[Communications of the Association for Information Systems](https://aisel.aisnet.org/cais)

Volume 57 Paper in press

2025

Ethical Information Disclosure: Exploring the Presence-Privacy Tradeoff in GeoMatching Applications for Sustainable Development

Zhenzhen Zhao
SKEMA Business School – Université Côte d'Azur

Damien Renard
Université Catholique de Louvain

Catherine Lejealle
ISC Paris

Thierry Delecolle
De Vinci Research Center

Recommended Citation

Zhao, Z., Renard, D., Lejealle, C., & Delecolle, T. (In press). Ethical Information Disclosure: Exploring the Presence-Privacy Tradeoff in GeoMatching Applications for Sustainable Development. Communications of the Association for Information Systems, 57, pp-pp. Retrieved from https://aisel.aisnet.org/cais/vol57/iss1/73

Communications of the Association for Information Systems

Accepted Manuscript

Ethical Information Disclosure: Exploring the Presence-Privacy Tradeoff in GeoMatching Applications for Sustainable Development

Zhenzhen Zhao
SKEMA Business School
Université Côte d'Azur
0000-0002-3060-074X

Damien Renard
Université Catholique de Louvain
0000-0003-2171-1031

Catherine Lejealle
ISC Paris
0000-0002-7361-4674

Thierry Delecolle
De Vinci Higher Education
De Vinci Research
0000-0001-5926-6573

Please cite this article as: Zhao, Z., Renard, D., Lejealle, C., & Delecolle, T. (in press). Ethical Information Disclosure: Exploring the Presence-Privacy Tradeoff in GeoMatching Applications for Sustainable Development. *Communications of the Association for Information Systems.*

Communications of the Association for Information Systems

Special Section Paper ISSN: 1529-3181

Ethical Information Disclosure: Exploring the Presence-Privacy Tradeoff in GeoMatching Applications for Sustainable Development

Zhenzhen Zhao
SKEMA Business School
Université Côte d'Azur
0000-0002-3060-074X

Damien Renard
Université Catholique de Louvain
0000-0003-2171-1031

Catherine Lejealle
ISC Paris
0000-0002-7361-4674

Thierry Delecolle
De Vinci Higher Education
De Vinci Research
0000-0001-5926-6573

Abstract:

This paper examines GeoMatching apps – mobile platforms that connect users based on location for mutual benefits – contributing to the United Nations' Sustainable Development Goals (SDGs) by facilitating access to services, jobs, and resource sharing. However, these apps raise privacy concerns, as users must share personal information. The study explores the tradeoff between the benefits of using GeoMatching apps and the risks of disclosing personal data. It introduces the "presence-privacy tradeoff," where users balance their desire for connection with their reluctance to share information due to privacy risks. The research focuses on how social presence (SP) - the sense of closeness and interaction - influences user attitudes and intentions towards using GeoMatching apps. An experimental study with 410 users compares two algorithmic models (LEIS and HFSD) with differing disclosure requirements, finding that while privacy concerns can hinder usage, SP can moderate these concerns. The study concludes that SP can help overcome privacy barriers, enhancing the potential of GeoMatching apps in supporting sustainability goals.

Keywords: Algorithm, Geolocation, Geomatching, Intrusion into Privacy, Privacy Calculus, Social Presence, Sustainable Development Goals.

[Department statements, if appropriate, will be added by the editors. Teaching cases and panel reports will have a statement, which is also added by the editors.]

[Note: this page has no footnotes.]

This manuscript underwent [editorial/peer] review. It was received xx/xx/20xx and was with the authors for XX months for XX revisions. [firstname lastname] served as Associate Editor.] **or** The Associate Editor chose to remain anonymous.]

1 Introduction

In recent years, there has been growing interest in developing mobile applications that connect two geolocated individuals to meet various business or personal needs. We define GeoMatching apps as *mobile apps that match two geolocated users bounded with mutual benefits based on the presence and display of their profile information*. For instance, Nextdoor links individuals seeking small jobs with households or businesses in need of services, allowing unskilled workers to earn additional income. FallingFruit connects people with surplus food available for free, reducing food waste and fostering community engagement. These apps generally enhance access to services, employment, and resource sharing, reinforcing the collaborative economy.

GeoMatching apps contribute to achieving the United Nations' Sustainable Development Goals (SDGs), such as reducing poverty, eliminating hunger, and promoting decent work. For example, Tinder's use aligns with SDG 3 (*Ensure healthy lives and promote well-being for all at all ages*) and SDG 5 (*Achieve gender equality and empower all women and girls*) (Hammond & Moretti, 2023) — though this relationship remains complex. Similarly, Airbnb was originally proposed with the ethos of the sharing economy and local authenticity (Guttentag et al., 2018), contributing to SDG 1 (*No poverty*) and SDG 8 (*Decent work and economic growth*). Car-sharing platforms such as Zipcar encourage sustainable transport (supporting SDG 9 – *Industry, innovation and infrastructure* – and SDG 13 – *Climate action*). Appendix A provides examples of GeoMatching apps relevant to each of the 17 SDGs and explains their contributions. However, as asserted by the Gartner Group in their 2024 report, "Sustainable IT: Don't Miss These Cost-Effective Opportunities," many companies still underutilize technology to unlock sustainable and cost-effective initiatives. Executives may not always implement the most impactful IT strategies to fully capitalize on these opportunities.[1]

Despite their sustainability benefits, GeoMatching apps raise significant privacy concerns, as users are required to disclose personal information. It is crucial to explore how these technologies, intersecting with broader sustainability objectives, face ethical issues that may hinder the full realization of the SDGs. Specifically, the core functionality of GeoMatching apps relies on users providing self-descriptive profile information to enable effective matching. While this disclosure is essential for optimal matching, users often have limited control over what data is disclosed to unknown users, raising the risk of intrusion into privacy (IP). This disclosure process is largely shaped by the algorithms that drive the system. Although extensive research on online privacy has examined the ambivalence between users' desire and reluctance to disclose personal information—such as the privacy paradox (Norberg et al., 2007) and privacy calculus (Dinev & Hart, 2006)—little is known about users' attitudes when information disclosure is required by algorithms. To advance the sustainable potential of GeoMatching technologies, it is thus crucial to explore the ethical implications of algorithm-driven information sharing.

Additionally, algorithms are increasingly studied in broader technological and ethical contexts. Prior work has emphasized the importance of addressing unforeseen algorithmic threats (Holzinger et al., 2021) and examines how algorithms interact with ecosystems of users seeking compensation for their data and participation (Kotlarsky *et al*., 2023; Schoormann *et al*., 2023). Within these ecosystems, social presence (SP) —defined as the feeling of closeness and others' presence in mediated environments (Short et al., 1976)—emerges as a key construct. Research shows that SP positively influences users' attitudes toward new devices (Gefen & Straub, 2004) and technologies (Hess *et al*., 2009; Tu, 2002). However, its potential role in balancing ethical concerns related to privacy with algorithmic GeoMatching apps remains underexplored. This paper seeks to address that gap. To that end, our first research question asks: *Can SP moderate the ethical dilemmas of privacy and facilitate the achievement of the SDGs?* We introduce the presence–privacy tradeoff, which captures the tension between users' desire to connect through sharing profile information and their simultaneous hesitation due to privacy concerns. This tradeoff is grounded in two core constructs: social presence (SP) and intrusion into privacy (IP). While users recognize the benefits of sharing information for effective matching, they remain concerned about how that information is perceived. We posit that SP may reduce the negative effect of IP, thereby fostering favorable attitudes towards using GeoMatching apps.

This research aims to investigate information disclosure from an algorithmic perspective. Building on the presence-privacy tradeoff, our second research question asks: *How does the level of algorithm-driven*

[1] https://www.gartner.com/en/documents/5473095

disclosure requirement moderate users' attitudes to use GeoMatching apps? To address this, we develop an operationalization of disclosure requirements in the context of GeoMatching algorithms. This includes key processes such as disclosure, search, matching, and learning. For instance, algorithms such as LEIS (Lower disclosure, Exclusive searching, Instant matching, Static learning - e.g., Uber) require minimal personal data and prioritize service-related criteria. In contrast, HFSD algorithms (Higher disclosure, Filtered searching, Selected matching, Dynamic learning - e.g., Tinder) ask users to share more personal information, as matching depends on browsing and selecting profiles. We posit that these algorithmic structures moderate the perceived tradeoff between presence and privacy.

To empirically test our research model, we conducted an experimental study involving 410 users across two treatment conditions, representing two levels of disclosure requirement driven by HFSD and LEIS algorithms. The findings support the presence–privacy tradeoff: while SP enhances user attitudes toward the app, IP undermines them. These attitudes, in turn, significantly influence users' behavioral intentions. Importantly, SP mitigates the adverse effects of IP-when users feel socially engaged by the app, they are more tolerant of privacy risks. However, this mitigating effect is moderated by the level of required disclosure: in high-disclosure settings, the negative impact of IP is magnified, while the benefits of SP are not correspondingly enhanced. These findings emphasize the psychological complexity of user engagement with algorithmic platforms, where perceived interpersonal connection must be carefully weighed against the perceived risks of data exposure. This nuanced understanding is essential for designing ethical GeoMatching systems that align with both user trust and sustainable digital innovation.

The remainder of this paper is structured as follows. First, we provide insights into the theoretical background by discussing online self-disclosure, followed by an introduction to the proposed presence-privacy tradeoff, GeoMatching algorithms, and the research model along with the associated hypotheses. The next section outlines the methodology, including the testing of the research model and the presentation of the results. Finally, the paper concludes with a discussion of the theoretical and managerial implications, addresses the limitations of the research, and offers suggestions for future studies.

2 Literature Review and Theoretical Background

In the following, we first present the literature on online self-disclosure, followed by our conceptualization of the presence-privacy tradeoff and GeoMatching algorithms, to ensure a common understanding of these concepts.

