those characteristics of the researcher(s) that are particularly prone to influence the research and that provide a sufficiently broad basis for the practice of reflexivity (see below). Here, we aim to develop a CPR framework applicable to a large range of research projects. We thus want to acknowledge our cultural and academic backgrounds and how they represent both a strength and weakness.

Reflexivity

Scrutinizing one's own position and biases is not done by simply including a positionality statement. Rather, such a statement defines the a priori starting point from which the research process can be traced and reflected upon. Reflexivity refers to "critical thinking that involves addressing the issues of identity and positionality by making the researcher's assumptions explicit and finding strategies to question these" (Wilson, Janes, and Williams 2022, 44). Embracing reflexivity beyond the initial positional statement may include a) explicitly describing the reflexivity process in the methodology section, outlining steps taken to monitor and address potential biases, b) discussing one's own assumptions, values, and biases, while interpreting the results and aiming to minimize the subjectivity throughout the process (see also further below), and c) honestly reflecting on the limitations the research and acknowledging how potential biases may have influenced the findings.

During the writing of this manuscript, we often recognized our own limitations in conceptualizing a truly comprehensive and broadly applicable framework. For example, an early version of this paper was still heavily influenced by our own position and experiences and thus included description, rather than critical assessment of privacy theories that originated in WEIRD contexts, embodied a positivist, quantitative approach to the comparative study of privacy, and failed to incorporate the reflexivity that we consider to be a critical part of the framework itself. Iterative deliberation among the authors, constant back-and-forth between existing literature, reviewer feedback, and critical assessment of our own conclusions enabled us to gain a deeper and more inclusive understanding of these ideas.

Validity and credibility

To increase validity and credibility in comparative research, we need to make sure that (a) the research questions can be meaningfully investigated across units of comparison (e.g., is privacy even a meaningful

object of investigation in all contexts?), (b) the instrument and methods implemented are unit-invariant (e.g., cross-contextual invariance of measures) and (c) the findings truly represent the actual "experience" of participants in each one of the units of comparison (e.g., the interpretation of interview data truly represents the interviewees' account of their lived experiences).

Different research traditions offer solutions to increase the validity and credibility of a research product. Mixed-methods approaches that usually first (qualitatively) explore a concept's transferability across contexts and units of comparison and then (quantitatively) test differences, are helpful to ensure the cross-unit applicability and validity of research questions, concepts, and hypotheses. Cross-cultural, cross-language, or cross-setting validation of instruments (e.g., back-and-forth translation, invariance tests, piloting with local experts) is needed to ensure functional equivalence across the chosen units of comparison (Esser and Vliegenthart 2017). For example, if we want to study people's privacy concerns, items that refer to the term (e.g., "In general, how concerned are you about your privacy while you are using the internet?"; see scale by Buchanan et al. 2007) cannot easily be translated to languages such as Russian, which does not have a native word for privacy.

Finally, qualitative research offers strategies to establish trustworthiness of a researcher's interpretation of data that can be applied to both confirmatory and exploratory, as well as quantitative and qualitative, comparative research projects (e.g., Corbin and Strauss 2007). Such strategies include, for example, recontacting participants to check whether the interpretation reflects their viewpoints adequately, triangulating results across different data sources, bringing in different theoretical perspectives, having different researchers analyze the data independently, and establishing consensus among a broader research team.

Identifying units that are meaningful for comparison

Through comparison, we want to elicit understanding about a phenomenon that would be unattainable from studying a single context or setting. Thus, the selection of units of comparison is an important step in its own right. For privacy research, this means coming up with units of comparison that are meaningful for understanding privacy or, alternatively, assessing whether available units of comparison may be meaningful for the same purpose.

Traditionally, comparative research involves contrasting a minimum of two macro-level units (e.g., countries or social milieus), during at least one point in time, with at least one object of investigation (Esser and Hanitzsch 2012). A systematic review of 147 comparative communication research articles (So 2017) showed that most (56%) focus on countries or nations. Indeed, relying on countries as units of comparison for privacy research is a potentially fruitful approach, provided the researchers are explicit about what aspects of the nation states are meaningful for understanding privacy. Yet, the same review alluded that 8.7% of the articles also compare systems (mostly political systems), 6.5% conduct comparisons across cultures, 1.6% compare different people (e.g., based on socio-demographics), and 1.1% compare markets (economic structures). Such units of comparison can be relevant to privacy research as they have been identified in prior research as meaningful in understanding how people think about and enact privacy in technologically mediated environments (e.g., Dal, Nisbet, and Kamenchuk 2023; Epstein and Quinn 2020; Han et al. 2013). With CPRF, we offer directions for approaching the task of identifying and assessing the meaningfulness of units of comparison by outlining five categories of such units. By means of methodological bracketing (Phipps 2001), we propose five central categories for units of comparison: cultural, social, political, economic, and technological (see Table 1). On the one hand, these categories are already implicitly used in existing CPR (see the work discussed above and the review by So 2017). On the other hand, they reflect the often expressed need to move beyond cross-cultural or cross-national comparisons and also conduct cross-political as well as cross-platform investigations (e.g., Matassi and Boczkowski 2021). In the following, we describe and justify the meaningfulness of each of these categories for CPR.

We acknowledge that this list of categories is not exhaustive. Concrete units of comparison that will emerge from within those categories, or even a recognition that new categories may be needed, will be a function of the disciplinary backgrounds and research foci of scholars doing the work. The categories, however, offer a starting point for systematic engagement with the potentially overwhelming breadth of units that can be used for comparison, their possible overlap, and interaction. We view such units as dynamic, changing over time, and interrelated, simultaneously shaping human behavior and being shaped by the exercise of individual agency.

Table 1. Categories of units of comparison.

Category	Description	Examples of cases within units of comparison
Cultural	Collectives of people with shared identities, values, or practices	Collectivist vs. individualist cultures; specific subculture compared in different geographic locations
Social	Sociological concepts that classify people into groups of similar characteristics	Adolescents vs. elderly; males vs. females; clustering based on socio-economic status
Political	Political concepts that differentiate political and/or regulatory systems	Democracies vs. autocracies; levels of surveillance; voting systems
Economic	Economic concepts that distinguish markets, commons, or economic power structures	Market economy vs. planned economy; monopolistic vs. oligopolistic market systems
Technological	Types or families of technological environments	Ephemeral vs. persistent communication; comparison based on affordances

Finally, the traditional macro-, meso-, and micro-level differentiation (Turner 2005) is useful for articulating the level on which a unit of comparison is located. While these three levels are inherently interdependent, systematic analysis requires distinguishing between them as they dictate units of observation, sampling strategy, type of aggregation, and analytical procedure. Comparative research frequently focuses on macro-level units of comparison (e.g., cultures, nations, political systems), but comparisons on a meso-level (e.g., organizations, or technological environments) or micro-level (e.g., social contexts or situations) may be equally important and fruitful.

Cultural units of comparison

Culture is a contested term in social science. This is in part due to the duality of relationships between culture and social phenomena as the two both shape and are shaped by each other. From an anthropological perspective, one can argue that people identify or are identified with certain cultures (e.g., national, age-related, gender-specific, or religious cultures), which in turn shape how they are perceived by others and also how they enact their own identity. Culture thereby can be understood as a set of shared beliefs, values, customs, behaviors, and artifacts that characterize a particular group, a collective of individuals, or an entire society (Jahoda 2012; Kroeber and Kluckhohn 1952). It is dynamic and evolving, maintained through mundane practices, and challenged through political and social developments. It reflects inherent power relations and societal structures, serving as a primary framework for agency (Goffman 1974). As such, the way people think and talk about privacy reflects certain cultural predispositions toward the place of an individual vis-a-vis commercial and government institutions. At the same time, norms and practices around privacy evolve within established cultural frameworks and thus are bound by how those frameworks structure individual agency.

Historically, much comparative research has focused on cross-cultural comparisons using countries as macro-level units (So 2017; Taras, Steel, and Kirkman 2016). Such focus has been criticized for ignoring cultural heterogeneity within nations and the fact that cultures are not bound by national borders (Livingstone 2013). For example, Remennick (2006) showed that Jewish immigrants from the former USSR residing in Germany, US/Canada, and Israel share more common beliefs and practices with each other than with their country of origin or their place of residence.

