Place-based privacy

Understanding attitudes and behaviours across China and beyond

by

Hongyu Zhang

B.E.S., University of Waterloo, 2015
M.Sc., Western University, 2017

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

Graduate and Postdoctoral Studies

(Geography)

MCGILL UNIVERSITY

(Montréal)

March 2024

Abstract

The emergence of the World Wide Web has eroded traditional boundaries, connecting individuals globally while giving rise to intricate privacy concerns. Within this context, the concept of geoprivacy takes centre stage, highlighting the control of personal location information flow and is influenced by dynamic factors such as time, culture, demographics, and trust. This dissertation posits geoprivacy as a social form that underpins fundamental aspects of social interaction rather than a unilateral desire for isolation from society. The need for location sharing by individuals necessitates a rehumanized, context-dependent exploration, as cultural norms and personal characteristics can lead to varying levels of geoprivacy expectations. Therefore, a human-centred approach is adopted to investigate user responses to regulatory mandates and probe geoprivacy concerns within China and beyond. The first manuscript clarifies the uniqueness of geoprivacy, establishing a humanistic perspective to counteract the dehumanizing effects of datafication and recognize the spatial variations of geoprivacy attitudes. The subsequent manuscript dismantles the ethnocentric view of geoprivacy. Through the analysis of social media data, the study unveils the specific landscape of geoprivacy attitudes within the Confucian realm and reiterates the importance of cultural distinctions in privacy studies. The third manuscript takes a step further by re-examining the relationship between knowledge, attitude, and behaviour, providing deeper contextual insights into understanding geoprivacy behaviours in computer-mediated environments. By employing data collected from an online survey, the study discovers gender disparities and regional divergences in the cognitive perspective of geoprivacy. In its entirety, the disserta-

tion synthesizes these contexts into place-based privacy, wherein geographical information becomes a pivotal determinant and extension of an individual's privacy attitudes. As both a humanistic and social concept, geoprivacy transcends mere degrees of anonymity in data disclosure. The empirical studies in this dissertation showcase the varying nature of geoprivacy perceptions even within the Chinese regions. These findings ultimately enrich the dialogue surrounding privacy, technology, and society, transforming geoprivacy from a self-reinforcing cycle of universal values into a diverse concept embraced by a broader population.

Résumé

L'émergence du World Wide Web a érodé les frontières traditionnelles, connectant les individus à l'échelle mondiale tout en suscitant des préoccupations complexes en matière de protection de la vie privée. Dans ce contexte, le concept de géoconfidentialité occupe une place centrale, soulignant le contrôle du flux d'informations de localisation personnelle et influencé par des facteurs dynamiques tels que le temps, la culture, la démographie et la confiance. Cette thèse considère la géoconfidentialité comme une forme sociale qui sous-tend les aspects fondamentaux de l'interaction sociale, plutôt que comme un désir unilatéral d'isolement de la société. Le besoin de partage de localisation par les individus nécessite une exploration réhumanisée et dépendante du contexte, car les normes culturelles et les caractéristiques personnelles peuvent conduire à des niveaux variables d'attentes en matière de géoconfidentialité. Par conséquent, une approche centrée sur l'humain est adoptée pour étudier les réponses des utilisateurs aux mandats réglementaires et sonder les préoccupations en matière de géoconfidentialité en Chine et au-delà. Le premier manuscrit clarifie le caractère unique de la géoconfidentialité, en établissant une perspective humaniste pour contrer les effets déshumanisants de la datafication et reconnaître les variations spatiales des attitudes en matière de géoconfidentialité. Le manuscrit suivant déconstruit la vision ethnocentrique de la géoconfidentialité. Grâce à l'analyse des données des médias sociaux, l'étude dévoile le paysage spécifique des attitudes en matière de géoconfidentialité dans le royaume confucéen et réitère l'importance des distinctions culturelles dans les études sur la protection de la vie privée. Le troisième manuscrit va plus loin en réexaminant la relation entre la connaissance,

l'attitude et le comportement, fournissant des informations contextuelles plus approfondies pour la compréhension des comportements en matière de géoconfidentialité dans les environnements informatisés. En utilisant des données collectées à partir d'une enquête en ligne, l'étude découvre des disparités entre les genres et des divergences régionales dans la perspective cognitive de la géoconfidentialité. Dans son ensemble, la thèse aborde une synthèse de ces contextes dans la protection de la vie privée basée sur le lieu, où l'information géographique devient un déterminant central et une extension des attitudes d'un individu en matière de protection de la vie privée. En tant que concept humaniste et social, la géoconfidentialité transcende les simples degrés d'anonymat dans le processus de divulgation des données. Les études empiriques menées dans le cadre de cette thèse mettent en évidence la nature variable des perceptions de la géoconfidentialité, même au sein de la régions chinoise. Ces résultats enrichissent en fin de compte le dialogue sur la vie privée, la technologie et la société, transformant la géoconfidentialité d'un cycle de valeurs universelles se renforçant lui-même en un concept diversifié adopté par une population plus large.