2.1 Online Self-Disclosure Literature: From User to Algorithm Perspective

Online self-disclosure refers to the act of sharing individuals' private information or personal preferences through online platforms (Shih *et al*., 2017). Despite the privacy risks associated with self-disclosure in online settings, users continue to reveal personal details in their communications and exchanges (Kordzadeh & Warren, 2017; Larson, 2023). This seemingly contradictory behavior is often motivated by the expectation of tangible benefits (e.g., Xu *et al*., 2009) or intangible rewards (e.g., Dinev & Hart, 2006; Krasnova *et al*., 2010; Xu *et al*., 2010). Research on online information disclosure spans various contexts, including online social networks (e.g., Chen & Sharma, 2015; Choi *et al*., 2015; Hayes *et al*., 2021; James *et al*., 2015; James *et al*., 2017; Jiang *et al*., 2013; Krasnova *et al*., 2010; Posey *et al*., 2010; Xu *et al*., 2010), personalization (e.g., Awad & Krishnan, 2006; Chellappa & Sin, 2005; Li & Unger, 2012; Shih *et al*., 2017; Sutanto *et al*., 2013; Xu *et al*., 2011), mobile advertising (e.g., Kurtz *et al*., 2021), mobile apps (e.g., Koohikamali *et al*., 2019), and the internet of things (e.g., Kim *et al*., 2022). Various theories, such as privacy calculus (Dinev & Hart, 2006; Dinev *et al*., 2013; Hayes *et al*., 2021; James *et al*., 2015; Jiang *et al*., 2013; Kordzadeh & Warren, 2017; Xu *et al*., 2009), dual calculus (Li, 2012), the privacy paradox (Barnes, 2006; Norberg *et al*., 2007), communication privacy management (Petronio, 2002), and multilevel information privacy (Bélanger & James, 2020), have been applied to these contexts. Table 1 summarizes key research contexts-such as social media, e-commerce, and AI ethics-where privacy-related trade-offs have been examined.

Table 1. Overview of Trade-offs in Various Contexts

Authors	Dimensions tested (independant / dependent variable)	Empirical study and context	Main findings
Larsen, 2023	**IV:** Impulsiveness, Desirability **DV:** Personal information disclosure	N = 2729, adults	Impulsivity correlates with certain privacy concerns; social norm conformity may lead to overstated privacy concerns, which can diverge from actual privacy behaviors.
Kordzaden & Warren, 2017	**IV:** Expected personal outcomes, Expected community outcomes, Affective commitment to virtual community **DV:** Willingness to communicate personal health information	No empirical study, health personal information	Emotional attachment (affective commitment) to online communities directly and indirectly influences personal health information sharing.
Chen & Sharma, 2015	**IV:** Perceived cyber risk **DV:** Self-disclosure extent, Perceived networking assistance, Social influence	N = 822 Facebook users	Attitude formation is influenced by classical conditioning, operant conditioning, and social learning, mediating the relationship between site usage and self-disclosure.
Choi et al., 2015	**IV:** Information dissemination, Network commonality **DV:** Perceived privacy invasion, Perceived relationship bonding	N = 109 Facebook users	Information dissemination and network commonality jointly affect perceived privacy invasion and relationship bonding, which in turn influence avoidance and approach behaviors.
James et al., 2017	**IV:** Perceived severity and susceptibility of others' information exposure through a user's social network activity **DV:** Perceived shared risk of exposing others' information	N = 317 undergraduate students as social network users	Culture, self-concern, and Facebook information disclosure self-efficacy affect risk perceptions, composed of severity and susceptibility of information exposure to others.
James et al., 2015	**IV:** Motivations to disclose (information-seeking, socializing, self-expression, fulfilling social expectations) **DV:** Privacy calculus	Social network users	Privacy calculus constructs shape how users manage different types of information on social networks.
Jiang et al., 2013	**IV:** Perceived anonymity of others, Perceived intrusiveness **DV:** Privacy concerns, Social rewards	N = 215 users of chat rooms	Users employ self-disclosure and misrepresentation to protect privacy; social rewards, perceived anonymity, and intrusiveness affect privacy concerns and behaviors.
Krasniva et al., 2010	(1st step) **IV:** Trust in other members, Trust in social network provider, Perceived control **DV:** Perceived privacy risks (2nd step) **IV:** Convenience, Enjoyment, Self-presentation, Relation building, Perceived privacy risks **DV:** Self-disclosure	N = 259 Facebook users	Disclosure is motivated by relationship maintenance and platform enjoyment; trust and control options mitigate perceived privacy risks.
Posey et al., 2010	**IV:** Convenience, Enjoyment, Self-presentation, Relationship building, Perceived risks **DV:** Self-disclosure	N = 529, 263 were from France and 266 from UK	Positive social influence, reciprocity, and trust increase self-disclosure in online communities; privacy risk beliefs reduce it.
Xu et al., 2010	**IV:** Trust in social ties, Privacy policy, Privacy seals, Privacy-enhancing features, Information privacy concerns **DV:** Perceived information control, Trust in social network owner	No	Privacy behavioral responses, concerns, perceived control, trust in providers and social ties, and organizational interventions play key roles in privacy management.
Xu et al., 2009	**IV:** Compensation, Industry self-regulation, Policy regulation- Disclosure privacy benefits, Intention to disclose personal information **DV:** Disclosure privacy benefits, Disclosure privacy risks	N = 528 users of location based-services	The effectiveness of privacy interventions depends on the information delivery mechanism; financial compensation is more impactful for push-based services.
Kurtz et al.,	**IV:** Perceived benefit, Perceived risk,	N = 294 users	Purchase intentions regarding

2021	Location context quality **DV:** Intention to disclose personal information	in of the Payback mobile app	location-based apps are influenced by user attitudes, perceived benefits and risks, and location context quality.
Koohikamali et al., 2019	**IV:** Initial use, Initial self-disclosure **DV:** Self-disclosure	Social network users	Initial social network use and self-disclosure result from trade-offs between privacy concerns and perceived benefits, which dynamically affect continued use.
Kim et al., 2022	**IV:** Perceived control, Authority over personal information **DV:** Willingness to provide personal information	Internet of things	Users prefer opt-in mechanisms and shared control over personal information; willingness to disclose increases with adequate rewards.
Dinev & Hart, 2006	**IV:** Internet trust, Personal Internet interest, Risk perception **DV:** Decision to disclose personal information	N = 369 e-commerce shoppers	Internet trust and personal interest can outweigh privacy concerns in decisions to disclose information online, despite inhibiting effects of privacy worries.
Dinev et al., 2013	(1st step) **IV:** Anonymity, Secrecy, Confidentially **DV:** Perceived information control (2nd step) **IV:** Perceived benefit of information disclosure, Information sensitivity, Importance of information transparency, Regulatory expectations **DV:** Perceived risk (3rd step) **IV:** Perceived information control, Perceived risk **DV:** Perceived privacy	N = 192 undergraduate students	Perceived information control and risk significantly determine privacy perceptions; risk depends on benefits, information sensitivity, transparency, and regulations.
Barnes, 2006	Issues concerning teens' privacy behavior and parental guidance in relation to the privacy paradox	No	Boundaries between private and public social media spaces are unclear, especially for teens, highlighting the need for improved privacy solutions.
Bélanger & James, 2020	Theory of Multilevel Information Privacy (TMIP) based on Communication Privacy Management and developmental privacy theories	No	Technological factors influence privacy decision-making by affecting social identity, cost-benefit analysis, and normative rules in information management.
Li, 2012	Synthesis of 15 privacy-related theories; identification of privacy trade-offs and dual-calculus models	No	A dual-calculus model integrates multiple theories, recognizing interrelated trade-offs in privacy decision-making.
Norberg et al. 2007	Exploration of the privacy paradox	N = 152 social network users	A privacy paradox exists whereby individuals disclose personal information despite expressing privacy concerns.
Petronio, 2002	Synthesis of literature on online privacy issues	No	Communication Privacy Management theory uses a boundary metaphor to describe how individuals regulate private and public information.
Du & Xie, 2021	Ethical implications of AI-enabled products in relation to corporate social responsibility and consumer privacy	No	AI-enabled products possess multi-functionality, interactivity, and varying intelligence stages, each raising ethical concerns including consumer privacy and bias; a multi-level framework is proposed for corporate social responsibility.
Meek et al., 2016	Ethical risks in AI systems and adequacy of embedding ethical decision-making in artificial agents	No	Literature identifies ethical risks in AI including unethical decisions, competition, unpredictability, and privacy concerns, extending to AGI.

Adanyin, 2024	Survey of ethical challenges in AI retail applications, including concerns about privacy and fairness	N = 300 users of e-commerce platforms	Consumers exhibit high concern over personal data collection by AI retail applications, distrust data management, and perceive algorithmic bias, while recognizing AI's potential to improve competitiveness and efficiency without compromising ethics.
Singh et al., 2024	Examination of AI and blockchain integration for consumer data protection	No	AI and blockchain integration present opportunities to enhance consumer data protection on e-commerce platforms.
Dwivedi et al., 2021	Identification of current challenges in AI and proposal of future research directions	No	Ethical challenges of AI include data sharing, system interoperability, and algorithmic discrimination, underscoring the importance of transparency.
Dwivedi et al., 2023a	Exploration of generative AI challenges (e.g., ChatGPT) and proposal of future research directions	ChatGPT	Generative AI poses reputational and legal risks, including privacy loss, fraudulent use, and misinformation, despite its business benefits.

With the rapid rise of online marketing and personalized services, another line of research has focused on the personalization versus privacy paradox (Awad & Krishnan, 2006; Chellappa & Sin, 2005). This paradox highlights the tension between users' desire for personalized services and their instinct to protect their personal information. On one hand, users value personalized offers; on the other hand, they worry about sharing their data with companies (Koh *et al*., 2020; Xu *et al*., 2011). The personalization-privacy paradox has been studied in diverse contexts, including online personalized services (Chellappa & Sin, 2005), personalized advertising (Awad & Krishnan, 2006; Sutanto *et al*., 2013), location-based services (Xu *et al*., 2009), location-based marketing (Xu *et al*., 2011), and ubiquitous commerce (Sheng *et al*., 2008). Table 2 summarizes the key contexts in which personalization-privacy paradox has been studied.

Table 2. Overview of Personalization–Privacy Paradox in Various Contexts

Authors	Dimensions tested (independant / dependent variable)	Empirical study and context	Main findings
Hayes et al., 2021	**IV:** Personalization **DV:** Perceived benefits of information disclosure, Perceived risks of information disclosure, Perceived value of information disclosure	N = 248 Facebook and Twitter US users	Strong consumer–brand relationships enhance the perceived value of information disclosure by increasing perceived benefits and reducing perceived risks; in contrast, perceived risks dominate privacy decisions in weaker relationships.
Sheng et al., 2008	**IV:** Personalization, Situation **DV:** Perceived privacy risks, Willingness to engage in ubiquitous commerce services	Ubiquitous commerce, experiment with scenario-based approach	The impact of personalization on privacy concerns and adoption intentions is context-dependent, with situational factors shaping customer perceptions and engagement with ubiquitous commerce services.
Sutanto et al., 2013	(1st step) **IV:** Perceived effectiveness of privacy-safe feature **DV:** Perceived intrusion to information boundary, Perceived personalization benefits (2nd step) **IV:** Perceived intrusion to information boundary, Perceived personalization benefits **DV:** Psychological comfort with the application (3rd step) **IV:** Psychological comfort with the application	N = 113 Field experiment non-personalized application and a personalized, non-privacy-safe application that transmitted user information to a central	Personalized applications increase usage compared to non-personalized versions; however, privacy-preserving personalization also enhances content engagement, indicating that privacy protection strengthens user satisfaction.