The meaningfulness of cultural units in the enactment of privacy is well noted in the literature (e.g., Miltgen and Peyrat-Guillard 2014; Trepte et al. 2017). For example, Murphy's (1984) anthropological study of the use of veils among men from Saharian Tuareg culture suggests that veils aid the management of social distancing because they hide relevant social cues, allowing men to be socially engaged while remaining aloof. Research on interpersonal relationships in Western cultures similarly suggests that withholding sensitive information or concealing affective states may support relationship initiation by adding ambiguity (e.g., Norton, Frost, and Ariely 2007). A comparative approach would enable understanding of how distance and ambiguity are utilized in different cultures to accomplish privacy.

Cultural units of comparison, however, can also refer to subcultures or any group who identify themselves as a collective, but are not necessarily bound by national borders (e.g., Amish people in the US, hip hop culture, quantified-self movement, hacker scene). While we do not aspire to prescribe how researchers should conceptualize culture for the purposes of CPR, we stress the need to approach the selection of cultural units intentionally. By requiring specific articulation, the CPRF proposes to systematically address the challenge posed by nested, overlapping, and concurrent cultural influences.

Social units of comparison

There are multiple ways for classifying people that would be meaningful for CPR. Units such as gender, life stage, socio-economic status, education, relationship types, family composition, ethnicity, social milieus, profession, political affiliation, types of users, etc. are

typically assigned to people by third parties such as researchers, businesses, or policy makers. The (assumed) homogeneity within these social groups, and the (assumed) distinctiveness between those groups is what makes them meaningful for those assigning the labels, but therefore also for comparative research. At times, such classifications are the result of deliberate planning and aimed at achieving certain goals (e.g., reducing complexity of empirical data through clustering, targeted marketing, tailored policy solutions). At other times, they emerge naturally from social interactions and practices or are adopted as a means for people to simplify the complexities of their social life. Presence of such exogenous classifications is meaningful for investigating privacy because privacy is, at least partially, socially constructed through such classifications. For example, when a policymaker is offering special protection to the privacy of minors, it delineates both what minors can and cannot do, as well as the role privacy plays for the formation of their agency.

Social units of comparison have been employed in research as meaningful explanatory variables. Extant socio-psychological research, for example, reveals how perceptions of privacy and the ways in which it is balanced with other needs are linked to different life stages (Peter and Valkenburg 2011). In Turkey, young adults were found to have higher needs for social interaction on Facebook compared to older adults, thus disclosing more personal information. Yet, due to the higher risks for privacy violations, they also implemented more privacy protection compared to middle-aged and older adults (Kezer et al. 2016). Such perspectives are valuable because they expose the social construction of privacy across life stages.

Using social units of comparison allows engaging with the unique questions associated with privacy in marginalized communities (Marwick and Boyd 2018), particularly with the growing commodification of privacy (Papacharissi 2010). For example, youth from low socio-economic backgrounds (Marwick, Fontaine, and Boyd 2017), similarly to political refugees in the U.S. (Simko et al. 2018), self-censored in order to protect their privacy, thus also withholding their voices from the public sphere (see Sannon and Forte 2022 for a thorough overview).

At the same time, privacy itself can be used as a meaningful social unit of comparison. For example, Westin used privacy preference statements in surveys to cluster people into three groups: privacy fundamentalist, privacy pragmatists, and the unconcerned (Westin 2003). This classification has often been used to study differences in (online) behaviors or how people respond to different scenarios where privacy considerations may matter (Woodruff et al. 2014). John et al. (2023) relied on aggregate privacy preferences to explain their comparative setup in a study of the role of privacy in decisions surrounding technology adoption for emergency remote teaching in schools during the COVID-19 pandemic.

However, it is important to recognize intersectionality, as cultural and social structures are not always distinct. For example, an individual may identify with a certain gender, and therefore feel part of a certain culture (e.g., LGBTQ+). Yet, the same individual may be assigned a social cluster (e.g., socially constructed gender that is defined mostly by biological sex), which may constrain their ability to enact or control their desired level of privacy. Similarly, a person may identify with a generation and its culture (e.g., baby boomers), but at the same time may be placed into a certain age-group (e.g., right now: older adults), which is a social classification independent of a generation. As such, differentiating cultural and social categories may at times be a useful heuristic, but we argue that CPR should strive to tease out and study their intersections (Hoffmann, Lutz, and Ranzini 2024).

As questions about privacy are often interwoven with questions about social inequality and power, CPR calls for both intentional selection of social units of comparison and explicit articulation of their value proposition for understanding privacy, privacy-related behaviors and how the accomplishment of privacy may act as a marker of status (Hoffmann, Lutz, and Ranzini 2024).

Political units of comparison

Such units refer to governance structures and associated institutional arrangements (Mendez and Mendez 2010). They are an explicit manifestation of power relations, which construct and constrain individual agency and autonomy. These may include different political systems (e.g., democracy, autocracy, monarchy), political parties and ideologies (e.g., conservatives, liberals), electoral frameworks, regulatory regimes and norms (e.g., PIPEDA, GDPR), or interest groups and stakeholders (e.g., private sector, civil society, local vs. national).

For privacy, which is inherently political and increasingly regulated (Möller et al. 2020), such units of comparison are meaningful because they determine the conditions under which individuals, groups, or organizations experience the flow of personal information. Concurrently, the ways in which privacy and data protection are regulated and implemented are contingent on political systems and regulatory

histories (Aho and Duffield 2020; Petkova 2019). Political and institutional manifestations of privacy, such as privacy policy paradigms and discourses (Epstein and Medzini 2022; Guay and Birch 2022; Lokot 2020; Wu et al. 2011), and governmental practices such as surveillance (Aho and Duffield 2020; Lyon 2014) or limits to free speech (Pearce, Vitak, and Barta 2018), can be both a basis and an object for comparison.

Comparing directives, acts, and other legal texts across diverse political systems reveals distinctions in privacy's conceptualization and in notions about who can be entrusted with its protection. For example, data localization is seen as a way of countering data colonialism and leveling the playing field for the Global South (Belli 2021). At the same time, it is criticized for enabling domestic surveillance by authoritarian regimes (Belli 2021; Taylor 2020). Focusing on political units can further contrast how different regulatory contexts emphasize "freedom from" intrusions over "freedom to" attain self-actualization (e.g., Koops et al. 2017; Masur 2020).

Purposeful and intentional choice of relevant political units of comparison should enable a more sophisticated inquiry into the duality of privacy as an inherently political construct. Given the interrelated nature of political concepts, a mixed-unit analysis (e.g., political systems and political parties) may be particularly fruitful for uncovering the underlying power structures shaping privacy.

Economic units of comparison

As personal data underpins economic activity and is treated as a valuable commodity, privacy may take on different meanings within different economic systems. Meaningful economic units of comparison for CPR may include economic systems (e.g., capitalistic, socialistic, nationalistic), market structures (e.g., monopolistic, competitive; open vs. closed markets), business models (e.g., data-centric vs. data-agnostic; for-profit vs. non-for-profit; advertisement-based, subscription-based, freemium, on-demand; B2B vs. B2C), or consumer mindsets (e.g., willingness to pay vs. expectation of free access or use).

Capitalism is frequently blamed for the increased commodification of personal data, which is at the basis of normative criticism of how major technological companies treat privacy (Fuchs 2011; Sevignani 2016; West 2019). Specific economic environments place different premiums on private information and provide alternative incentives for protecting, invading, and exploiting individual privacy (Spiekermann et al. 2015). Market structures may thereby shape interactions between individuals who use certain services, companies which provide those services, and regulators who aim to align information flows with data protection law (Bazarova and Masur 2020). Financial and structural incentives fuel the development of the data broker industry and frameworks for privacy-compromising internet use (e.g., Facebook's "Free Basics"; Reviglio 2022; Nothias 2020). The exploitative practices of companies such as Alphabet/Google and Meta/Facebook, and their business models of data accumulation (Zuboff 2019) are rarely systematically compared for privacy implications outside of security research (e.g., Daryabar et al. 2016).