Research Contributions

- This dissertation conceptualizes geoprivacy as a social form influenced by cultural, spatial, and temporal factors.
- The studies found that within the Chinese demographic, a significant portion conveyed indifference toward data privacy, contrasting with a proactive group of privacy advocates who contributed to resistance to involuntary location disclosure.
- The display of IP location impacted users' willingness to express their spatial selves on social media, leading some individuals to opt out of specific platforms.
- A positive relation was observed between privacy knowledge, attitude, and behaviour, which aligns with existing literature.
- Declarative knowledge (e.g., privacy rights) demonstrated an unexpected negative relation with privacy concerns.
- Females emerged as more active participants in online discussions regarding unwanted location disclosure, showcasing higher privacy protection behaviours despite lower privacy literacy levels.
- Regional variations in privacy concerns were discerned within China, with respondents from Northeast China standing out as a population with lower privacy concerns, hinting at potential geopolitical influences on individuals' values and beliefs.

Author Contributions

This dissertation comprises manuscripts that, with the support of my supervisor, Grant McKenzie, have undergone either publication in articles or the review process mandated by the Research Ethics Board (REB) office at McGill University. The statement of contributions and ethics approval are outlined below:

1. A version of the discussion on territory and place in Section 1.2 appears in Zhang, H. (2023). Place-based privacy: A humanistic reflection on solitude and anonymity. In *Proceedings of the 8th Conference on Spatial Knowledge and Information Canada*. The article has been published on `osf.io`, an open access repository.

2. Chapter 3 has been published in Zhang, H., & McKenzie, G. (2023). Rehumanize geoprivacy: from disclosure control to human perception. *GeoJournal*, *88*(1), 189–208. A copyright clearance has been obtained from the publisher, Springer Nature, under license number 5583390601720.

3. Chapter 4 has been submitted to *Social Science Computer Review*, with me as the first author and my supervisor as the second author.

4. Chapter 5 has been submitted to *Information Technology and People*, with me as the first author and my supervisor as the second author. The online survey within the chapter received approval from REB #1 at McGill University under the file number 22-11-005.

5. A version of Section 6.3 appears in Zhang, H., & McKenzie, G. (2022). Towards place-based privacy: Challenges and opportunities in the "smart" world. In *Proceedings of the 2022 IEEE International Symposium on Technology and Society (ISTAS)*. The Institute of Electrical and Electronics Engineers (IEEE) does not require individuals working on a thesis to obtain a formal reuse license.

For each of the items above, my roles include the following: conceptualization, methodology, formal analysis, writing – original draft, writing – review and editing, visualization, and funding acquisition. My supervisor's responsibilities involve writing – review and editing, supervision, project administration, and funding acquisition.

Table of Contents

Appendices

List of Tables

List of Figures

List of Abbreviations

CAC	Cyberspace Administration of China
CCPA	California Consumer Privacy Act
CIGI	Centre for International Governance Innovation
EULA	End User License Agreement
FoMO	Fear of Missing Out
GDPR	General Data Protection Regulation
GeoSN	Geosocial Network
GIS	Geographic Information System
GPS	Global Positioning System
IP	Internet Protocol
Ipsos	Institut Public de Sondage d'Opinion Secteur
IUIPC	Internet Users' Information Privacy Concerns
KAB	Knowledge-Attitude-Behaviour
KPI	Key Performance Indicator
LBS	Location-Based Service
LDA	Latent Dirichlet Allocation
PIPL	Personal Information Protection Law
PRC	People's Republic of China
QoS	Quality of Service
RADP	Reverse-Auction-Based Dynamic Price

RSFP Random-Selection-Based Fixed Price

SCS Social Credit System

UGC User-Generated Content

UML Unsupervised Machine Learning

UTP User-Tailored Privacy

VIP Very Important Person

VPN Virtual Private Network

WTA Willingness to Accept

WTP Willingness to Pay

Acknowledgements

I would like to express my gratitude and appreciation to the following individuals and organizations who have played a significant role in the completion of my doctoral dissertation. First and foremost, I am indebted to the pioneering work of Yi-Fu Tuan in humanistic geography. His profound *geosophy* in understanding the human experience of place has been a constant source of inspiration throughout my doctoral study. His contributions have shaped my perspective on human geography and provided a solid theoretical foundation for my research.