	DV: Intention to save advertisements (reflecting content gratification	server.	
Chellapa et al., 2013	**IV:** Perceived value of personalization, Privacy control, Trust-building factors **DV:** Likelihood of using personalization services	N = 243 users of five popular online industry categories	Trust in the vendor positively influences consumers' intention to use personalized services, suggesting that building trust can mitigate privacy concerns and promote engagement.
Awad & Krishnan, 2006	**IV:** Previous experiences of online privacy invasion, Privacy concerns, Importance of privacy policies, Willingness to be profiled online for personalized advertising and services, Importance of information transparency **DV:** Importance of information transparency	N = 523 from from the Digital Research, Inc. (DRI) Family Panel.	Consumers who prioritize information transparency are less willing to be profiled, creating a challenge for firms aiming to provide transparency while relying on user profiling.

In this research, we introduce the concept of the presence-privacy tradeoff, which refers to privacy concerns that arise between users (social privacy) in a computer-mediated environment, as opposed to the privacy concerns between users and firms (institutional privacy). While much of the existing research on privacy focuses on user perspectives, few studies have examined the role of technology or mechanisms driving privacy concerns. Responding to calls for more research on the impact of new technologies on privacy (Chan *et al*., 2005), scholars have begun exploring how technological features affect privacy. For instance, Xu *et al*. (2009) investigate the roles of different information delivery mechanisms in enhancing the effectiveness of privacy interventions within location-based services.

We shift the focus from users to algorithms by examining how disclosure requirements, shaped by the type of algorithm employed, moderate the presence-privacy tradeoff, specifically, by influencing the effects of SP and IP on users' attitudes and intentions to use GeoMatching apps. This research extends the current understanding of privacy concerns by exploring the intersection of algorithmic design and user behavior in the context of social privacy.

2.2 Presence-Privacy Tradeoff and Core Concepts

In this section, we present our conceptualization of the presence-privacy tradeoff. With the rise of the internet, computer-mediated communication (CMC) has become increasingly popular, creating an extensive social world, often termed cyberspace (Walther, 1992). The difference between face-to-face and CMC lies in the types of information shared. While face-to-face interactions provide rich nonverbal and paralinguistic cues, CMC is comparatively "silent" (Herring, 1996). In face-to-face settings, individuals use these cues to decide whom to trust, but in an online context, users often begin in a state of mistrust (Sztompka, 1999). By interpreting personal information, users classify profiles and decide whether to engage. While such disclosure reduces ambiguity and uncertainty, it also raises privacy concerns. We suggest that the result is what we call the *presence-privacy tradeoff, defined as the dilemma between users' desire to disclose profile information to establish computer-mediated connections and their reluctance to reveal such personal information*. Although the presence–privacy tradeoff is developed in the context of GeoMatching, it captures a generalizable tension relevant to a wide range of digital systems that rely on user profiling and algorithmic matching.

The key difference between the presence-privacy tradeoff and the personalization-privacy paradox (Awad & Krishnan, 2006; Chellappa & Sin, 2005) lies in context, data recipient, and user motivation. The personalization–privacy paradox typically arises in user-to-firm contexts (e.g., e-commerce or advertising), where users share data to obtain personalized recommendations or services. In contrast, the presence–privacy tradeoff occurs in computer-mediated connection-seeking, where users disclose information to be visible or connect with other individuals—not to firms. The recipient of the information thus shifts from organizations to other users, and the user motivation changes from seeking personalization to establishing presence and connections.

This distinction also reflects different sources of privacy risk. In the personalization–privacy paradox, privacy concerns stem from how firms collect and use data (institutional privacy). In the presence–privacy tradeoff, concerns focus on social privacy, namely how personal information is exposed and perceived by other users. For instance, Raynes-Goldie (2010) observed that users may fear social exposure more than institutional surveillance.

Therefore, while our work is conceptually inspired by the personalization–privacy paradox, it introduces a novel theoretical framing by adapting the logic of privacy tradeoffs to algorithmically mediated, peer-to-peer matching contexts. Given this distinction, it is crucial to explore how social privacy concerns, embedded in the presence-privacy tradeoff, affect users' attitudes and intentions to use (IU). The following subsections introduce two key concepts related to the presence-privacy tradeoff: social presence (SP) and intrusion into privacy (IP). These concepts help explain how the tradeoff between presence and privacy shapes user intention to engage in online interactions.

2.2.1 Social Presence

The concept of social presence (SP) is a key component in the proposed presence-privacy tradeoff. Initially developed by Short *et al*. (1976), SP theory examines how the social context influences the use of a communication medium. SP is closely related to media richness theory (Daft & Lengel, 1983, 1986), which categorizes communication channels by their ability to effectively convey meaning and resolve ambiguity (richer media are more capable of clarifying complex or unclear messages).

SP theory focuses on the extent to which a medium allows a communicator to perceive their interaction partners as psychologically present during computer-mediated communication (Short *et al*., 1976). Media are classified based on how well they allow communicators to express intimacy, warmth, and establish personal connections. A higher level of SP indicates that the medium fosters a sense of personal, sociable, and sensitive human contact (Short *et al*., 1976) - for example, face-to-face interactions or video conferencing. In contrast, lower SP is typically found in less immediate forms of communication, like email (Gefen & Straub, 2004).

Research shows that the perception of SP positively influences attitudes towards adopting new devices (Gefen & Straub, 2004) and technologies (Hess *et al*., 2009; Tu, 2002).

2.2.2 Intrusion into Privacy

A high degree of SP can help clarify ambiguity and uncertainty, but it can also lead to increased privacy concerns. Privacy is defined by Westin as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (1967, p. 7). Related interpretations include "freedom from unwanted intrusions by others" (Foxman & Kilcoyne, 1993, p. 107) and an individual's "right to be let alone" (Brandeis & Warren, 1890, p. 193). There are numerous philosophical, legal, behavioral, and everyday definitions of privacy (Margulis, 2011), leading to the conclusion that it is an elusive and elastic concept (Allen, 1988; Dinev *et al*., 2013). Scholars have developed diverse theories and measures of privacy (e.g., Altman, 1990; Westin, 1967; Petronio, 2002), but there is no consensus on specific theories or measures (Norberg *et al*., 2007). Researchers are advised to select a particular theory of privacy based on the specific requirements of their study (Margulis, 2011).

In this research, we employ the concept of intrusion into privacy (IP) to represent the privacy dimension within our proposed presence-privacy tradeoff. IP is conceptualized as the invasion of an individual's solitude (Teeter & Loving, 2001) and is frequently used in contexts involving technology. Existing literature confirms that the notion of intrusiveness can be applied to mobile app contexts (Wottrich *et al*., 2018). In this article, we utilize scales of intrusiveness to measure such intrusion. In traditional media, intrusiveness - especially in advertising - is considered a common issue that impedes user goals (Li *et al*., 2002) and helps explain why users often find advertising irritating (Edwards *et al*., 2002). Beyond advertising, intrusiveness can be defined as "the degree to which a person deems the presentation of information as contrary to his or her goals" (Edwards *et al*., 2002, p. 85).

In our study, we aim to understand how the two dimensions of the presence-privacy tradeoff - SP and IP - affect users' attitudes and intentions towards using GeoMatching apps, as well as how these dynamics are moderated by the level of disclosure required by two different GeoMatching algorithms.

2.3 GeoMatching Algorithms Conceptualization

To facilitate connections, users must disclose self-descriptive profile information. While information disclosure is crucial, users often do not have full control over what they share. Insufficient disclosure of private information can hinder the functionality of these matching apps. The level of personal information disclosed is influenced by the algorithms employed by the app, which can either enable or restrict the amount of information shared. This study conceptualizes GeoMatching algorithms as progressing through four key phases: disclosing, searching, matching, and learning. The first phase, disclosing, involves varying levels of information disclosure. Some apps require minimal disclosure (lower disclosing, e.g., Uber), while others permit extensive disclosure (higher disclosing, e.g., Tinder). For instance, Uber requires users to share their geolocation, while Tinder allows users to disclose their geolocation, gender, age, sexual orientation, photos, hobbies, and partner preferences. The second phase pertains to searching. Some apps use geolocation as the sole criterion for searches (exclusive searching, e.g., Uber), while others enable users to search based on additional criteria (filtered searching, e.g., Tinder allows age and gender selections). The third phase relates to matching mechanisms. GeoMatching apps can provide real-time matching services, differing in whether they employ instant matching or selected matching based on user intervention. Uber employs instant matching, automatically pairing drivers and passengers without user choice, whereas Tinder utilizes selected matching, allowing individuals to choose from a list of potential matches. The final phase involves learning, where the algorithm interprets and learns from extracted data to achieve specific objectives (i.e., artificial intelligence). Dynamic learning refers to a personalized matching algorithm that adapts based on users' previous choices and preferences. For example, Tinder learns user preferences (e.g., age group, hobbies) based on prior swipes, enabling the display of more relevant matches. In contrast, static learning describes a fixed matching algorithm, such as Uber's, which does not integrate machine learning capabilities at the matching level.

It is important to note that these four phases of algorithms are interconnected. For instance, when the disclosing scheme permits users to share more personal information, it enables the searching scheme to utilize criteria beyond just location. Consequently, the matching process tends to be more manually selected rather than automated, and the learning scheme is often more dynamic than static. Thus, we can categorize two types of GeoMatching algorithms: the LEIS algorithm, characterized by lower disclosing, exclusive searching, instant matching, and static learning, and the HFSD algorithm, characterized by higher disclosing, filtered searching, selected matching, and dynamic learning. Figure 1 illustrates these two types of GeoMatching algorithms.