Comparing the strategies and market positioning of companies could involve assessing how companies differentiate themselves based on privacy features, privacy assurances, or privacy-related certifications or policies. For example, Han et al. (2013) analyzed more than 500 pairs of free Android apps and their paid counterparts for differences in data collection practices and privacy policies. In contrast to users' expectations, they found that paid versions do not guarantee more protection in practice. Comparative researchers can analyze the impact of privacy as a competitive factor in different industries and sectors. This could include analyzing the revenue models of companies that rely on collecting and monetizing user data versus those that prioritize privacy protection. For example, collecting less information can result in consumers' willingness to pay higher prices (Preibusch, Kübler, and Beresford 2013).

Economic aspects can also be interesting to investigate as the result of different privacy approaches. For example, this could involve evaluating the economic consequences of different privacy practices, decision-making, or policy making, such as the potential costs and benefits to users, businesses, industries, or the overall economy.

Despite their promise, economic factors are neglected in privacy research outside of economics. Incorporating economic units of comparison in privacy research offers another perspective on the ways in which inequality and power are distributed and negotiated in contemporary societies.

Technological units of comparison

Individuals increasingly communicate and conduct their daily lives across different technological environments that afford different conceptions and mechanisms for privacy, resulting in multimodal communication patterns (Banks 2017). As such, comparing across different

media and platforms is important to "foster a denaturalization process whereby a case once thought to be unique is reconceptualized in light of other, similar or different, cases" (Matassi and Boczkowski 2021, 208).

A lot of comparative work in communication has taken a *channel-centered* approach, which refers to comparisons across devices (e.g., smartphone, tablet, desktop computer, fitness tracker), types of applications (e.g., social network sites, online shopping websites, email), branded applications (e.g., Facebook, Instagram, WhatsApp), and features (e.g., status update, profile, messenger, chat) (Meier and Reinecke 2021). Although a valuable approach, particularly if an explicit contrast between two units (e.g., Facebook vs. Twitter) is of interest, it is limited in explaining variance in perceptions, attitudes, or behaviors.

A *communication-centered* approach extends the channel-centered approach by focusing more explicitly on characteristics of interaction (e.g., the configuration and directionality of interaction, interaction partners) and messaging (e.g., content, mode, persistence, ephemerality, accessibility) (Meier and Reinecke 2021). In fact, as comparative researchers, we often chose certain applications (e.g., Facebook and Twitter) for comparison because they determine or constrain certain types of interactions and messaging.

Both channel- and communication-centered approaches can be criticized for technological determinism because they suggest a strong uniformity in how certain channels or characteristics of communication influence behaviors. The concept of affordances, "the multifaceted relational structure between an object/technology and the user that enables or constrains potential behavioral outcomes in a particular context" (Evans et al. 2017, 36), acknowledges the dynamic, interdependent relationship between subject and object. Instead of clustering technology by device, platform, or branded application, an *affordance-centered approach* would highlight similarities and differences in the dynamic interaction between the attributes and abilities of users, the materiality of technologies, and the contexts of technology use across such clusters (Evans et al. 2017). Particularly, if we steer away from labeling affordances, but engage in describing the *interplay* between features (e.g., number, breadth or type of privacy settings), what it suggests to different users (e.g., those with different levels of privacy literacy, concerns, or attitudes), and the context of use (e.g., for the purpose of socializing with others), we can better understand the antecedents and determinants of privacy-related behaviors (e.g., disclosure).

For example, Hollenbaugh (2019) used differences in available privacy settings and the inherent ephemerality of content (communication-centered) as a basis for (channel-centered) comparison between Facebook and Snapchat users, demonstrating how the latter were more open in terms of their privacy management and disclosure. Zhang, Bazarova, and Reddy (2021) investigated differences in depth of disclosure related to distress during the COVID-19 pandemic across different platforms (channel-centered) also by focusing on particular affordances of these platforms (affordance-centered). They found that people disclosed more *via* Zoom compared to other platforms, but also that affordances related to persistence, anonymity, and visibility control were stronger positive predictors of depth of disclosure independent of the platforms.

Technological arrangements restrict and enable information flows and privacy (Rossi 2021). Thus for CPR, the analysis of similar families of technological arrangements (i.e., those which provide similar affordances of interaction and messaging), in contrast to specific devices or platforms may often be more meaningful for understanding variability in privacy outcomes.

Assessing the comparability of the object of investigation

Another element of the CPRF refers to scrutinizing the object of investigation and assessing its comparability across the cases within units of comparison. Crafting a comparative design, particularly for a fuzzy concept such as privacy, requires decisions about the conceptualization of the object of study, the levels on which it can be observed, and the ways it can be measured (Vasalou, Joinson, and Houghton 2015). In many ways, such decisions are contingent on established knowledge about the phenomenon in a particular context, the research goals, and the epistemological position of the researcher. Fundamentally, the researcher can choose between an *etic approach*, studying a phenomenon across contexts using established criteria independent of specific contexts, an *emic approach*, studying a phenomenon from within specific contexts, or a combination of the two (cf. Esser and Vliegenthart 2017).

For example, researchers may want to compare privacy protection behaviors (e.g., actively limiting access to the self) across different contexts. Following an etic approach means designing instruments that capture a preconceived understanding of privacy protection behaviors, independent of context (e.g., a list of universal behaviors such as using pseudonyms at

registration). Such an approach allows analyzing differences in privacy protecting behaviors resulting purely from dissimilarities in contexts. An emic approach assumes that privacy protecting behaviors can differ in form, appearance, and subjective meaning assigned to them by participants in each specific context. The goal here is to expose and *understand* specific privacy protection behaviors, occurring in specific contexts (e.g., using encryption for email, withholding private information in a face-to-face conversation). A combination of the two approaches could be to first identify the relevant privacy protection behaviors in each context and then design context-sensitive instruments that nonetheless capture privacy protection behaviors in a comparable way (e.g., closing a door to restrict parents' access is similar to restricting a social media post so that parents can't see it). In the latter case, however, consolidating results from unique contexts into one analysis can be quite challenging, as different measurements require proof that the resulting data are indeed comparable (Esser and Vliegenthart 2017).

This example highlights that for a meaningful comparison, we need to compare *functionally equivalent* aspects, facets, or dimensions of the phenomenon (e.g., we can compare the height of two different animals, but not the height of one animal with the color of another). Establishing functional equivalence, however, is not always straight-forward. Comparing across different, potentially multiple cases within units of comparison means focusing on their similar functions or purposes rather than their specific forms or structures (Van Deth 2006).

For the etic approach, functional equivalence is fundamental as it requires structural invariance of instruments across contexts (Esser and Harnitzsch 2012; Wirth et al. 2012). For example, if we study privacy protection behaviors of young adolescents and older adults while using Facebook, we can use the same instrument (e.g., "Is your social media profile public or private?") as the same settings are available to both age groups. Yet, measurement instruments do not need to be 100% identical, but rather exhibit functional equivalence (Esser and Vliegenthart 2017). When comparing levels of knowledge about data protection law (Masur, Teutsch, and Trepte 2017), researchers would have to adapt any existing measure to the legal systems in which it is assessed. While items will differ across cases, they will still represent the same idea.

When using an emic approach, investigating the functional equivalence of a phenomenon can be its own research goal. As mentioned before, the label of privacy does not always translate across languages (e.g., the Russian language does not have a native word for privacy). If we use an emic approach to conduct a meaningful comparison, functional equivalence of the object of investigation is again required. As mentioned in the example above, different types of behaviors can serve to control the access to the self (e.g., closing a door, planting hedges, using privacy settings on social media, remaining anonymous, using encryption). Some of them are only observable in specific contexts. Yet, due to the similar role and function in relation to privacy, we can nonetheless compare people's engagement with them.

Engaging in comparative research of such fuzzy concepts as privacy, one has to be aware of potential differences in how the concept itself, or an aspect of the phenomenon that one aims to investigate, are perceived, interpreted, and enacted or manifested across cases. It is critical to draw on local expertise to establish functional equivalence and identify any variation that needs to be taken into account. The need for local expertise may appear obvious when adopting an emic approach, as it focuses on context-specific experiences and interpretations. Yet, an etic approach equally needs local expertise to assess both functional and instrumental equivalence. Finally, the team needs ongoing communication to maintain equivalence of conceptualizations, and depending on the chosen approach, also equivalence of instruments.