I appreciate my supervisor, Grant McKenzie, for his guidance, expertise, and receptiveness to students' ideas. His insightful feedback, constructive criticism, and consistent encouragement have significantly enhanced the calibre of this dissertation. I am thankful for his dedication and commitment to fostering my intellectual development. I would also like to thank Raja Sengupta and Carsten Keßler for serving as my committee members and Tim Elrick for providing me with employment opportunities at the Geographic Information Centre.

I would like to acknowledge the generous financial support provided by Fonds de Recherche du Québec – Société et Culture (FRQSC) and the Department of Geography at McGill University. Their investment in my research allowed me to pursue my studies with focus and dedication. I appreciate their confidence in my work and belief in its potential impact.

I am grateful to my friends, Luci Xi Lu, Ziyue Wang, and Shih-Chung Wei, for engaging in thoughtful discussions about my research and offering valuable feedback. Exploring a

peripheral research topic in geography has been challenging, and your thoughtful words and consistent support have been instrumental in making this work possible. I would also like to extend my gratitude to Annie Seong Lee and the members of the Platial Analysis Lab, including Mikael Brunila, Priyanka Verma, Dan Qiang, Daniel Romm, and Clara Féré, for their dynamic conversations surrounding academic life – special thanks to Clara Féré for proofreading the French translation of my abstract.

I want to thank all the participants who took part in my research. Their willingness to share their opinions and experiences was essential in enriching this study and contributing to a better understanding of individuals' location privacy concerns.

Amid the background of a global pandemic, my family members shouldered the responsibility of caring for our elderly relatives and exhibited remarkable patience in supporting my doctoral study. It is regrettable, and I deeply regret that due to travel restrictions, I could not bid a final farewell to my grandpa, who passed away during this challenging time.

To everyone mentioned above and to those who have supported me in various other ways, both seen and unseen, this dissertation would not have been possible without your contributions, guidance, and steadfast belief in my abilities.

Thank you all for being an integral part of my academic journey and making this achievement a reality.

Dedication

To my beloved mom and dad

Chapter 1

Introduction

1.1 Motivation

Since the Cambridge Analytica scandal, Meta (formerly known as Facebook) has been plagued by a series of privacy breaches, one after another, and it seems that the company still needs to learn how to effectively prevent future privacy violations (Heiligenstein, 2023). The launch of Threads, Meta's Twitter competitor app, has also been put under scrutiny in July 2023. The app was unavailable in the European Union due to compliance issues, bringing data privacy concerns back to the forefront in discussing Mark Zuckerberg's latest mission (Kelly, 2023). As one of the most popular social media companies, Meta's privacy-related headlines continue to make individuals contemplate information privacy in the digital age. The reality is, it is not just Meta. Leading internet companies routinely gather user information and endeavour to capitalize on it, riding the wave of the growing personal data market driven by the surge in social media usage (Spiekermann et al., 2015). At the same time, regulators have been trying to keep pace with the rapid advancement of technologies by enhancing data privacy laws. Since the implementation of the General Data Protection Regulation (GDPR) in 2018, new privacy regulations have emerged across the globe, including in the United States[3], the European Union[4], and China[5]. As a result, news coverage has extended from privacy breaches to privacy regulations, continuously capturing

[3]e.g., in California, Virginia, Colorado, and Utah (Securiti Research Team, 2023).
[4]e.g., the Digital Services Act and Digital Markets Act (European Commission, 2023).
[5]e.g., the Personal Information Protection Law (PIPL) (Creemers et al., 2020).

the attention of consumers and internet users.

Geographers, too, have recognized the significance of geoinformation in relation to privacy. The connection between physical privacy and traditional geography will be established in the next section. In this section, the focus is information privacy, which has become a pivotal issue in digital geography (Elwood & Leszczynski, 2011). Concerns regarding the misuse of geoinformation can be traced back to earlier times, as discussed in the concept of geoslavery (Dobson & Fisher, 2003). More recently, the uniqueness of geoprivacy has been deliberated in the context of pervasive computing (Keßler & McKenzie, 2018). As both a social media user and a geographic information science researcher, I am concerned about the topic at the intersection of geography and privacy. My goal is to gain a deeper understanding of this subject from a cognitive perspective[6], as data protection algorithms and policies are fundamentally designed to address individuals' desire for privacy.