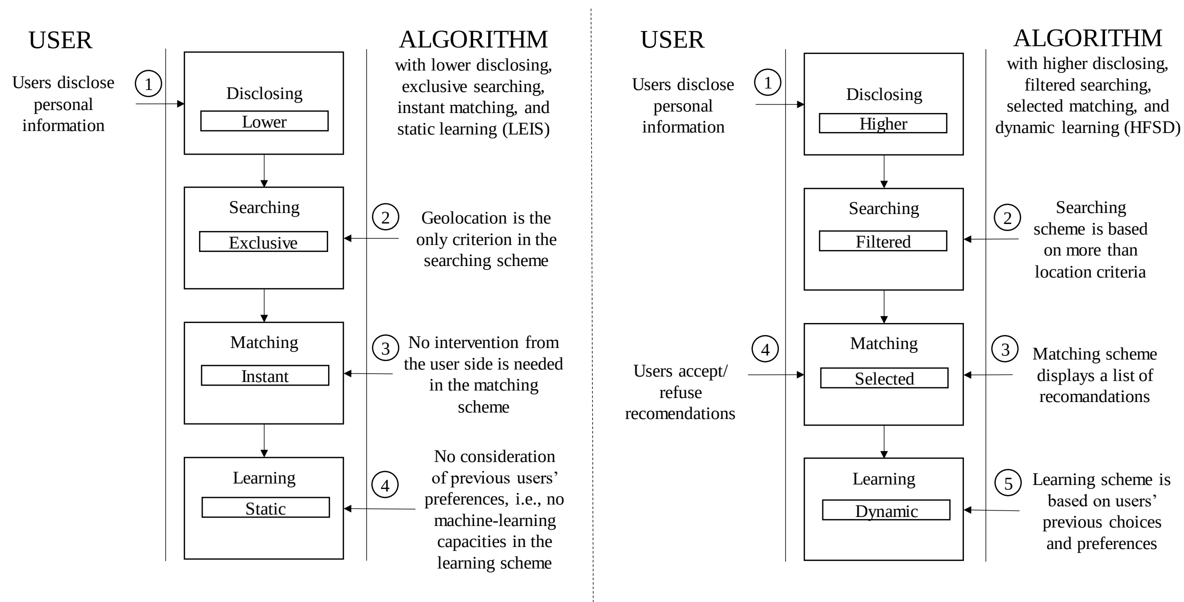


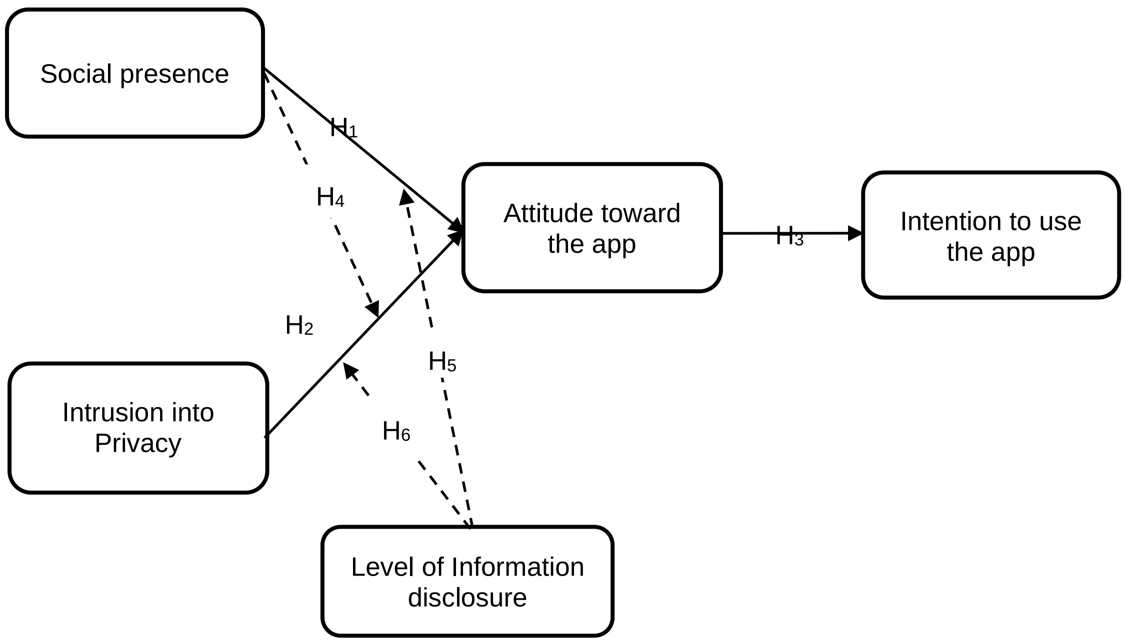
Figure 1. GeoMarching Algorithms

In summary, the proposed GeoMatching algorithms regulate the level of user information required for disclosing, searching, matching, and learning. Among these four sequential phases, the level of disclosure requirement is the critical factor that enables the other three phases to function effectively. In this research, information disclosure operates as a contextual factor that moderates how users perceive and respond to social presence and privacy intrusion in shaping their attitudes and intentions. The next section will present the research model and associated hypotheses.

3 Research Model and Hypothesis Development

This study investigates the presence–privacy tradeoff—captured through SP and IP—and examines how disclosure requirements, prompted by two types of algorithms, moderate these elements on users' attitudes and intentions to use GeoMatching apps. The research model is illustrated in Figure 2, and six hypotheses are outlined below.

Figure 2. Conceptual Framework



3.1 Social Presence and Attitude Towards Using GeoMatching

According to SP theory, the significance of SP is contingent upon the contextual requirements (Song *et al*., 2008). The necessity for SP varies across different situations. In the context of our research, we argue that GeoMatching apps necessitate psychological connections and a sense of human warmth. Prior studies have demonstrated that a higher level of SP in social commerce positively influences user trust in shopping sites and enhances the enjoyment experienced, which in turn fosters more favorable user attitudes (Hassanein & Head, 2007). Similarly, we posit that in the context of GeoMatching, SP is positively associated with users' attitudes toward use (AU).

Hypothesis 1: In GeoMatching apps, SP has a positive effect on AU.

3.2 Intrusion in Privacy and Attitude Towards Using

The detrimental effects of privacy concerns on user attitudes have been empirically validated in various privacy contexts, including both institutional privacy (e.g., Chellappa & Sin, 2005; Malhotra *et al*., 2004) and social privacy (e.g., Child *et al*., 2009). In the context of GeoMatching, if the matching process induces users' concerns about intrusion into their privacy when providing personal information, it is likely to result in decreased AU. Therefore, we hypothesize a similar negative correlation:

Hypothesis 2: In GeoMatching apps, IP has a negative effect on AU.

3.3 Attitude and Intention to Use

Attitude is defined as "a mental and neural state of readiness, organized through experience, exerting a directive or dynamic influence upon an individual's response to all objects and situations with which it is related" (Allport, 1935, p. 810). Understanding attitudes provides insights into the preferences and behaviors of individuals and groups (Allport, 1935). Building on this foundational work, scholars agree that attitudes are evaluative tendencies that encompass cognitive, affective, and behavioral antecedents and consequences (Albarracín, 2005; Eagly & Chaiken, 1993, 2007). Consequently, we hypothesize that a direct relationship exists between attitude and intention to use (IU):

Hypothesis 3: In GeoMatching apps, AU has a positive effect on IU.

3.4 Interaction Effect Between Social Presence and Intrusion in Privacy

In computer-mediated communications, SP is characterized by the sensation of human contact, sensitivity, and sociability. To mitigate privacy concerns, users must feel a sense of closeness and the presence of others. This assumption aligns with social conformity theory, which posits that individuals are more inclined to disclose information when they observe others doing the same (Ash, 1956; Bond & Smith, 1996; Chen & Sharma, 2015; Nord, 1969). In the context of GeoMatching, we argue that the more personal and relatable users perceive these apps to be, the more likely they are to experience reduced concerns about IP and to develop a positive AU. Thus, we formally hypothesize:

Hypothesis 4: In GeoMatching apps, a tradeoff exists between SP and IP, such as SP increases (decreases), the negative effect of IP on AU decreases (increases).

3.5 Level of Disclosure Requirement as Moderator

In GeoMatching apps, where users share personal and location-specific information to connect with others nearby, the level of self-disclosure requirement can amplify how they respond to the attitudes towards the app. When users are required to disclose more, they tend to feel more emotionally invested and socially exposed. In this context, SP features—such as personalized messages, visible user activity, or real-time chat—become more psychologically significant. The more users disclose, the more they may rely on these cues to feel seen and connected, which can amplify the positive impact of SP on their overall attitudes towards the app (Short *et al*., 1976; Gefen & Straub, 2004). On the other hand, high disclosure requirement can also heighten users' sensitivity to privacy threats. According to communication privacy management theory (Petronio, 2002), individuals manage private information through negotiated boundaries, and when more personal data is shared, these boundaries become more fragile. Thus, any perception of privacy intrusion-such as unclear data practices or lack of user control—can feel more severe and damaging (Xu *et al*., 2009; Dinev & Hart, 2006).

Hypothesis 5: In GeoMatching apps, the positive effect of SP on AU is stronger in the higher disclosure condition (compared to lower disclosure condition).

Hypothesis 6: In GeoMatching apps, the negative effect of IP on AU is stronger in the higher disclosure condition (compared to lower disclosure condition).

4 Methodology

4.1 Research Design and Procedure

We conducted a between-subjects online experiment. The objective was to test the effects of perceived social presence (SP) and intrusion into privacy (IP) on attitude toward the app (AU) and intention to use the app (IU), and to examine whether these effects differ depending on the level of algorithmic disclosure. We operatively implemented the level of information disclosure through two app conditions: HFSD (high-disclosure) and LEIS (low-disclosure), based on how much personal data the algorithm requires.

A pre-test was conducted with 54 students to ensure that the HFSD interface was perceived as significantly more disclosive than the LEIS one. The participants were randomly assigned to one of two different diagrams of algorithms corresponding to two app mockups (Diagrams and mockup examples are illustrated in the Appendix B). Participants were then asked to rate the perceived level of data disclosure required by the algorithm using a 5-point Likert scale adapted from Koohikamali et al. (2019), with items such as, "This algorithm asks the user to provide a limited amount of personal information, using minimal personal data aside from geolocation data." An analysis of variance (ANOVA) confirmed the effectiveness of the manipulation. Participants exposed to the high-disclosure condition (HFSD) reported significantly greater perceived data disclosure (M = 4.27) than those in the low-disclosure condition (LEIS) (M = 2.86), $F(1,52) = 36.70$, $p < .001$.