Explaining how meaningful units of comparisons interact with privacy

We envision the five categories of units of comparison to be applicable to both inductive and deductive approaches to studying privacy. Independently of whether the researchers pursue a critical or a more positivist take on privacy research, using the CPRF involves the comparison across at least two meaningful cases within a unit of comparison (e.g., two or more political systems, two or more online platforms) with respect to at least one object of investigation (e.g., privacy regulations, privacy policies, privacy infrastructures, privacy concerns, self-disclosure, attitudes, privacy literacy).

Studying privacy comparatively entails engaging with *how* the units of comparison interact with privacy-related aspects. Thereby, the object of investigation has to be at the same or a lower level of analysis as the unit of comparison, while accounting for potential interdependencies between micro, meso, and macro level factors. In the simplest form, one

can consider how two cases (e.g., Germany vs. Israel) within a single macro-level unit of comparison (countries), within one of the aforementioned categories (cultural unit of comparison), help us learn something about an object of investigation (e.g., privacy concerns). Next, one can consider how multiple cases (e.g., Facebook, Instagram, Snapchat, BeReal) of the same meso-level unit of comparison (social network sites) in one category (technological) help us in explaining differences in a micro-level object of investigation (e.g., self-disclosure). However, the ultimate value of the CPR lies in investigating how multiple cases (e.g., adolescents, emerging adults, older adults and Facebook, Instagram, Snapchat) across different units of comparison (life stages and social network sites) can explain variability in an object of investigation (e.g., privacy protection strategies). The latter may be particularly interesting, as cases within different units of comparison and within different categories (potentially also across macro, meso, or micro levels of analysis) are not always ontologically distinct; they may in fact interact and offer explanation of potential differences in an object of investigation (cf. fig. 1 by Matassi and Boczkowski 2021).

There are several approaches for a systematic consideration of possible relationships between units of comparison and the object of investigation, as well the interactions between the units of comparison themselves. The implementation of those approaches may differ in quantitatively and qualitatively oriented research, but engaging with them is essential in establishing a baseline for comparison. In what follows, we will use a hypothetical example of a study of privacy and political expression (cf. work by Dal, Nisbet, and Kamenchuk 2023) in order to illustrate various uses of CPRF.

Quantitatively oriented approaches

Quantitatively oriented approaches involve data collection methods and research designs such as cross-sectional and longitudinal surveys, experiments, or content analysis of naturally occurring texts (e.g., news, policies, laws), among others. The most common quantitatively oriented approach to comparative research is "small-*N* studies" that follow a quasi-experimental logic (Esser and Vliegenthart 2017). Here, *N* refers to the number of cases (e.g., Germany and Russia) within a unit of comparison (countries). Akin to the idea of purposeful sampling in qualitative research (see below), the basic idea is to intentionally sample a relatively limited number of cases that maximize variance in specific features (or interactions thereof) that are assumed to explain variance in the outcome variable. Within each case, we then randomly sample a sufficient number of observations (e.g., *n* of participants) that allows investigating the research phenomena with sufficient statistical power. Such an approach allows for both confirmatory and exploratory studies.

Confirmatory studies formulate and test hypotheses about how a specific feature(s), represented across cases within a unit of comparison, relates to a specific outcome(s). Let's imagine we want to investigate the relationship between regulatory systems (macro-level) and political expression (micro-level). We hypothesize that there will be more political expression in an environment with stronger privacy protection and less state-mandated surveillance. Here, we would purposefully sample countries that differ in terms of their regulatory approaches to privacy and surveillance (a political unit of comparison; e.g., Germany as a proxy for high privacy protection and low surveillance and Russia as a proxy for low privacy protection and high surveillance). Measuring political expression in both cases would allow to test differences across the cases using standard linear modeling (e.g., t-test, analysis of variance, regression-based approaches).

We could also hypothesize that the unit of comparison acts as a moderator of a particular relationship between two variables. In the example above, we could assume that higher privacy concerns negatively relate to political expression. Taking into account the influence of the regulatory system on this relationship, we may further assume that whereas high concerns in the German population may not lead to less political expression (as they do not have to fear any ramifications), higher concerns may lead to less political expression in Russia (as they fear political repercussions). Here, we would measure both privacy concerns and political expression in both cases to test the interaction between regulatory systems and privacy concerns in predicting political expression (i.e., cross-level interaction analyses).

We can also assume that the relationship between privacy concerns and political expression is affected not just by the regulatory system within which it exists (political unit of comparison), but also by the social status of the participants (social unit of comparison); for example, belonging to a minority would strengthen the effects of concern on political expression. To study both influences, we need to purposefully sample people from certain minorities and from the majority in both countries. Then, we could investigate the distinct or interactive impact of both units of comparison on the relationship of interest (e.g.,

using moderation analysis with two interaction terms or a three-level interaction term) as the same minority groups may experience privacy differently depending on the regulatory system in which they live.

The generalizability of findings of small-*N* studies is limited to the intentionally sampled cases within a chosen unit of comparison (e.g., Germany vs. Russia; cf. Esser and Vliegenthart 2017), and cannot be applied to other cases, even within the same unit of comparison (e.g., to France). Large-*N* studies, in contrast, purposefully focus on "parsimonious explanatory designs, where the impact of a few key variables is tested on as many cases as possible, thereby identifying universal laws that can be widely generalized" (Esser and Vliegenthart, 2017, 11). Rather than purposefully sampling a few cases ($N = 3–10$ countries), such designs are based on large and diverse samples of cases ($N > 50$ countries). Within each case, we again randomly sample a sufficient number of observations (n). The goal is to identify abstract relationships between attributes of *all* cases and measured outcome variables, rather than to study the unique quality of individual cases. Continuing with the example above, we could assess the general impact of the regulatory regime on political expression. We hence would sample participants from a variety of countries that represent a wide range of regimes from low privacy protection and high state surveillance to high privacy protection and low state surveillance. Often, such studies are conducted as secondary data analyses of large scale public surveys (e.g., World Value Survey, European Social Survey). Although the standard analytical techniques outlined above are applicable here (e.g., analysis of variance to compare differences across all cases), large-N studies will often use multilevel modeling to study the relationship of interest across all cases, while accounting for case-specific deviations from an overall pooled effect.

We want to emphasize that the principles described above for quantitatively oriented confirmatory research, in terms of case selection and analytical approach, apply to quantitatively oriented *exploratory* research as well. Here, the focus would be on identifying differences *via* descriptive analysis that may help formulating hypotheses for future confirmatory research.

Qualitatively oriented approaches

Qualitative comparative research engages with the complexity of social phenomena by exploring the subjective meanings, experiences, perspectives, and behaviors of individuals or groups (or with the complexity of documents, policies, infrastructures, etc.) (Berg-Schlosser 2012). Rather than investigating a phenomena in a standardized, comparatively inflexible way based on existing theory, qualitative research generally follows an inductive approach, where researchers immerse themselves in the data to develop, question, extend, or modify existing theories and hypotheses (Corbin and Strauss 2007). Depth and holistic understanding of unique cases or individual experiences is thereby more important than breadth and generalizability (Creswell and Creswell 2018). Qualitative approaches are characterized by the use of data collection methods such as interviews, focus groups, document analysis, and ethnographic observation.

Similarly to small-*N* quantitative research, intentionality in case selection is at the core of inductive, qualitative approach to comparison (Corbin and Strauss 2007). Different from small-*N* quantitative research, however, intentionality here applies to both selection of cases within a unit of comparison (e.g., Germany and Russia) and selection of observations within each case (e.g., specific individuals, texts, images). In our hypothetical example, we may still choose to investigate the German and the Russian cases as encapsulating meaningful contextual factors, such as level of privacy protection and surveillance, that in turn, may impact political speech. Selecting the observations for each case, however, will now require intentional choices that are particularly helpful for gaining insights about the phenomenon of interest. Such choices depend on the research question at hand and may be directed toward different goals (Creswell and Creswell 2018).

Intentional sampling allows for an emergent, iterative development of the insight, thus offering room for new, unanticipated understanding of the phenomenon. Qualitative analysis is intentionally open, flexible, and iterative, whereby insights gained from observations often lead to modifications of both case selection and the additional sampling of specific observations within these cases during the study itself (Patton 2015). Iterating between analysis and sampling is also known as *theoretical sampling,* a core aspect of qualitative analysis approaches such as grounded theory (Corbin and Strauss 2007; Suri 2011). Depending on the research question and/or the emerging insights throughout the analysis, researchers may engage in different types of intentional sampling techniques for the selection of observations, including purposeful sampling, maximizing variation, ensuring diversity and exhaustiveness/saturation, or negative case sampling (Suri 2011; Patton 2015). In the

following, we illustrate how these approaches may apply to our hypothetical example.