1.2 The Intersection of Privacy and Geography

The classical definitions of privacy are two-fold. Before the 20$^{\text{th}}$ century, the concept was tied to individuals' physical boundaries, and *being alone* was established as a fundamental right in American legal studies (Warren & Brandeis, 1890). The notion has since gained momentum in the area of *personal information control* (Westin, 1967) as data exchange became faster and more convenient, thanks to the inventions such as telephones and the Internet. While the right to privacy is subject to debate, the notion of privacy as an interest, or something desirable to have (DeCew, 1997), is considered a foundational assumption of the dissertation. This section traces the philosophical origins of privacy and establishes its relationship with core concepts in geography.

The origin of privacy is intrinsically linked to human interactions in the physical world,

[6]As the title of the dissertation suggests, the cognitive perspective refers to analyzing individuals' geoprivacy perception, attitude, and behaviour.

reflecting the realization of geographic concepts. The distinction between public and private, for example, has been captured in political philosophy. In Aristotle's *Politics*, the polis is a public sphere of political structure while the oikos is a private sphere of family life (Aristotle, 1999). Over time, there has been a growing trend to segregate inappropriate places from the public sphere, thereby limiting the extent of public power in private affairs (DeCew, 1997). A similar dichotomy of public and private property can be found in John Locke's *Second treatise on government* (1690). According to Locke, nature is "a state of perfect freedom" and earth is "common to all" persons. Nevertheless, every individual has an exclusive property right in their "own person", which resonates with Sir Edward Coke's declaration that a person's house is their "castle and fortress" (1604). Public means, contrary to Aristotle's perspective, came to be seen by Locke as necessary safeguards for private ends, such as life, liberty, and property (DeCew, 1997).

The establishment of public and private spheres, both situated on earth, is inherently tied to *territory* and *place*[7]. The ancient Greek philosopher Plato regarded places as a fundamental element of human existence (Kymäläinen & Lehtinen, 2010). In human geography, places are locations with tangible structures, individual significance, and daily routines (Cresswell, 2009). The spatial extent of places can range from a mere corner of a room to the expanse of the entire earth, but every place has its boundary. When we examine the various senses of territories within different communities based on their living environments, we observe that farm communities tend to have relatively static boundaries around their homes. In contrast, migratory herders have a more dynamic range of activity (Tuan, 1976). A similar pattern can be found between work-from-home programmers and long-haul truck drivers in the modern workplace. Workplace surveillance, in this case, raises distinct ethical concerns that need to be addressed, particularly as the boundary between the public workplace

[7]A version of this paragraph appears in Zhang, H. (2023). Place-based privacy: A humanistic reflection on solitude and anonymity. In *Proceedings of the 8th Conference on Spatial Knowledge and Information Canada*.

and private home becomes blurred and the location of the workplace changes, sometimes in a cross-national setting. Another factor that affects individuals' privacy attitudes is their emotional attachment to a specific place. As described by Tuan (1976), humans pause and establish a connection with a place over time, and each pause transforms a location into a meaningful place. Private places can thus be explored through the lens of place-based identities by considering individuals' psychological connections to their memorable places.

While the abstraction of spatial information has been widely accepted in geographic information science, the representation of place, commonly referred to as *platial information*, still requires theoretical development. Diverse researchers including spatial scientists, environmental psychologists, and linguists have made efforts to formalize the concept of place. Current approaches involve distinguishing between place and space (Blaschke et al., 2018), establishing place reference systems (Scheider & Janowicz, 2014), and exploring various media for representing places (Jones et al., 2008). As Mocnik (2022) emphasizes, maps and spatial datasets are not the sole representations of a place; other visual means, audio, texts, and components of the human sensory system also contribute. Platial information, viewed as a multimedia form, can serve as a valuable tool for modelling privacy attitudes. Place descriptions about identities (Twigger-Ross & Uzzell, 1996), affective states (Smith et al., 2011), and affordances (Jordan et al., 1998) can also be incorporated alongside spatial information for modelling privacy behaviour. Platial information, in this regard, is considered a set of contextual factors influencing individuals' privacy attitudes and behaviours.

Apart from the public-private divide in political philosophy, the origin of privacy has also been investigated in biological and anthropological studies. Alan Westin compared "territory rules" in animals with "trespass concepts" in human society and concluded that a desire for privacy is not exclusive to humans. For the purpose of propagation, animals of all kinds seek private space to ensure "individual well-being and small-group intimacy" (Westin, 1984; Klopfer & Rubenstein, 1977). The universal need for privacy has also been

evident in cross-cultural settings (Mead, 1973). Most societies have established physical boundaries by maintaining distance and avoiding contact with others. Even in primitive cultures, psychological means such as averting one's eyes or facing a wall were used to create social barriers (Westin, 1984). Thus, modern society has significant potential to enhance physical and psychological autonomy.