4.2 Data Collection

Next, we recruited a total of 420 participants from a community created by an innovation-focused company. We randomly assigned the participants to two treatment conditions (groups). In group 1, the respondents were invited to answer a questionnaire after using the mockup of the online dating app presented in the pretest. In group 2, the respondents were invited to answer questions after experiencing the mockup of the ride-hailing app presented in the pretest.

In total, 207 users for group 1 and 203 users of group 2 were retained after samples with missing or erroneous data were removed. Demographic characteristics are consistent for both groups: there were 65% women (Group 1) and 62% women (Group 2) with an average age of 30 years (Group 1) and 29 years (Group 2). Samples collected are in line with other studies. The social app category is more used among female users (Seneviratne *et al*., 2015), and based on a study run by INSEE (2019), the most representative user of mobile phones with internet services is aged between 25-39 years.

4.3 Measurement and Group Comparisons

We developed measurement scales for the constructs based on the literature review and adapted them to fit our context. Attitude (AU) and intention to use (IU) were embedded in a five-point scale adapted from Venkatesh *et al*. (2003), which is widely used in the domain of information systems. Intrusion into privacy (IP) was measured using a five-point scale adapted from Li *et al*. (2002), while social presence (SP) was assessed using a five-point scale adapted from Gefen and Straub (2004). All scales were translated into French and checked by three bilingual speakers of English and French. Minor changes in wording were made for some of the items to improve comprehension. Back-translation was performed in the final step to ensure that the minor changes enhanced the scales' clarity.

Although disclosure was not directly measured in the main study, we conducted independent-sample t-tests to assess whether the manipulation influenced SP and IP perceptions. Table 3 reports the descriptive statistics and group comparisons. Participants in the HFSD condition reported a significantly higher SP ($t = 2.45$, $p = .015$) and significantly higher IP ($t = 5.10$, $p < .001$) compared to the LEIS condition. These results provide empirical support for the salience of the manipulation and help contextualize the tradeoff effect tested in the structural model.

Table 3. Group Comparisons

	Level of Information disclosure		**t**	***p*-value**
	Low	High		
Social Presence	3.65	3.89	2.45	0.015
Intrusion into Privacy	2.80	3.45	5.10	0.000

4.4 Measurement Model Assessment

We employed Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4. PLS-SEM was selected due to the model's complexity, the inclusion of mediation and moderation effects, the sample size, and the exploratory nature of the study (Hair et al., 2022). The primary objective was prediction and theory building rather than theory confirmation, making PLS-SEM preferable over CB-SEM. Bootstrapping with 5,000 resamples was used to estimate path coefficients, significance levels, and confidence intervals. The model hypothesizes that algorithm disclosure affects AU via two mediators: SP and IP. AU then influences IU. An interaction term (SP × IP) was introduced to test a possible trade-off effect, in line with recent theorizing on privacy–presence dualities.

Table 4 summarizes the measurement items and presents the statistics for each construct. We assessed reliability and validity using Cronbach's alpha (α), Composite Reliability (CR), and Average Variance

Extracted (AVE). All constructs demonstrated good internal consistency with α and CR values exceeding .70, and convergent validity with AVE values above .50 (Fornell & Larcker, 1981). Indicator loadings ranged from .81 to .91, well above the recommended threshold of .70, indicating strong indicator reliability.

Table 4. Loadings of Indicator Constructs

Construct	AVE	CR	α	Loadings	Item Wording
AU	0.619	0.829	0.712	0.905 0.850 0.810	Using this app is a good idea. Using this app is fun. I like using this app.
IU	0.889	0.958	0.936	0.943 0.949 0.940	I intend to use this app in the future. I predict I will use this app in the future. I plan to use this app in the future.
SP	0.869	0.952	0.928	0.914 0.933 0.925 0.929	There is a sense of human contact in this app. There is a sense of sociability in this app. There is a sense of human warmth in this app. There is a sense of human sensitivity in this app.
IP	0.824	0.930	0.892	0.879 0.911 0.906 0.899	This app is invasive to my solitude. This app is interfering with my solitude. This app is obtrusive to my solitude. This app is intrusive to my solitude.

Note: α = Cronbach's alpha; CR = Composite Reliability; AVE = Average Variance Extracted

Discriminant validity was assessed using the Fornell–Larcker criterion. For each construct, the square root of the AVE exceeded its correlations with other constructs, suggesting satisfactory discriminant validity (Table 5). This indicates that each latent construct captures distinct phenomena within the measurement model.

Table 5. Discriminant Validity – Fornell-Larcker Criterion

Construct	AU	IU	SP	IP
AU	**0.787**			
IU	0.605	**0.943**		
SP	0.488	0.507	**0.932**	
IP	-0.566	-0.471	-0.440	**0.907**

Note: Diagonal elements in bold represent the square root of AVE. Off-diagonal values are inter-construct correlations.

5 Results

The model demonstrated acceptable explanatory and predictive power. Specifically, it explained 18.1% of the variance in attitude toward the app (R^2 = 0.181) and 19.6% of the variance in intention to use (R^2 = 0.196), both of which represent moderate levels according to Chin (1998). Predictive relevance was confirmed using Stone-Geisser's Q^2, with positive values obtained for both attitude (Q^2 = 0.120) and intention (Q^2 = 0.144), indicating that the model has satisfactory out-of-sample predictive ability. The standardized root mean square residual (*SRMR*) was 0.065, which is below the 0.08 threshold, suggesting acceptable model fit. All variance inflation factors (*VIFs*) were below 3.3, confirming the absence of multicollinearity concerns.

Table 6. PLS-SEM Results

	Path	Beta	t-value	Result
Main paths				
H1	Social Presence → Attitude toward the app	0.315***	4.576	Supported
H2	Intrusion into Privacy → Attitude toward the app	-0.316***	3.894	Supported
H3	Attitude toward the app → Intention to use the app	0.443***	8.524	Supported
Moderating effects				
H4	Social Presence x Intrusion into Privacy → Attitude toward the app	0.154***	3.083	Supported
H5	Social Presence x Level of Disclosure Information → Attitude toward the app	-0.056 ns	0.544	Not supported
H6	Intrusion into Privacy x Level of Disclosure Information → Attitude toward the app	0.233**	1.990	Supported
Control variables				
Age	Age → Attitude toward the app	0.075**	1.873	Significant
Frequency of use	Frequency of use → Attitude toward the app	0.107*	2.084	Significant
Gender	Gender → Intention to use the app	-0.024 ns	0.241	Not Significant
Note: Significance level at ***: p-value < 0.0001; **: p-value <0.01; *: p-value <0.05; ns: non-significant				

The structural model results are presented in Table 6. All hypothesized main effects were supported. All hypothesized main effects were supported. Specifically, social presence had a significant positive effect on users' attitude toward the app (β = 0.315, t = 4.576, p < 0.001, f^2 = 0.046), supporting **H_1**. Similarly, intrusion into privacy negatively influenced attitude (β = –0.316, t = 3.894, p < 0.001, f^2 = 0.045), confirming **H_2**. In line with **H_3**, attitude toward the app significantly predicted intention to use (β = 0.443, t = 8.524, p < 0.001, f^2 = 0.244). The model also tested three moderation effects. Supporting **H_4**, the interaction between social presence and intrusion into privacy was positive and significant (β = 0.154, t = 3.083, p < .01). As illustrated in Figure 3, social presence moderates the effect of privacy intrusion such that its negative impact on attitude is attenuated when social presence is high. In contrast, **H_5** was not supported; the interaction between social presence and disclosure was nonsignificant (β = –0.056, t = 0.544, *n.s.*). Interestingly, the interaction between intrusion into privacy and disclosure was positive and significant (β = 0.233, t = 1.990, p < 0.05), supporting **H_6**, and suggesting that the negative effect of intrusion was more pronounced under high disclosure. Among the control variables, age (β = 0.075, t = 1.873, p < 0.05) and frequency of app use (β = 0.107, t = 2.084, p < 0.05) had significant effects on attitude, while gender had no significant effect on intention to use (t = 0.241, *n.s.*).

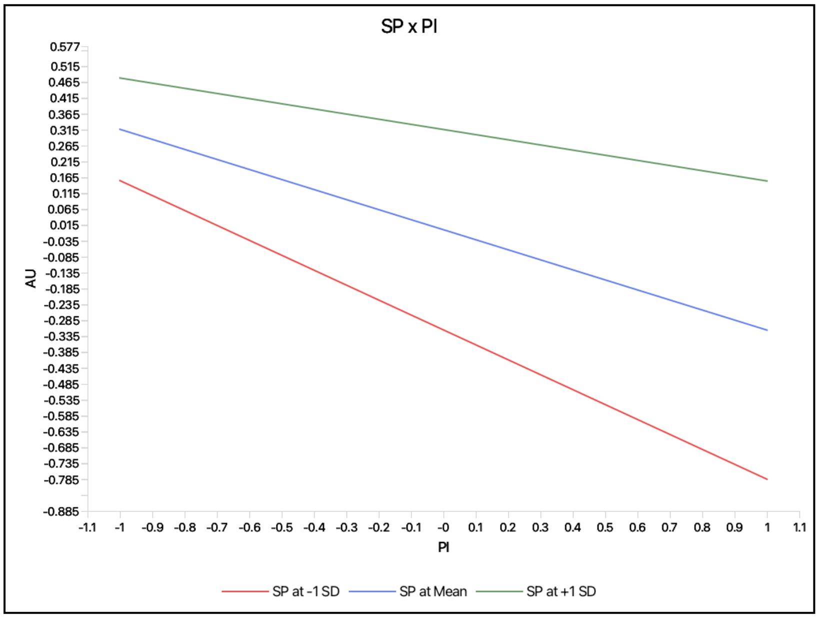


Figure 3. Moderating Effect of Social Presence on Privacy Intrusion

6 Discussion

6.1 Theoretical Contributions

Privacy concerns represent one of the most significant ethical, legal, social, and political issues of the information age (Bélanger & Crossler, 2011; Dinev, 2014; Dinev *et al*., 2013; Hong & Thong, 2013; Li, 2011; Pavlou, 2011; Smith *et al*., 2011), and they are central to information systems research (Lowry *et al*., 2017). Users who frequently engage with apps, or who have used them for extended periods, continue to express privacy concerns (Goncalves *et al*., 2014). In this context, this research offers several key theoretical contributions. A primary contribution of this study is the conceptualization of the presence-privacy tradeoff, which reflects individuals' simultaneous desire and reluctance to display their self-descriptive profile information. While extensive research has focused on information disclosure and privacy concerns through various theories (e.g., privacy calculus, risk calculus, privacy paradox, personalization-privacy paradox), our conceptualization emphasizes the significance of presence in computer-mediated communications. In the absence of nonverbal or paralinguistic cues, the visibility of a profile is crucial for mitigating user mistrust. The presence of personal information can diminish uncertainty and enhance transparency, but it concurrently heightens concerns regarding social privacy. The findings from our empirical study affirm that this presence-privacy tradeoff is operational in the context of GeoMatching, demonstrating that both dimensions - social presence (SP) and intrusion into privacy (IP) - significantly influence individuals' attitudes towards using GeoMatching apps. To be more specific, the strong positive relationship between SP and attitude aligns with SP theory (Short *et al*., 1976), suggesting that users are more comfortable and receptive when they perceive human-like cues. This highlights the emotional and relational dimensions of technology acceptance. The negative effect of IP on attitude supports the privacy calculus theory (Culnan & Armstrong, 1999; Dinev & Hart, 2006), which posits that users weigh benefits against risks. Intrusive data practices damage user trust and result in negative attitudes. The finding also confirms that a favorable attitude is a critical antecedent to behavioral intention.