To study privacy and political expression in different regulatory regimes, a researcher may start by *purposefully sampling* participants that are actively engaged in political expression (Suri 2011). This may allow the researcher to understand how people who are politically expressive perceive and experience the regulatory regime, how they understand and practice their privacy, and how they view and make sense of possible connection (or lack thereof) between privacy and their political speech. At the same time, a researcher may also want to *maximize variation* in the focal behavior, thus choosing extreme cases of participants who engage in political expression and those who consciously choose to remain silent. Upon analyzing the first participants in each case, an emerging insight may be that minority status in both Germany and Russia plays a role in how people experience privacy and surveillance in connection to political expression. After deciding to purposefully sample participants from such minorities, the researchers may realize that they started with a certain notion of minority and proceed to refine this notion in light of emerging findings, requiring an adjustment to their sample. While some minorities, for instance, can share characteristics across both cases (e.g., immigrants), others may be unique and somewhat counterintuitive (e.g., stance toward the war in Ukraine).

Refining the sample in such a way may necessitate engaging with other units of comparison such as technological choices. For example, initial interviews with political activists among the studied minorities reveal that they use different online platforms and communication channels. As a consequence, the researchers may decide to actively recruit users of these (and other) platforms to further enhance the diversity of the studied sample. Such a refinement not only leads to a more holistic engagement with the subjective experiences of the participants, but also provides the added opportunity to assess the combined or interactive impact of different units of comparison (in this case: countries, minority status, and technological platform) on the relationship between privacy concerns and political expression.

Regardless of the actual mode of data collection, comparative analysis of qualitative data needs specialized expertise in the case within the unit of comparison. In our hypothetical example, making sense of the subjective experiences and perceptions of participants in both Russian and German regulatory systems would require local expertise in both contexts within the research team.

During the analysis, it is crucial to maintain a constant awareness of the a priori formulated positionality statement and to document the evolving thought-process (Massoud 2022) to avoid downplaying or neglecting data that suggests unexpected patterns, assuming them to be an exception rather than a widespread phenomenon. Fundamental to rigorous qualitative data analysis, such practice enables avoidance of an unconscious focus on evidence that supports a particular viewpoint. For example, a researcher investigating differences in political expression between Germany and Russia would rely on their a priori defined positionality to recognize instances where e.g., participants in Russia express relatively more political freedom than expected, despite the country/culture's authoritarian tendencies.

Finally, moving between in-depth examination of unique cases and cross-case comparison is paramount for CPR. At the very basic level, this approach allows drawing direct comparisons between similar behaviors, perceptions, and rationalizations across cases. Additionally, it may allow identifying otherwise neglected themes or aspects of the phenomenon in one case by explicitly observing and labeling them in the other.

In our example, a researcher may find that the personality of a German political activist may strongly explain her motivation to participate in online political expression, despite pronounced privacy concerns. This observation-specific finding may lead to a new label "personality" that is then explicitly investigated in other observations and cases in which it may not have been as salient.

The road ahead: Discussion, limitations, and research agenda

We proposed and illustrated the use of the CPRF – a systematic framework for conducting comparative privacy research. The framework is motivated by our critical analysis of the existing literature. First, we highlighted five major shortcomings of contemporary privacy theories voiced in the literature: (1) the unreasonably strong assumption that privacy is a universal value; (2) a strong focus on situations of privacy violations; (3) attention to individuals rather than collectives; (4) uniform treatment of privacy as a research object; and (5) uncritical assumptions about existence of transparent and accountable privacy governance structures and institutions. We argue that such shortcomings limit the understanding of privacy as a continuously changing phenomenon and hinder the transferability of existing theories to other, non-WEIRD

contexts. Second, we reviewed existing CPR, pointing out that it remains scarce, largely descriptive, and limited in its explanatory power by an excessive focus on nation states as units of comparison, thus overlooking other potential sources of variation in privacy outcomes.

Based on this analysis, we proposed the CPRF, which consists of four main elements: First, consistent with best practice in qualitative research, it calls for identifying one's own biases and assumptions to establish both transparency and trustworthiness of the comparison by injecting a clear positionality statement and practicing reflexivity throughout the project. Second, it involves identifying and justifying meaningful units of comparison for better understanding variation in privacy outcomes. CPRF therefore suggests five categories of such meaningful units of comparisons (cultural, social, political, economic, and technical) to systematically explore the source of variation. Third, the framework requires assessing the comparability of the object under study to ensure functional equivalence and to take potential context-sensitive variation into account during conceptualization and operationalization of the studied concepts. Finally, CPRF involves scrutinizing the interaction between the chosen unit(s) of comparison with the object of investigation and systematically thinking through or exploring the mechanisms that explain their entanglement. CPRF is methodologically agnostic and thus applicable to all modes of investigation, ranging from confirmatory to exploratory and quantitative to qualitative approaches. Depending on the chosen approach, the final step then includes a rigorous assessment of the sampling and analysis strategies.

Limitations of the framework

First, by the very nature of placing "methodological brackets" (Phipps 2001) around complex and interrelated ideas, this proposal is a compromise between different points of views and opinions. While working on this framework, our international team of authors had in-depth discussions about terminology (e.g., about terms such as "culture"), classification (e.g., which categories of units of comparison to include), theoretical perspectives (e.g., what theories to review), and applications (e.g., use of the framework across methodologies). It is important to acknowledge these tensions when viewing CPRF as the final product. With that, we explicitly focused on five categories that suggest macro-level units of comparison, as we deem them particularly important for a nuanced understanding of privacy. However, other units of comparison, such as between-person differences (e.g., personality characteristics) or within-person processes (e.g., comparing different situations), might be worth considering. We invite scholars with different backgrounds to explore the benefits of adopting CPRF for their particular mode of investigation.

Second, CPRF is highly aspirational. Closely adhering to the proposed framework will often result in complex, expansive, and expensive designs, as the main value of it lies in assessing the interactive power of units of comparison in explaining variation in privacy outcomes. Such complexity often clashes with the practical considerations of conducting research such as time, cost, and available human capacity. That said, when it comes to resolving the tension between the desired and possible in research, CPRF offers ways to make informed bracketing decisions. An in-depth engagement with several units of comparison also offers the means to choose those that align with practical considerations as well as are most promising to meeting the research goals.

Third, our framework does not explicitly address temporal dynamics in both units of comparison and outcomes. An extension of CPRF might add a longitudinal, or cross-temporal, component (Esser and Hanitzsch 2012), as local and global events, as well as moving through different life stages, may change perceptions, practices, and markets (Keulen and Kroeze 2018).

Finally, the proposed framework requires empirical application and testing. Empirical CPR research thereby should build on established comparative methodologies (Esser and Hanitzsch 2012). Future research should systematically identify and analyze the methodological challenges and pitfalls of using this framework.

Research agenda

We believe privacy is more important than ever given the growing datafication of our lives. A rigorous adoption of the CPRF can advance the scope and nuance attributable to privacy and its outcomes. To focus on several fundamental questions facing privacy researchers, and inform privacy regulation and technology design, we outline the following important and sustainable trajectories for CPR moving forward. First, researchers should use CPRF to systematically test the applicability and generalizability of currently established theories beyond the contexts of their origin. This holds the promise to identify generalizable aspects of established theories, as well as expose Western assumptions that are irrelevant to other

cultural, social, political, economic, or technological settings. Second, researchers should aim to seek out new perspectives on privacy conceptualization. Acknowledging the inherent WEIRD basis of existing theories of privacy should motivate research to actively seek alternative ways of thinking about variation in privacy outcomes. CPRF offers guidance for those venturing into those uncharted territories. Third, researchers should systematically investigate the impact of different units of comparison on a variety of privacy-related outcomes.