The cognitive aspect of privacy links the notion to the phenomenological perspective of *distance*. Our common understanding of distance is a straight-line interpretation in Euclidean space (i.e., aerial distance). Other forms of distance include effective distance (e.g., highway or railway), distance measures in units of time, money, or effort, as well as cognitive and affective distance (Pirie, 2009). As discussed by Witthuhn (1979), real distances between places can be distorted by human perceptions, especially in unfamiliar environments. Thus, the investigation of privacy attitudes needs to consider phenomenological distance, which is mediated by personal and cultural factors such as languages, emotions, and worldviews (Handel, 2018). According to Heidegger's *Being and Time* (2008), people live in an experiential rather than an abstract world. Distance is not always continuous in the sense of "being-in-the-world" (Heidegger, 2008). Through emotional "leaps" (Handel, 2018), an actual distant place may feel closer in one's mind, and vice versa. The "more-than-measurable" property of phenomenological distance (Handel, 2018), as a result, creates unavoidable variations of acceptable social boundaries between individuals and complicates the efforts of theorizing privacy attitudes.

1.3 Dissertation Structure

The objective of my doctoral research is to examine individuals' geoprivacy perceptions, attitudes, and behaviours in various contexts. The dissertation consists of scholarly papers contributing to the common theme of geoprivacy. Two main aspects, namely theoretical

development and empirical investigations, are included in the dissertation. The research questions of each aspect, as well as the organization of the dissertation, are presented as follows.

Chapter 1 establishes the context for the discussion of geography and privacy. This chapter introduces the rationale behind the study of information privacy through the philosophical roots of physical privacy and explores the potential contributions of geographers to this discourse. It proceeds to present the research questions about geoprivacy in theory and practice and ends by outlining the structure of the dissertation.

Chapter 2 offers an overview of classic and contemporary literature in privacy studies, effectively framing geoprivacy as a social form that establishes the backdrop for subsequent chapters in this dissertation. The chapter then elaborates on the essential concepts employed in this dissertation and presents varied privacy concerns among global citizens, specifically focusing on the United States and Canada.

Given the prevalence of data-centric anonymization techniques in geoprivacy research, the theoretical part of this research proposes deconstructing the concept of geoprivacy from a human-centred perspective. **Chapter 3** delves into the concept of geoprivacy and calls for interdisciplinary thinking on the subject. This chapter reviews the privacy paradox phenomenon, lists the sources of individuals' geoprivacy concerns, categorizes recent anti-geosurveillance attempts, and promotes the *platial* interpretation of geoprivacy. This chapter emphasizes the multi-faceted nature of geoprivacy, which is demonstrated through an analysis of cultural, demographic, legal, and economic impact on geoprivacy perception. Specifically, this chapter aims to address the following questions:

1. What is *privacy* to humans in the hybrid physical-virtual world? What are the implications of information privacy in light of the influx of big geospatial data?

2. Considering that there is a plethora of research on privacy, how does *geoprivacy* differ

or stand out as a human geography concept?

3. What are the spatial variations in geoprivacy perception? How do cultural, demographic, regulatory, and monetary considerations influence or mediate the spatial variations?

The empirical part of this research focuses on public opinion analysis of social media users in China. Originally designed to counter disinformation, development of the IP location feature[8] provides an unprecedented opportunity to examine individuals' geoprivacy concerns in East Asian culture. The lack of research on privacy concerns in China (Li, 2020) makes this exploration timely and significant. **Chapter 4** looks into geoprivacy concerns on Chinese social media using Weibo data. Users' reactions to the IP location feature are examined by deep reading with the help of a Latent Dirichlet Allocation (LDA) topic model. The mix of supportive and opposing voices marks the specific discourse of geoprivacy concerns in the Confucious state. This chapter, in particular, seeks to answer the following questions:

4. What clusters of public opinions can be extracted from social media discussions about IP location? What are the spatial-temporal variations of the discussions?

5. Do netizens believe that IP location is an effective approach to counter disinformation? What are their opinions regarding the balance between anti-disinformation efforts and geoprivacy protection?

Chapter 5 then analyzes geoprivacy concerns of Chinese individuals via an online survey. Ordinal logistic regression is implemented to measure the relationship between privacy knowledge, attitude, behaviour, and their moderating factors. The regional variation in geoprivacy concerns is a noteworthy finding, challenging the conventional assumption of national conformity. The research questions addressed in this chapter are as follows:

6. What factors influence individuals' protective behaviours about their geoprivacy? Do these factors include privacy knowledge and attitudes, demographic variables (such as age, gender, and geographic origins), or the IP location feature?