Another contribution stems from the significant interaction effect between SP and IP. This finding emphasizes the compensatory role of SP in mitigating the negative impact of IP on attitude. Specifically, despite the utilization of different algorithms, the sense of closeness and the perceived presence of others diminish the adverse effects of social privacy concerns. This observation bears important implications for SP theory, suggesting that the warmth and sensitivity conveyed by personal information (e.g., a user's photo) can alleviate IP, indicating that self-descriptive profiles can serve dual purposes: representing potential privacy threats while also offering reassurance.

The third contribution lies in our exploration of moderating effects from an algorithmic perspective, diverging from the user-centric focus typical in existing research streams. Limited studies have investigated how technology or algorithms impact privacy concerns. We propose an operationalization of information disclosure within GeoMatching apps through various algorithmic phases: disclosing, searching, matching, and learning. Users adjust their perceptions of SP and IP based on the level of information disclosure enabled by these algorithms. As disclosure increases, users may become more responsive to both relational cues and privacy threats, thereby moderating the impact of SP and IP on their attitudes toward the app.

Contrary to expectations, the high-disclosure condition did not enhance the positive effect of SP on attitude. This result is noteworthy as it challenges the assumption that relational features are always more powerful when users are more personally invested. This may be explained by several interrelated psychological mechanisms. First, users may experience emotional saturation or a ceiling effect, where the baseline impact of social presence is already high, and additional disclosure yields diminishing returns (Lim & Benbasat, 2000). Second, heightened disclosure could trigger cognitive dissonance or risk aversion, as users may perceive social cues as attempts to increase trust while simultaneously feeling vulnerable about revealing personal data—leading to ambivalence or resistance (Joinson, 2001; Malhotra *et al.,* 2004). Third, a mismatch between social cues and the nature of disclosed information may weaken emotional engagement. If social presence features (e.g., chatbots, emojis) are perceived as superficial or misaligned with the sensitivity of personal disclosures, users may not feel genuinely reassured (Nowak & Biocca, 2003). Together, these dynamics may help explain why greater personal disclosure does not always strengthen the influence of social presence on user attitudes in GeoMatching apps.

As expected, the negative effect of IP on attitude is stronger in the higher-disclosure condition. When users disclose more personal information, they become more vigilant and defensive, amplifying the psychological weight of privacy concerns. This aligns with boundary regulation theory (Altman, 1975) and communication privacy management (CPM) theory (Petronio, 2002), both of which emphasize that individuals actively manage the flow of private information and adjust their openness based on perceived risks. In high-disclosure contexts, users experience a sense of vulnerability; thus, any perceived privacy violation feels more intrusive and threatening, leading to stronger negative attitudes.

Finally, beyond the specific case of GeoMatching, this research contributes to a broader understanding of how perceived social presence and algorithmic disclosure requirements influence user engagement in digitally mediated environments. The presence–privacy tradeoff identified in this study offers a conceptual lens that is applicable to a wide range of algorithm-driven platforms -including those in mobility, healthcare, education, and recruitment - where user profiling, social connection, and ethical concerns must be carefully balanced. More broadly, this work advances the literature on emerging technologies, a field that has only recently begun to examine how operational-level mechanisms influence privacy perceptions and, ultimately, the realization of the SDGs. Emerging technologies are inherently malleable and convergent (Brey, 2017; Moor, 2005), enabling the development of novel services that simultaneously create complex political, technological, economic, legal, and ethical challenges. In computer-mediated environments, algorithms serve not only as technical tools but also as normative agents that shape user behavior and institutional practices. Within the sustainability context—which includes social, environmental, and economic dimensions (Elkington, 1997)—this research highlights how digital innovations, such as algorithmically mediated ecosystems, can either hinder or facilitate progress toward the SDGs (Corbett et al., 2023). By examining how user-to-user interactions are governed by algorithmic disclosure logic, we provide insights into how ethical tensions might be managed in pursuit of sustainable digital transformation (Kotlarsky *et al*., 2023).

6.2 Managerial Implications

From a managerial perspective, this study offers several key implications. By addressing privacy concerns through a well-calibrated presence-privacy tradeoff, GeoMatching apps can help build a foundation of trust, aligning with SDG 16 (Peace, Justice, and Strong Institutions) by promoting ethical and accountable practices in technology design. This insight is transformative for marketers and product designers: SP serves as a counterbalance to privacy concerns and positively influences users' attitudes towards GeoMatching apps, enabling them to engage with less reluctance. Therefore, when designing GeoMatching apps, designers and policymakers should intentionally design for social presence to enhance user engagement and trust. App developers should prioritize the integration of features that foster a sense of human contact, warmth, and sensitivity, utilizing a diverse range of media forms. These practices not only enhance user experience but also foster an ethical approach to data collection and user engagement, reinforcing trust and inclusivity in digital spaces. On the other hand, practitioners must prioritize privacy-by-design principles, ensuring transparency, data minimization, and user control to prevent negative reactions. Clear privacy policies and opt-in data settings can mitigate risk perception.

Moreover, our research illustrates how two types of GeoMatching algorithms moderate the effects of presence-privacy tradeoff on users' attitudes and intentions to use. Developers should not assume that greater disclosure enhances social engagement. In high-disclosure environments, users may need additional safeguards or reassurances (e.g., encryption, anonymization) rather than just relational warmth. In high-disclosure apps (e.g., dating), privacy protections must be more robust. Regulators should consider stricter data protection requirements for high-sensitivity apps and impose graded compliance frameworks based on the level of user disclosure. By ensuring that GeoMatching algorithms prioritize transparency and user control over information disclosure, companies can further promote sustainable industrialization and foster innovation that upholds user rights and trust.

6.3 Limitations and Future Research

Despite its significant contributions to our understanding of the presence-privacy tradeoff and the operationalization of information disclosure via algorithms in the context of GeoMatching, this research acknowledges several limitations that future studies should address. A primary concern of this study lies in its reliance on a simulated environment, which may limit the external validity of the findings. Real-world applications often involve more complex and dynamic user interactions that are difficult to fully replicate in controlled experimental settings. Another key limitation is the use of self-reported measures for critical constructs such as perceived privacy and social presence. These measures are susceptible to common biases, including social desirability and recall bias, which may affect data accuracy. Although self-reports are widely used in privacy-related research, future studies should consider incorporating objective behavioral tracking or experience sampling methods to complement self-perceived responses.

Furthermore, while this study focuses on two specific GeoMatching algorithmic frameworks—LEIS and HFSD—these serve as conceptual archetypes representing distinct trade-offs between information disclosure, search criteria, matching mechanisms, and learning dynamics in location-based matching applications. We acknowledge that these algorithm types are tailored to particular experimental and application contexts (e.g., ride-hailing and dating services) and may not fully capture the diversity of GeoMatching algorithms across different domains. Consequently, the findings and insights derived herein should be interpreted with caution when considering other algorithms or application scenarios. Future work is needed to extend this operationalization to a broader range of algorithmic designs, validate the proposed typology across diverse platforms, and explore how alternative configurations might influence user perceptions and privacy trade-offs.

Another limitation of this study lies in the cultural homogeneity of the sample. Participants were primarily based in France, and the study did not examine how cultural differences might influence privacy perceptions, trust formation, or disclosure behaviors. Since prior research has shown that cultural values can shape users' privacy concerns and online behavior, future studies should consider cross-cultural comparisons to enhance the generalizability and cultural applicability of the findings.

Additionally, it would be valuable to measure both social and institutional privacy and to compare their effects on users' attitudes and intentions regarding GeoMatching apps. We also posit that the presence-privacy tradeoff extends beyond the GeoMatching context and can be applied to other technologies. Future research could investigate this tradeoff in various computer-mediated environments and further explore the dual aspects of artificial intelligence (AI)-enabled applications, framing SP as a bright side and IP as a dark side. The integration of AI in this context is aligned with recent calls for AI's role in supporting sustainability goals, as highlighted by Dwivedi et al. (2023b) and Wamba et al. (2024), who demonstrate AI's capacity to enhance social impact and sustainability. Similarly, Johnson et al. (2021) and Harfouche et al. (2023) emphasize the importance of AI applications in fostering societal well-being and institutional responsibility. Research might also investigate the influence of SP on well-being outcomes, such as loneliness, directly linking findings to SDG 3 (Good Health and Well-Being), as discussed by Lakshmi and Corbett (2023) in their exploration of AI's dual roles in promoting positive societal outcomes while managing ethical considerations.

Finally, while GeoMatching apps offer pathways to advance certain SDGs, they face criticism regarding social, environmental, and economic impacts. Concerns include potential labor market deregulation, insufficient ecological responsibility, and tax practices that may undermine economic sustainability. Despite these challenges, a balanced approach is essential to examine both the promise and limitations of GeoMatching platforms in achieving SDGs, encouraging future research to explore ways these technologies can contribute to sustainability while addressing critical regulatory and ethical issues.

References

Adanyin, A. (2024). Ethical AI in Retail: Consumer Privacy and Fairness. *arXiv preprint arXiv:2410.15369*.

Albarracin, D., Johnson, B. T., & Zanna, M. P. (Eds.). (2005). *The Handbook of Attitudes*. Mahwah, NJ: Lawrence Erlbaum.

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.