To inspire new and sustainable privacy research, we recommend that future research should use CPRF to engage with the following pressing issues:

1. Engage with questions of privacy and power, particularly by better understanding how marginalized communities are affected by privacy regulations, practices, and norms, and how they deal with resulting privacy issues. Such research may involve the contrasting of cultural (e.g., identity of marginalized groups), social (e.g., socio-economic or immigration status) and political units of comparison (e.g., policies specific to the marginalized group).
2. Assessing the role of technology and platform providers in shaping the power imbalance between large companies and individual users. A focus on technical (e.g., different platforms or products), economic (e.g., different business models), and political units of comparison (e.g., differences in policy and regulation efforts) may help to understand the impact of corporate surveillance on individual agency.
3. Evaluating digital inequality resulting from socio-technological arrangements (technical and economic units of comparison) and traditional socio-economic markers of inequality such as age, gender, education, or income, as well as their intersection (social units of comparison).
4. Assessing how state surveillance practices in different regimes (political unit of comparison) affect individual privacy concerns, political expression and other individual freedoms.
5. Assessing the impact of decision-making with constitutive effects (e.g., government or corporate policy making) on global as well as local privacy and data protection issues. Such research may involve contrasting political (e.g., type of regulation or policy) and cultural units of comparison (e.g., different countries or regions).
6. Evaluating tensions between privacy regulation and technological innovation, whereby lack of restrictions on the use of personal data can create opportunities for technological innovation, but at the same time place unprotected populations at risk. Such research would investigate the impact of political (e.g., innovation policy) or economic (e.g., level of economic development) units of comparison on privacy outcomes (e.g., levels of privacy protection afforded to citizens).

We hope that CPRF provides a basis for future, more systematic work and thereby contributes to global, as well as local, efforts to address pressing privacy issues. It is our hope that CPRF will serve as an invitation for future discussions about how we, as a community of scholars, conceptualize and empirically engage with privacy research.

Note

1. We are aware of the limitations of this oversimplifying binary distinction and acknowledge that neither the category WEIRD, nor the residual category non-WEIRD do justice to the complexity of human lives in different countries, cultures, and regions (cf. Ghai 2021). For the purpose of our argument here, however, we find this categorization useful as a way to characterize the predominant privacy research at this point in time.

Authors' contributions

Philipp K. Masur and Dmitry Epstein share co-first authorship and contributed equally to the article.

Funding

Philipp K. Masur's work was supported by the Dutch Science Foundation, Grant #VI.Veni.211S.06. Christoph Lutz' work was supported by the Research Council of Norway, Grant #275347.

References

Aaronson, S. A. 2019. What are we talking about when we talk about digital protectionism? *World Trade Review* 18 (4):541–77. doi:10.1017/S1474745618000198

Aho, B., and R. Duffield. 2020. Beyond surveillance capitalism: Privacy, regulation, and big data in Europe and China. *Economy and Society* 49 (2):187–212. doi:10.1080/03085147.2019.1690275

Allen, A. L., and E. Mack. 1990. How privacy got its gender. *Northern Illinois University Law Review* 10 (3):441–78.

Altman, I. 1975. *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole.

Altman, I. 1977. Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues* 33 (3):66–84. doi:10.1111/j.1540-4560.1977.tb01883.x

Arora, P. 2019. Decolonizing privacy studies. *Television & New Media* 20 (4):366–78. doi:10.1177/1527476418806092

Banks, J. 2017. Multimodal, multiplex, multispatial: A network model of the self. *New Media & Society* 19 (3):419–38. doi:10.1177/1461444815606616

Baruh, L., E. Secinti, and Z. Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67 (1):26–53. doi:10.1111/jcom.12276

Bazarova, N. N., and P. K. Masur. 2020. Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology* 36:118–23. doi:10.1016/j.copsyc.2020.05.004

Beck, U. 2007. Beyond class and nation: Reframing social inequalities in a globalizing world. *The British Journal of Sociology* 58 (4):679–705. doi:10.1111/j.1468-4446.2007.00171.x

Belli, L. 2021. BRICS countries to build digital sovereignty. In *CyberBRICS: Cybersecurity regulations in the BRICS countries*, ed. L. Belli, 271–80. Cham, Switzerland: Springer.

Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *Information Society* 20 (5):313–24. doi:10.1080/01972240490507956

Bennett, C. J. 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Bennett, C. J. 2013. The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western Democracies. *First Monday* 18 (8):1–23. doi:10.5210/fm.v18i8.4789

Bennett, C. J., and C. D. Raab. 2020. Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance* 14 (3):447–64. doi:10.1111/rego.12222

Berg-Schlosser, D. 2012. *Mixed methods in comparative politics: Principles and applications*. New York: Springer.

Bignami, F. 2007. Privacy and law enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law* 8 (1):233–56.

Buchanan, T., C. Paine, A. N. Joinson, and U. D. Reips. 2007. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology* 58 (2):157–65. doi:10.1002/asi.20459

Capurro, R. 2005. Privacy. An intercultural perspective. *Ethics and Information Technology* 7 (1):37–47. doi:10.1007/s10676-005-4407-4

Cho, H., B. Knijnenburg, A. Kobsa, and Y. Li. 2018. Collective privacy management in social media: A cross-cultural validation. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25 (3):1–33. doi:10.1145/319310

Cho, H., M. Metzger, S. Trepte, and E. Nekmat. 2023. A cross-country study of comparative optimism about privacy risks on social media. *International Journal of Communication* 17:2003–23.

Cho, H., M. Rivera-Sánchez, and S. S. Lim. 2009. A multinational study on online privacy: Global concerns and local responses. *New Media & Society* 11 (3): 395–416. doi:10.1177/1461444808101618

Choi, T. R., and Y. Sung. 2018. Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and Informatics* 35 (8):2289–98. doi:10.1016/j.tele.2018.09.009

Citron, D. K., and J. Solove. 2022. Privacy harms. *Boston University Law Review* 102 (3):793–863.

Corbin, J., and A. Strauss. 2007. *Basics of qualitative research: Techniques and procedures for developing grounded theory.* 3rd ed. Thousand Oaks, CA: SAGE.

Corlett, S., and S. Mavin. 2018. Reflexivity and researcher positionality. In *The SAGE handbook of qualitative business and management research methods*, eds. C. Cassell, A. L. Cunliffe, and G. Grandy, 377–99. Thousand Oaks, CA: SAGE.

Creswell, J. W., and J. D. Creswell. 2018. *Research design: Qualitative, quantitative, and mixed methods approaches.* 5th ed. Thousand Oaks, CA: SAGE.

Dal, A., and E. C. Nisbet. 2022. To share or not to share? How emotional judgments drive online political expression in high-risk contexts. *Communication Research* 49 (3):353–75. doi:10.1177/0093650220950570

Dal, A., E. C. Nisbet, and O. Kamenchuk. 2023. Signaling silence: Affective and cognitive responses to risks of online activism about corruption in an authoritarian context. *New Media & Society* 25 (3):646–64. doi:10.1177/14614448221135861

Daryabar, F., A. Dehghantanha, B. Eterovic-Soric, and K. K. R. Choo. 2016. Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. *Australian Journal of Forensic Sciences* 48 (6):615–42. doi:10.1080/00450618.2015.1110620

De Wolf, R., and T. De Leyn. 2023. Toward a better understanding of minorities' privacy in social Media. In *The Routledge handbook of privacy and social media*, eds. S. Trepte, and P. K. Masur, 45–53. London: Routledge.

Dienlin, T., and M. J. Metzger. 2016. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a U.S. representative sample. *Journal of Computer-Mediated Communication* 21 (5):368–83. doi:10.1111/jcc4.12163

Dinev, T., and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17 (1):61–80. doi:10.1287/isre.1060.0080

Dinev, T., M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti. 2006. Privacy calculus model in e-commerce: A study of Italy and the United States. *European Journal of Information Systems* 15 (4):389–402. doi:10.1057/palgrave.ejis.3000590

Duke, S. A. 2021. Nontargets: Understanding the apathy towards the Israeli security agency's Covid-19 surveillance. *Surveillance & Society* 19 (1):114–29. doi:10.24908/ss.v19i1.14271

Epstein, D., and K. Quinn. 2020. Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society* 6 (2):1–13. doi:10.1177/2056305120916853

Epstein, D., and R. Medzini. 2022. Conversations with fellow leaders: Privacy framing in congressional hearings after Cambridge Analytica. *Telecommunications Policy* 46 (10):102427. doi:10.1016/j.telpol.2022.102427

Esser, F., and R. Vliegenthart. 2017. Comparative research methods. In *The international encyclopedia of communication research methods*, ed. J. Matthes, 1–22. New York: Wiley-Blackwell.