Chapter 6 contributes to the broader discourse on geoprivacy by discussing the legal implications of the IP location feature in the context of the Civil Code of the People's Republic of China, as well as future research directions concerning geoprivacy behaviours. The concept of place-based privacy is proposed to integrate the key attributes of the tension field and establish a connection with the content covered in the previous chapters, thereby completing a full circle of discussion on geoprivacy.

Finally, **Chapter 7** summarizes the dissertation by connecting the motivations and rationales between manuscripts. The chapter underscores the discovery of spatial variations in geoprivacy attitudes from Chapter 4 and 5 and highlights prospective research areas, such as tailoring privacy recommendations through platial information and developing the field of feminist geoprivacy. The chapter concludes by reiterating the social values associated with geoprivacy.

[8]IP location is a feature mandated by the Chinese authority in 2022 that involuntarily discloses users' provincial-level locations on Chinese social media (Cyberspace Administration of China, 2022).

Chapter 2

Literature Review

This chapter serves as a high-level literature review for the dissertation, providing readers with essential insights into geoprivacy. The chapter starts with an analysis of privacy concerns from the physical world to the information age, acknowledging the cultural specific nature of this evolving concept. The chapter then introduces the definitions of the key concepts, followed by a comparative analysis of data privacy concerns. Subsequent chapters 3, 4, and 5 each contain their dedicated review sections, which address detailed research questions accordingly.

2.1 Understanding Privacy

Privacy is a multifaceted and intricate concept (Solove, 2005). Acting as an overarching term and a collection of interests, privacy covers various situations (Waldman, 2018) and represents a group of interrelated notions rather than a single idea (Solove, 2005). Privacy is also an evolving concept. The contemporary interpretation of "privacy protection" during the digital transformation markedly diverges from the conventional definitions expounded in Section 1.2. To gain an in-depth comprehension of our present standing, it is imperative to first examine the notion of privacy in modern history, predating the pervasive integration of virtual technology into our daily lives.

Numerous studies on privacy have drawn upon Westin's seminal work (1967), wherein he elucidates the concept regarding personal agency and control over individual accessibil-

ity. Despite its significance, the rights-based definitions of privacy can be too broad, overly restrictive, or unconvincing when weighed against competing values, such as terrorism prevention (Waldman, 2018). The literature in social and environmental psychology offers some alternative perspectives. Among those, Altman's theory of privacy regulation stands as a popular framework (1975). According to Altman, privacy manifests as a dynamic "regulation process," wherein an individual or collective entity determines their level of accessibility (or "self-boundary") to others contingent on "circumstances" (Altman, 1975). Operating as an "interpersonal boundary-control process," privacy effectively governs and modulates interactions with others (Altman, 1975, pg. 10). The privacy regulation theory also states that privacy is dialectic, optimized, and inclusive. The notion is dialectic because privacy involves both a restraint and a solicitation of interaction, which renders privacy an inherently dynamic process that is time- and context-dependent (Altman, 1975; Cohen, 2012). This characteristic of privacy may explain the phenomenon of the privacy paradox, wherein an incongruity between privacy attitudes and behaviours is observed (see also Sections 3.1.2 and 5.2.1). Moreover, privacy constitutes an "optimizing process" to strike a balance between the level of "desired privacy" in ideal situations and the "achieved privacy" in actual circumstances (Altman, 1975). The need for optimization is partially influenced by the "commodification" of privacy, in which the "neoliberal ethic of productivity" compels users to meticulously weigh trade-offs when making information disclosure decisions (Arora, 2019a). Furthermore, privacy is inclusive and applicable to both individuals and groups. For instance, Proshansky et al. (1970) posited self-identity and autonomy as pertinent constructs of privacy. Altman (1975) also contends that "privacy mechanisms serve to help me define me" (p. 50), underscoring privacy concerns as social imperatives. Although privacy is frequently related to self-determination (Cohen, 2012), group privacy assumes its social values in upholding social justice, mitigating discrimination, and nurturing cohesive communities (Taylor et al., 2016), representing a perspective often underexplored within the domain of privacy scholarship.