Allport, G.W. (1935). Attitudes. In C. Murchison (Ed.), *Handbook of social psychology* (pp.798- 844). Worecester, Mass: Clark University Press.

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

Altman, I. (1990). Toward a transactional perspective: a personal journey. In *Environment and Behavior Studies* (pp. 225-255). Springer, Boston, MA.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*, 411–423.

Ash, S. E. (1956). Studies of independence and conformity: A minority of one against a unanimous. *Psychological Monographs*, 70, 177-190.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017-1041.

Bélanger, F., & James, T. L. (2020). A Theory of Multilevel Information Privacy Management for the Digital Era. *Information Systems Research*.

Bond, R., & Smith, P. B. (1996). Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological bulletin*, 119, 111.

Botsman R. & Rogers R., 2011, *What's mine is yours: the rise of collaborative consumption*, Harper Collins, New York.

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, 4, 193-220.

Brey, P. (2017). Ethics of emerging technology. *The ethics of technology: Methods and approaches*, 175-191.

Chan, Y. E., Culnan, M. J., Greenaway, K., Laden, G., Levin, T., & Smith, H. J. (2005). Information privacy: Management, marketplace, and legal challenges. *Communications of the Association for Information Systems*, 16, 12.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, 6, 181-202.

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: the case of Facebook users. *European Journal of Information Systems*, 24, 93-106.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, 60, 2079-2094.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, 26, 675-694.

Corbett, J., Dennehy, D., & Carter, L. (2023). Introduction to the Special Section: Digital Innovation for Social Development and Environmental Action. *Communications of the Association for Information Systems*, *53*, 22-41.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10, 104-115.

Daft, R. L., & Lengel, R. H. (1983). *Information richness: A new approach to managerial behavior and organization design*. College Station, TX: Texas A & M University.

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32, 554–571.

Dinev, T. (2014). Why would we care about privacy?. *European Journal of Information Systems* (2014) 23, 97–102.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, 17, 61-80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22, 295-316.

Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. *Journal of Business Research*, *129*, 961-974.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, *57*, 101994.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., ... & Wright, R. (2023a). Opinion Paper:"So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International journal of information management*, *71*, 102642.

Dwivedi, Y. K., Sharma, A., Rana, N. P., Giannakis, M., Goel, P., & Dutot, V. (2023b). Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions. *Technological Forecasting and Social Change*, *192*, 122579.

Eagly, A., & Chaiken, S. (1993). *Psychology of Attitudes*. NY: Harcourt, Brace Jovanovich.

Eagly, A., & Chaiken, S. (2007). *The Advantages of an Inclusive Definition of Attitude*. Social Cognition, 25, 582-602.

Edwards, S. M., Li, H., & Lee, J. H. (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of advertising*, 31, 83-95.

Elkington, J., & Rowlands, I. H. (1999). Cannibals with forks: The triple bottom line of 21st century business. *Alternatives Journal*, *25*, 42.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*, 39–50.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, 12, 106-119.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services. *Omega*, 32, 407-424.

Goncalves, L. R., De Pechpeyrou, P., & Bénavent, C. (2014). Jusqu'où les consommateurs acceptent-ils d'être géolocalisés?/How far are consumers willing to accept location-based services? *Revue Française du Marketing*, *248*, 27-42.

Guttentag, D., Smith, S., Potwarka, L., & Havitz, M. (2018). Why tourists choose Airbnb: A motivation-based segmentation study. *Journal of Travel Research*, *57*, 342-359.

Hamari, J., Sjöklint, M., & Ukkonen, A. (2016). The sharing economy: Why people participate in collaborative consumption. *Journal of the association for information science and technology*, *67*, 2047-2059.

Hammond, N., & Moretti, A. (2023). Data like any other? Sexual and reproductive health, Big Data and the Sustainable Development Goals. *Sexualities*, 13634607231152599.

Harfouche, A., Quinio, B., Saba, M., & Saba, P. B. (2023). The Recursive Theory of Knowledge Augmentation: Integrating human intuition and knowledge in Artificial Intelligence to augment organizational knowledge. *Information Systems Frontiers*, *25*, 55-70.

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, 65, 689-708.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, 55, 16-30.

Herring, S. C. (Ed.). (1996). *Computer-mediated communication: Linguistic, social, and cross-cultural perspectives* (Vol. 39). John Benjamins Publishing.

Hess, T. J., Fuller, M., & Campbell, D. E. (2009). Designing interfaces with social presence: Using vividness and extraversion to create social recommendation agents. *Journal of the Association for Information Systems*, 10, 1.

Holzinger, A., Weippl, E., Tjoa, A. M., & Kieseberg, P. (2021). Digital transformation for sustainable development goals (SDGs)-a security, safety and privacy perspective on AI. In *International cross-domain conference for machine learning and knowledge extraction*. 1-20). Cham, Springer International Publishing.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 275-298.

INSEE (2019), Equipement des ménages en biens durables selon différentes caractéristiques (2004-2019): retrieved on September 16th 2024 from https://www.insee.fr/fr/statistiques/2385827.

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*, 54, 851-865.

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management*, 52, 893-908.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note - privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24, 579-595.

Johnson, M., Albizri, A., & Harfouche, A. (2023). Responsible artificial intelligence in healthcare: Predicting and preventing insurance claim denials for economic and social wellbeing. *Information Systems Frontiers*, *25*, 2179-2195.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European journal of social psychology*, *31*, 177-192.

Kim, W., Park, Y., Shin, J., & Jo, M. (2022). Consumer preference structure of online privacy concerns in an IoT environment. *International Journal of Market Research*, 64, 630-651.

Koh, B., Raghunathan, S., & Nault, B. R. (2020). An empirical examination of voluntary profiling: Privacy and quid pro quo. *Decision Support Systems*, 132, 113285.

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, 119, 46-59.

Kordzadeh, N., & Warren, J. (2017). Communicating personal health information in virtual health communities: an integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems*, 18, 1.

Kotlarsky, J., Oshri, I., & Sekulic, N. (2023). Digital sustainability in information systems research: Conceptual foundations and future directions. *Journal of the Association for Information Systems*, *24*, 936-952.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, 25, 109-125.

Kurtz, O. T., Wirtz, B. W., & Langer, P. F. (2021). An Empirical Analysis of Location-Based Mobile Advertising—Determinants, Success Factors, and Moderating Effects. *Journal of Interactive Marketing*, 54, 69-85.

Lakshmi, V., & Corbett, J. (2023). Using AI to improve sustainable agricultural practices: a literature review and research agenda, *Communications of the Association for Information Systems*, 44, 123-166.

Larson, R. B. (2023). Privacy concerns and social desirability bias. *International Journal of Market Research*, 14707853231222810.

Li, H., Edwards, S. M., & Lee, J. H. (2002). Measuring the intrusiveness of advertisements: Scale development and validation. *Journal of Advertising*, 31, 37–47.

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21, 621-642.

Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. *Communications of the Association for Information Systems*, 28, 28.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems*, 54, 471-481.

Lim, K. H., & Benbasat, I. (2000). The effect of multimedia on perceived equivocality and perceived usefulness of information systems. *MIS quarterly*, 449-471.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, 26, 546-563.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: The construct, the scale, and a causal model. *Information systems research*, 15, 336-355.

Margulis, S. T. (2011). Three theories of privacy: An overview. In Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 9-17). Springer, Berlin, Heidelberg.

Meek, T., Barham, H., Beltaif, N., Kaadoor, A., & Akhter, T. (2016, September). Managing the ethical and risk implications of rapid advances in artificial intelligence: A literature review. In *2016 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 682-693). IEEE.

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and information technology*, *7*, 111-119.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41, 100-126.

Nord, W. R. (1969). Social exchange theory: an integrative approach to social conformity. *Psychological Bulletin*, 71, 174.

Nowak, K. L., & Biocca, F. (2003). The effect of the agency and anthropomorphism on users' sense of telepresence, copresence, and social presence in virtual environments. *Presence: Teleoperators & Virtual Environments*, *12*, 481-494.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS quarterly*, 977-988.

Petronio, S (2002). *Boundaries of privacy: dialectics of disclosure*. State University of New York Press, Albany.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European journal of information systems*, 19, 181-195.

Preacher, K. J. and Hayes A.F. (2008). Asymptotic and Resampling Strategies for Assessing and Comparing Indirect Effects in Multiple Mediator Models. *Behavior Research Methods*, 40, 879–891.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15.

Schoormann, T., Strobel, G., Möller, F., Petrik, D., & Zschech, P. (2023). Artificial intelligence for sustainability-a systematic review of information systems literature. *Communications of the Association for Information Systems*, *52*, 8.

Seneviratne, S., Seneviratne, A., Mohapatra, P., & Mahanti, A. (2015). Your installed apps reveal your gender and more!. *ACM SIGMOBILE Mobile Computing and Communications Review*, 18, 55-61.

Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, 9, 15.

Shih, H. P., Lai, K. H., & Cheng, T. C. E. (2017). Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters?. *European Journal of Information Systems*, 26, 432-450.

Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. London: Wiley.

Singh, B., Jain, V., Kaunert, C., Dutta, P. K., & Singh, G. (2024). Privacy matters: Espousing blockchain and artificial intelligence (AI) for consumer data protection on e-commerce platforms in ethical marketing. In *Ethical Marketing Through Data Governance Standards and Effective Technology* (pp. 167-184). IGI Global.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Song, J. H., Hollenbeck, C. R., & Zinkhan, G. M. (2008). The value of human warmth: Social presence cues and computer-mediated communications. *ACR North American Advances*.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS quarterly*, 1141-1164.

Sztompka P. (1999), *Trust: A Sociological Theory*, Cambridge, Cambridge University Press.

Teeter, D. L., & Loving, B. (2001). *Law of mass communications: Freedom and control of print and broadcast media*. 10th ed. Foundation Press.

Tu, C. H. (2002). The relationship between social presence and online privacy. *The internet and higher education*, *5*(4), 293-318.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 425–478.

Walther, J. B. (1992). Interpersonal effects in computer-mediated interaction: A relational perspective. *Communication research*, 19, 52-90.

Wamba, S. F., Queiroz, M. M., & Trinchera, L. (2024). The role of artificial intelligence-enabled dynamic capability on environmental performance: The mediation effect of a data-driven culture in France and the USA. *International Journal of Production Economics*, 268, 109131.

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

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, 44-52.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, 51, 42-52.

Xu, H., Parks, R., Chu, C. H., & Xiaolong (Luke) Zhang. (2010, December). Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding. In *AMCIS* (p. 503).