Esser, F., and T. Hanitzsch. 2012. On the why and how of comparative inquiry in communication studies. In *The handbook of comparative communication research*, eds. F. Esser, and T. Hanitzsch, 3–22. London: Routledge.

European Commission. 2011. Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union. Last accessed January 4, 2025. https://europa.eu/eurobarometer/surveys/detail/864.

European Commission. 2015. Special Eurobarometer 431: Data protection. Last accessed January 4, 2025.https://europa.eu/eurobarometer/surveys/detail/2075.

European Commission. 2019. Special Eurobarometer 487a: The General Data Protection Regulation. Last accessed January 4, 2025. https://europa.eu/eurobarometer/surveys/detail/2222.

Evans, S. K., K. E. Pearce, J. Vitak, and J. Treem. 2017. Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication* 22 (1):35–52. doi:10.1111/jcc4.12180

Fuchs, C. 2011. Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society* 9 (4):220–37. doi:10.1108/14779961111191039

Fullenwieder, L., and A. Molnar. 2018. Settler governance and privacy: Canada's Indian Residential School Settlement Agreement and the mediation of state-based violence. *International Journal of Communication* 12:1332–49.

Ghai, S. 2021. It's time to reimagine sample diversity and retire the WEIRD dichotomy. *Nature Human Behaviour* 5 (8):971–2. doi:10.1038/s41562-021-01175-9

Ginosar, A., and Y. Ariel. 2017. An analytical framework for online privacy research: What is missing? *Information & Management* 54 (7):948–57. doi:10.1016/j.im.2017.02.004

Goffman, E. 1974. *Frame analysis: An essay on the organization of experience*. Cambridge; MA: Harvard University Press.

Guay, R., and K. Birch. 2022. A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008–2016). *Big Data & Society* 9 (2):1–13. doi:10.1177/20539517221112925

Hagendorff, T. 2018. Privacy literacy and its problems. *Journal of Information Ethics* 27 (2):127–45.

Han, J., Q. Yan, D. Gao, J. Zhou, and R. H. Deng. 2013. Comparing mobile privacy protection through cross-platform applications. Accessed December 12, 2024. https://ink.library.smu.edu.sg/sis_research/1698

Helm, P. 2016. Group privacy in times of big data: A literature review. *Digital Culture & Society* 2 (2):137–52. doi:10.14361/dcs-2016-0209

Henrich, J., S. J. Heine, and A. Norenzayan. 2010. Most people are not WEIRD. *Nature* 466 (7302):29– doi:10.1038/466029a

Hoffmann, C. P., C. Lutz, and G. Ranzini. 2024. Inequalities in privacy cynicism: An intersectional analysis of agency constraints. *Big Data & Society* 11 (1):1–13. doi:10.1177/20539517241232629

Hofstede, G. 1984. Cultural dimensions in management and planning. *Asia Pacific Journal of Management* 1 (2):81–99. doi:10.1007/BF01733682

Hollenbaugh, E. E. 2019. Privacy management among social media natives: An exploratory study of Facebook and Snapchat. *Social Media + Society* 5 (3):1–14. doi:10.1177/2056305119855144

Ioannou, A., and I. Tussyadiah. 2021. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society* 67:101774. doi:10.1016/j.techsoc.2021.101774

Jafar, A. J. N. 2018. What is positionality and should it be expressed in quantitative studies? *Emergency Medicine Journal: EMJ* 35 (5):323–4. doi:10.1136/emermed-2017-207158

Jahoda, G. 2012. Critical reflections on some recent definitions of culture. *Culture & Psychology* 18 (3):289–303. doi:10.1177/1354067X12446229

John, N., S. Joeckel, D. Epstein, and L. Dogruel. 2023. Privacy and distance learning in turbulent times: A comparison of German and Israeli schools during the beginning of the COVID-19 pandemic. *Learning, Media and Technology* 48 (3):514–27. doi:10.1080/17439884.2022.2089682

Keulen, S., and R. Kroeze. 2018. Privacy from a historical perspective. In *The handbook of privacy studies*, eds. B. Van der Sloot, and A. De Groot, 21–56. Amsterdam: Amsterdam University Press.

Kezer, M., B. Sevi, Z. Cemalcilar, and L. Baruh. 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10 (1):2. doi:10.5817/CP2016-1-2

Koops, B. J., B. Newell, T. Timan, I. Skorvanek, T. Chokrevski, and M. Galic. 2017. A typology of privacy. *University of Pennsylvania Journal of International Law* 38 (2):483–575.

Krasnova, H., N. F. Veltri, and O. Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering* 4 (3):127–35. doi:10.1007/s12599-012-0216-6

Kroeber, A. L., and C. Kluckhohn. 1952. *Culture: A critical review of concepts and definitions*. Cambridge, MA: Harvard University Press.

Lee, Y. H., and C. W. Yuan. 2020. The privacy calculus of "friending" across multiple social media platforms. *Social Media + Society* 6 (2):1–10. doi:10.1177/2056305120928478

Li, Y., E. H. R. Rho, and A. Kobsa. 2022. Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology* 41 (3):655–77. doi:10.1080/0144929X.2020.1831608

Li, Y., R. Ghaiumy Anaraky, and B. Knijnenburg. 2021. How not to measure social network privacy: A cross-country investigation. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5, 1–32. New York: ACM. doi:10.1145/3449218

Livingstone, S. 2013. Challenges to comparative research in a globalizing media landscape. In *The handbook of comparative communication research*, eds. F. Esser, and T. Hanitzsch, 414–29. London: Routledge.

Lokot, T. 2020. Data subjects vs. people's data: Competing discourses of privacy and power in modern Russia. *Media*

and Communication 8 (2):314–22. doi:10.17645/mac.v8i2.2883

Lyon, D. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1 (2):1–13. doi:10.1177/2053951714541861

Marchant, G. E. 2020. Governance of emerging technologies as a wicked problem. *Vanderbilt Law Review* 73:1861–78.

Marwick, A. E., and D. Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16 (7):1051–67. doi:10.1177/1461444814543995

Marwick, A. E., and D. Boyd. 2018. Understanding privacy at the margin: Introduction. *International Journal of Communication* 12:1157–65.

Marwick, A. E., C. Fontaine, and D. Boyd. 2017. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society* 3 (2):1–14. doi:10.1177/2056305117710455

Massoud, M. F. 2022. The price of positionality: Assessing the benefits and burdens of self-identification in research methods. *Journal of Law and Society* 49 (S1):64–86. doi:10.1111/jols.12372

Masur, P. K. 2020. How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication* 8 (2):258–69. doi:10.17645/mac.v8i2.2855

Masur, P. K., and M. Scharkow. 2016. Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society* 2 (1):1–13. doi:10.1177/2056305116634368

Masur, P. K., and S. Trepte. 2021. Transformative or not? How privacy violations experiences influence online privacy concerns and online information disclosure. *Human Communication Research* 47 (1):49–74. doi:10.1093/hcr/hqaa012

Masur, P. K., D. Teutsch, and S. Trepte. 2017. Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [Development and validation of the online privacy literacy scale]. *Diagnostica* 63 (4):256–68. doi:10.1026/0012-1924/a000179

Matassi, M., and P. Boczkowski. 2021. An agenda for comparative social media studies: The value of understanding practices from cross-national, cross-media, and cross-platform perspectives. *International Journal of Communication* 15:207–28.

Matzner, T., P. K. Masur, C. Ochs, and T. V. Pape. 2015. Self-data-protection: Empowerment or burden? In *Data protection on the move: Current developments in ICT and privacy/data protection*, eds. S. Gutwirth, R. Leenes, and P. de Hert, 277–305. Dordrecht, The Netherlands: Springer.

Meier, A., and L. Reinecke. 2021. Computer-mediated communication, social media, and mental health: A conceptual and empirical meta-review. *Communication Research* 48 (8):1182–209. doi:10.1177/0093650220958224

Mendez, F., and M. Mendez. 2010. Comparing privacy regimes: Federal theory and the politics of privacy regulation in the European Union and the United States. *Publius: The Journal of Federalism* 40 (4):617–45. doi:10.1093/publius/pjp031

Miltgen, C. L., and D. Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems* 23 (2):103–25. doi:10.1057/ejis.2013.17

Möller, J. E., J. Nowak, S. Kannengießer, and J. E. Möller. 2020. The politics of privacy: A useful tautology. *Media and Communication* 8 (2):232–6. doi:10.17645/mac.v8i2.3373

Murphy, R. F. 1984. Social distance and the veil. In *Philosophical dimensions of privacy: An anthology*, ed. F. D. Schoeman, 34–55. 1st ed. Cambridge, UK: Cambridge University Press.