The literature in human geography and environmental psychology has also introduced factors influencing privacy attitudes and behaviours that are not explicitly covered by legal studies defining privacy through universal standards (e.g., Warren & Brandeis, 1890). As discussed in Section 1.2, privacy is related to fundamental geographical concepts such as territory, place, and distance. In his *Humanistic Geography*, for instance, Tuan (1976) epitomizes this connection by associating privacy with the pursuit of solitude and the avoidance of social interaction in crowded environments. Likewise, Altman (1975) studied the interplay between privacy, personal space, territoriality, and crowding and argued that privacy is "central to understanding environment and behavior relationships" (p. 6). Not only did he emphasize the dynamic and circumstance-dependent nature of privacy, Altman's framework for achieving privacy also integrates environmentally related behaviours, territorial responses, and cultural mechanisms in addition to verbal (e.g., contents of speech) and paraverbal behaviours (e.g., voice intensity). Examples of these environmental behaviours include maintaining distance from others, setting up parameters of social space, and referencing cultural customs and norms (Altman, 1975; Cohen, 1999). These mechanisms underscore the interconnection between perceived privacy and the physical environment.

Sociologists have suggested another perspective on interpreting privacy distinct from the rights-based approach. Rather than asserting privacy as a universal value, Georg Simmel (1906) regards it as a "universal sociological form" enabling individuals to conceal certain things within specific contexts. Although this distinction may appear subtle, its ramifications are substantial. Such framing imbues the desire for privacy with social values, elevating the concept beyond individual preferences. As a model for societal relationships (Rachels, 1975), privacy enables the maintenance of human connections that would otherwise be unattainable in a world of full knowledge (Waldman, 2018; Merton, 1968). Protecting privacy, in Waldman's view, encourages sharing through alleviating the inherent vulnerability associated with disclosure (2018). Therefore, Waldman (2018) argued for conceptualizing privacy

"as an important part of relating to society, not detaching from it" (p. 35), which resonates with the dialectic attribute of privacy (Altman, 1975). When narrowly construed as an individual entitlement, privacy can be eclipsed by more compelling imperatives, such as counter-terrorism efforts or law enforcement endeavours (Waldman, 2018). Conversely, as a social form, privacy is functional in shaping social structure (Durkheim, 1893). Recognizing that protecting privacy equates to protecting the common good (Citron & Henry, 2010), the collective benefits empower states to adopt a more considerate approach in crafting privacy regulations.

Up to this point, we have discovered from the physical privacy theories that our immediate environment influences our attitudes and behaviours towards privacy and that privacy serves to facilitate rather than hinder social interactions. Do these theories still hold relevance in today's technologically driven landscape? How has the advent of big data and ubiquitous computing reshaped the field of privacy studies? According to Brunton & Nissenbaum (2015), digital privacy advocacy revolves around the reclamation of control over data concerning ourselves. However, Nissenbaum (2020) claimed that privacy is not a right to secrecy or control, but rather a right to "appropriate flow of personal information" (p. 127). In her theory of privacy as contextual integrity, *privacy* is defined as "context-relative information norms" that manage the circulation of personal information within specific social contexts, including both the collection and dissemination of information (Nissenbaum, 2004). While the influence of place, politics, convention, and cultural expectations has been acknowledged in shaping privacy contexts, Nissenbaum (2004) did not favour cultural relativism but believed in universalism of contextual integrity across cultures. However, the systematic norms she proposed, namely appropriateness and flow or distribution of information, are inherently subjective and pose challenges in legal codification. The social network theory aims to address this challenge. As noted by Strahilevitz (2005), the probability that a given piece of information would circulate within a given group of individuals and reach

a broader audience should determine the categorization of information as public or private. This theory can assist judges in determining whether information, once initially disclosed, was presumably to become public irrespective of any subsequent disclosures, which affords a legal basis for decisions regarding information privacy (Waldman, 2018). In her elaborations of contextual integrity, Nissenbaum (2004) did account for the dynamic and evolving nature of privacy. She asserted that instances of privacy invasions can be considered when established norms within a specific context are disrupted by novel interactions or technologies. This deliberation renders her theory flexible and adaptive to evolving societal development (Waldman, 2018). For a more detailed categorization of digital privacy perceptions, Egan (2022) suggested looking into individuals' level of digital experience because those with a high level of internet proficiency may develop a different perspective on privacy in the digital space compared to their expectations in the physical world.

It is concerning that culturally specific expectations of privacy are often overlooked in digital privacy research despite the recognized influence of context on privacy regulations. In fact, not only is privacy considered a foreign concept in China (see Section 4.2.1), but the term also lacks a direct translation in the majority of the world's languages (Miller et al., 2016). Critics thus argue for a culturally relativistic approach to privacy, emphasizing the need to acknowledge the distinctiveness of each culture and exercising caution when attempting to superimpose the orientation of one culture onto another (Herskovits, 1949; Altman, 1977; Segall et al., 1998). As an illustration, information-sharing behaviours can exhibit significant cultural disparities: the percentage of individuals who opt for complete online disclosure is notably higher in Saudi Arabia compared to the figures in the United States and France (Arora, 2019b). Regrettably, cultural relativism may not receive sufficient consideration in the context of the globalization of privacy, where regulations such as the General Data Protection Regulation (GDPR) are applied globally, and Western ideologies are reinforced repeatedly by citations in the literature (Egan, 2022). As Altman (1977)

stated, privacy is both culturally pervasive and culturally unique. While all cultures possess the capacity to regulate privacy, the specific mechanisms employed to achieve privacy may differ. Consequently, privacy embodies a spectrum of diverse values that demands pluralism rather than a collection of shared values that requires unification (Solove, 2008).