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 26, 135-174.

Zhao, X., Lynch, J. G., & Chen, O. (2010). R considering Baron and Kenny: Myths and Truths about Mediation Analysis, *Journal of Consumer Research*, 37, 197–206.

Appendix A: Sustainable Developement Goals and GeoMatching

Table 7. SDG and GeoMatching

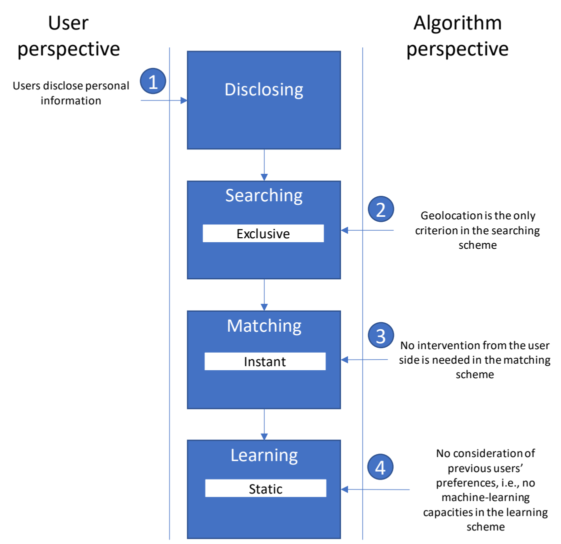
SDG 1: no poverty sharing of goods and services (Zipcar) or housing (Couchsurfing) bartering and exchanging services (BarterQuest) microfinance and peer-to-peer lending (Kiva or Twino) access to local employment and training (YouMeeJobs) community support and volunteering (Nextdoor)	SDG 2: zero hunger food or meals sharing between neighbors (Olio, ShareTheMeal) Donations (FoodRescue US, ShareWaste) urban gardening and local production (Grow Stuff for gleaners, Falling Fruit) local solidarity and mutual support: (Nextdoor, Entourage)
SDG 3 : good health and well-being sport and physical activity meetups (Meetup) psychological support between individuals (Voisins Malin, Voisins Solidaires dating and meeting new friends (MeetUp, Tinder) step converter into currency (SweatCoin)	SDG 4: quality education peer tutoring (Meet in Class) or collaborative academic support (Study Buddy) sharing educational resources (SkillShare) or exchange of skills and mentoring (Teach Surfing) or easy organization of local educational workshops (Evenbrite) support for students at risk of dropping out school (School In the cloud) through parental support (Yoopies, WonderSchool)
SDG 5: gender equality support and mutual aid between women (Hey Vina, Peanut) especially in vulnerable situations (Circle of 6) accès à des opportunités professionnelles pour les femmes (Sharp Bumble Bizz) sharing household and family tasks (FairShare, OurHome) support for female leadership and entrepreneurship (Elpha) education on gender equality and women's rights (Rebel Girls), including through dating apps that allow women to make the first move (Tinder)	SDG 6 : clean water and sanitation reporting and mapping of water points and sanitation facilities (Watermap) and awareness and education on hygiene and sanitation (Sanitation First) crowdfunding for water and sanitation projects (GiveWater) community collaboration for water and sanitation (NextDrop)
SDG 7 : affordable and clean energy energy sharing between individuals(Power Ledger) collective solar energy production (WeShareSolar)	SDG 8: decent work and economic growth (see SDG 1) connecting people for freelance jobs and local services (TaskRabbit, Fiverr and see SGD1) carpooling and delivery (Uber, Lyft, Deliveroo, Uber Eats) professional mutual aid and local networking (Nextdoor, Sharp)
SDG 9: industry innovation and infrastructure industrial coworking and access to infrastructure like 3D printers for prototyping (ProtoLabs Network) connecting for innovation and R&D: (UpWork) (UpWork) and sharing technical skills and knowledge	SDG 10: reduced inequalities (see SDG 1) donations of items between individuals (GEEV) and shared services for the local economy: (Nextdoor) microfinance and peer-to-peer lending

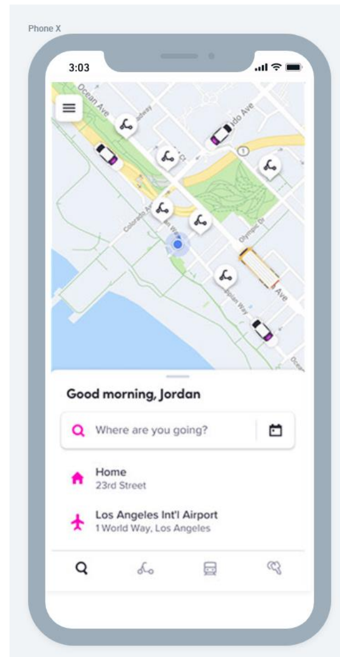
(MeetUp, SkillShare)	sharing skills and job opportunities
SDG 11: sustainable cities and communities smart mobility (CityMapper) resource sharing and circular economy (Falling Fruit, Next Drop) citizen participation and community engagement (FixMyStreet, CitizenLab) smart energy management (PowerLedger)	SDG 12: responsible consumption and production (see SDG 2) fighting food waste: (Olio, Falling Fruit) via collaborative consumption and circular economy (GEEV, Falling, Mutum) sustainable production and resource sharing: (ShareWaste) short supply chains and local consumption (OpenFoodNetwork) product transparency and ecological impact (Yuka, Clear Fashion)
SDG 13: climate action carsharing or ridesharing (CarPoolWorld, craigslist.org CraigsList, Zipcar), bike and electric scooter sharing (Lime) renewable energy sharing (PowerLedger)	SDG 14: life below water beach cleanups and fighting plastic pollution (CleanSwell) recycling of fishing nets and marine equipment (Ghost Fishing) management of marine protected areas and sustainable navigation (Navily) and monitoring (iNaturalist)
SDG 15: life on land participatory science for biodiversity monitoring (PlantNet, Inaturalist) or for invasive species (ObsMapp) management of natural parks and reserves (WildEyeWildness, MammalMapper or Birdtrack)	SDG 16: peace justice and strong institutions reporting incidents and human rights violations (Ushahidi, EyeWitness) ou la corruption (Bribespot) or consentement in relationship (LegalFling) elections monitoring (elmo) and transparency and accountability of public institutions (GovernEye) monitoring justice and access to legal services (OpenGouv) civic participation and local governance (NextDoor, FixMyStreet)

Appendix B: Diagrams and mockup examples used for the pretest

LEIS Algorithm - Lower disclosing, Exclusive searching, Instant matching and Static learning

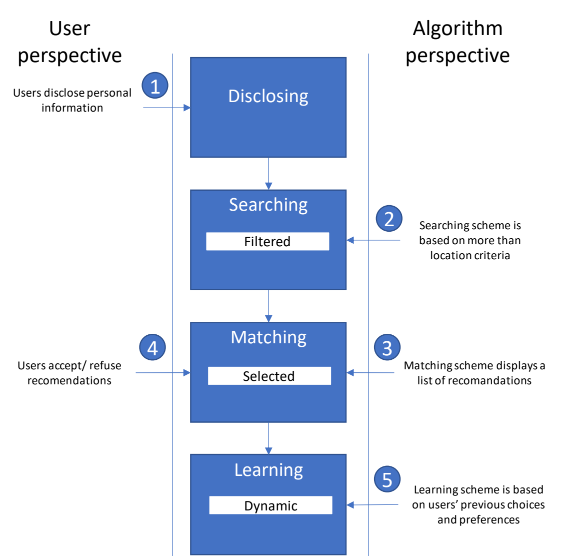
One screenshot of app prototype that follows LEIS algorithm

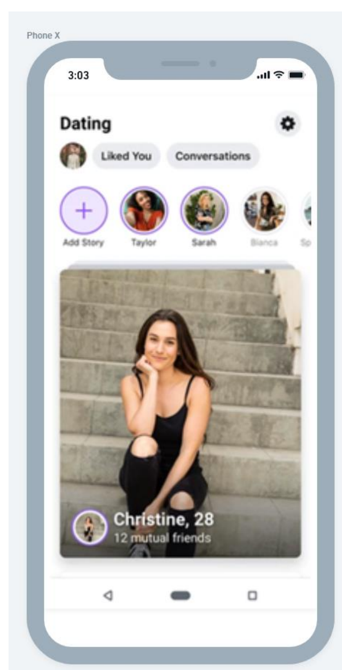




HFSD Algorithm - Higher disclosing, Filtered searching, Selected matching and Dynamic learning

One screenshot of app mockup that follows HFSD algorithm





About the Authors

Zhenzhen Zhao received her Ph.D. degree in computer science from Institut Mines-Télécom and Université Pierre et Marie Curie, Paris, France. She is currently an Associate Professor at the Digitalisation Academy, SKEMA Business School (Paris campus). She has also been a Visiting Researcher at Vrije Universiteit Brussel (Belgium) and Tsinghua University (China). Her research lies at the intersection of marketing and human–computer interaction (HCI), focusing on bringing HCI research into the marketing discipline by understanding and shaping online consumer behavior through platform design. She is particularly interested in the implications of virtual communities, mobile applications, gamification, user experience, and design thinking. Her work has appeared in the *Journal of Interactive Marketing*, *Information & Management*, and many other outlets.

Damien Renard received his Ph.D. in Management Sciences from Paris Dauphine University. He is currently Professor of Communication at UCLouvain. His research focuses on the modalities of participation, collaboration, and immersion in digital platforms and immersive technologies. He has published in international peer-reviewed journals such as the *Journal of Business Research*, *Journal of Interactive Marketing*, *Journal of Advertising Research*, *International Journal of Innovation Management*, and *IEEE Transactions on Engineering Management*.

Catherine Lejealle received her Ph D. in Sociology from Paris Sorbonne University. She is currently Associate Professor of Digital Marketing at ISC Paris. Her research focuses on the adoption of new technologies by consumers and brands. She has published in international peer-reviewed journals such as the *Journal of Innovation Economics & Management, Journal of Consumer Behaviour or Journal of Knowledge Management*.

Thierry Delécolle is Vice-President of De Vinci Higher Education and Associate Professor at EMLV Business School. He holds a PhD in Management Science form University Paris-Dauphine, his research interests are in the field of CRM, CSR, digital and business models. He published papers in international journals and authored or co-authored books and pedagogical cases in strategy and marketing for which he received the AFM and ATLAS-AFMI best cases awards in particular.