Nissenbaum, H. F. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford Law Books.

Norton, M. I., J. H. Frost, and D. Ariely. 2007. Less is more: the lure of ambiguity, or why familiarity breeds contempt. *Journal of Personality and Social Psychology* 92 (1):97–105. doi:10.1037/0022-3514.92.1.97

Nothias, T. 2020. Access granted: Facebook's free basics in Africa. *Media, Culture & Society* 42 (3):329–48. doi:10.1177/0163443719890530

Papacharissi, Z. 2009. The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld. *New Media & Society* 11 (1–2):199–220. doi:10.1177/1461444808099577

Papacharissi, Z. 2010. Privacy as a luxury commodity. *First Monday* 15 (8). https://firstmonday.org/ojs/index.php/fm/article/download/3075/2581. doi:10.5210/fm.v15i8.3075

Patton, M. Q. 2015. *Qualitative research & evaluation methods: Integrating theory and practice*. 4th ed. Thousand Oaks, CA: SAGE.

Pearce, K. E., and J. Vitak. 2016. Performing honor online: The affordances of social media for surveillance and impression management in an honor culture. *New Media & Society* 18 (11):2595–612. doi:10.1177/1461444815600279

Pearce, K. E., J. Vitak, and K. Barta. 2018. Socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication* 12:1310–31.

Pekárek, M., and S. Pötzsch. 2009. A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society* 2 (1):81–93. doi:10.1007/s12394-009-0016-4

Peter, J., and P. M. Valkenburg. 2011. Adolescents' online privacy: Toward a developmental perspective. In *Privacy online: Perspectives on privacy and self-disclosure in the social web*, eds. S. Trepte, and L. Reinecke, 221–34. Berlin: Springer.

Petkova, B. 2019. Privacy as Europe's First Amendment. *European Law Journal* 25 (2):140–54. doi:10.1111/eulj.12316

Petro, G., and M. Metzger. 2023. The right to group privacy. In *The Routledge handbook of privacy and social media*, eds. S. Trepte, and P. K. Masur, 45–53. London: Routledge.

Petronio, S. S. 2002. *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Phipps, A. G. 2001. Empirical applications of structuration theory. *Geografiska Annaler Series B: Human Geography* 83 (4):189–204. doi:10.1111/j.0435-3684.2001.00106.x

Preibusch, S., D. Kübler, and A. R. Beresford. 2013. Price versus privacy: An experiment into the competitive advantage of collecting less personal information.

Electronic Commerce Research 13 (4):423–55. doi:10.1007/s10660-013-9130-3

Regan, P. M. 1995. *Legislating privacy: Technology, social values and public policy*. Chapel Hill, NC: University of North Carolina Press.

Remennick, L. 2006. Russian jews in the global city of Toronto: A pilot study of identity and social integration. *Espace populations sociétés. Space populations societies* 1:61–81. doi:10.4000/eps.1235

Rennie, E., T. Yunkaporta, and I. Holcombe-James. 2018. Privacy versus relatedness: Managing device use in Australia's remote Aboriginal communities. *International Journal of Communication* 12:1291–309.

Reviglio, U. 2022. The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview. *Internet Policy Review* 11 (3):1–27. doi:10.14763/2022.3.1670

Rossi, J. 2021. What rules the internet? A study of the troubled relation between web standards and legal instruments in the field of privacy. *Telecommunications Policy* 45 (6):102143. doi:10.1016/j.telpol.2021.102143

Sannon, S., and A. Forte. 2022. Privacy research with marginalized groups: What we know, what's needed, and what's next. Accessed December 12, 2024. https://arxiv.org/pdf/2206.15037

Sevignani, S. 2016. *Privacy and capitalism in the age of social media*. New York: Routledge.

Simko, L., A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno. 2018. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*, 409–423. New York: IEEE. doi:10.1109/SP.2018.00023

So, C. Y. K. 2017. Mapping comparative communication research: What the literature reveals. In *Advancing comparative media and communication research*, eds. J.M. Chan and F. L.F. Lee. London: Routledge.

Solove, D. 2008. *Understanding privacy*. Cambridge, MA: Harvard University Press.

Spiekermann, S., A. Acquisti, R. Böhme, and K.-L. Hui. 2015. The challenges of personal data markets and privacy. *Electronic Markets* 25 (2):161–7. doi:10.1007/s12525-015-0191-0

Suri, H. 2011. Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal* 11 (2):63–75. doi:10.3316/QRJ1102063

Taras, V., P. Steel, and B. L. Kirkman. 2016. Does country equate with culture? Beyond geography in the search for cultural boundaries. *Management International Review* 56 (4):455–87. doi:10.1007/s11575-016-0283-x

Tavani, H. T. 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy* 38 (1):1–22. doi:10.1111/j.1467-9973.2006.00474.x

Taylor, R. D. 2020. "Data localization": The internet in the balance. *Telecommunications Policy* 44 (8):102003. doi:10.1016/j.telpol.2020.102003

Trepte, S., L. Reinecke, N. B. Ellison, O. Quiring, M. Z. Yao, and M. Ziegele. 2017. A cross-cultural perspective on the privacy calculus. *Social Media + Society* 3 (1):1–13. doi:10.1177/2056305116688035

Triandis, H. 1988. Collectivism v. individualism: A reconceptualisation of a basic concept in cross-cultural social psychology. In *Cross-cultural studies of personality, attitudes and cognition*, eds. G. K. Verma, and C. Bagley, 60–95. London: Palgrave Macmillan.

Turner, J. H. 2005. A new approach for theoretically integrating micro and macro analysis. In *The Sage handbook of sociology*, eds. C. Calhoun, C. Rojec, and B. S. Turner, 405–22. London: SAGE.

Van Deth, J. W. 2006. *Equivalence in comparative politics*. London: Routledge.

Van Eeten, M. J., and M. Mueller. 2013. Where is the governance in Internet governance? *New Media & Society* 15 (5):720–36. doi:10.1177/146144481246285

Vasalou, A., A. N. Joinson, and D. Houghton. 2015. Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the Association for Information Science and Technology* 66 (5):918–29. doi:10.1002/asi.23220

Warren, S. D., and L. D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4 (5):193–220. doi:10.2307/1321160

West, S. M. 2019. Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society* 58 (1):20–41. doi:10.1177/0007650317718185

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

Westin, A. F. 2003. Social and political dimensions of privacy. *Journal of Social Issues* 59 (2):431–53. doi:10.1111/1540-4560.00072

Wilson, C., G. Janes, and J. Williams. 2022. Identity, positionality and reflexivity: Relevance and application to research paramedics. *British Paramedic Journal* 7 (2):43–9. doi:10.29045/14784726.2022.09.7.2.43

Wirth, W., S. Kolb, F. Esser, and T. Hanitzsch. 2012. *Handbook of comparative communication research*. Routledge.

Woodruff, A., V. Pihur, S. Consolvo, L. Schmidt, L. Brandimarte, and A. Acquisti. 2014. Would a privacy fundamentalist sell their DNA for $1000 … if nothing bad happened as a result? The Westin categories, behavioral Intentions, and consequences. In *10th Symposium on Usable Privacy and Security*, 1–18. Berkeley, CA: USENIX Association.

Wu, P. F., J. Vitak, and M. T. Zimmer. 2020. A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology* 71 (4):485–90. doi:10.1002/asi.24232

Wu, Y., T. Lau, D. J. Atkin, and C. A. Lin. 2011. A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy* 35 (7):603–16. doi:10.1016/j.telpol.2011.05.002

Zhang, R., N. N. Bazarova, and M. Reddy. 2021. Distress disclosure across social media platforms during the COVID-19 pandemic: Untangling the effects of platforms, affordances, and audiences. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. New York: ACM. doi:10.1145/3411764.3445134

Zuboff, S. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Profile Books.