Indeed, the concept of privacy has primarily been viewed through an ethnocentric lens, prompting a call for the decolonization of privacy within media studies (Arora, 2019a). Theories in digital privacy have been constructed based on the analysis of privacy attitudes and behaviours of Western-based, white, and middle-class demographics (Chakravartty et al., 2018; Taylor, 2017). This trend tends to go unnoticed, overshadowed by the "deeply structured, essentializing, and historically reproduced power asymmetries within social and technical norms, knowledge, values, and infrastructures" (Arora, 2019a, p. 367). Given the widespread datafication of the population in the global south by Western monopolies (Dourish & Mainwaring, 2012), the process of decolonizing privacy involves "dismantling essentialisms that are regurgitated through scholarship" (Arora, 2019a, p. 366), urging us not to generalize privacy expectations based on demographics and cultures (Arora, 2019a; Nissenbaum, 2020). Arora (2019a) also underscored the danger of a capitalistic worldview. The market-driven neoliberal ideology treats privacy as an exchangeable commodity based on rational decisions (e.g., Acquisti et al., 2013), which presents challenges for the institution of inclusive privacy policies. Finally, privacy in feminist studies has long been perceived as "oppression by patriarchal systems" (Arora, 2019a, p. 370) rather than a matter of personal choice because of the historical confinement of women to domestic environments (Gavison, 1992). In this context, social norms take precedence over individual consent, and women's information disclosure behaviours are often constrained by their roles in the family and their reputation (Arora & Scheiber, 2017). Hence, it is essential to consider feminist perspectives alongside non-white and non-market-driven viewpoints in our discussions of privacy.

2.2 Key Concepts

The following concepts are essential for studying geoprivacy from a cognitive aspect. This section will define these concepts and their synonyms relevant to this dissertation.

Information privacy Information privacy, also known as data privacy or digital privacy, is the counterpart of physical privacy. As a traditional concept, physical privacy pertains to concerns about access to private space. Information privacy, on the other hand, relates to concerns about access to personally identifiable information (Smith et al., 2011).

Geoprivacy The concept of geoprivacy is closely related to *geodata* or *geoinformation*. As such, the discussion of geoprivacy in this dissertation leans towards *information privacy* instead of privacy in general. Different types of geodata can be related to individuals. According to Nouwt (2008), geodata becomes *personal data* when it is linked to "an identified or identifiable natural person". The inclusion of "locations of people" turns geodata into *location data*. Individuals' location history can also be discerned using *traffic data*, such as data logs in mobile communications, which can be mapped to *movement data* that indicates the trajectory or the duration of an individual's movement. In this dissertation, *geoprivacy* is defined as protecting information privacy concerning geodata (Nouwt, 2008)[9].

Location privacy The term location privacy is frequently used interchangeably with geoprivacy (e.g., Keßler & McKenzie, 2018). However, the former concept has a narrower scope. As defined by Beresford & Stajano (2003), location privacy refers to "the ability to prevent other parties from learning one's current or past location". The definition focuses on protecting personal location data but does not consider when location data needs to be preserved

[9]This universal definition of geoprivacy does not contradict the culturally relativistic view of privacy outlined in Section 2.1. Essentially, the concept itself is universally applicable, but the prioritization of privacy relative to other competing values is culturally specific.

in what context. This contextual dimension of information privacy will be discussed along with geoprivacy in Chapter 3.

Disclosure control Disclosure control is a set of statistical techniques. The goal of these methods is minimizing the risk of re-identification of individuals or entities while maximizing the amount of information in data releases (Hundepool et al., 2010). Disclosure control methods can be perturbative or non-perturbative. The former introduces noise (or error) in data, while the latter suppresses or aggregates data (Hundepool et al., 2010). Both types enhance confidentiality in data releases.

Privacy concern Privacy concern, according to Tan et al. (2012), refers to "the degree to which a user believes using a system would result in a loss of control over their personal information." The term relates to humans' mental desire for privacy. The subsequent concepts are closely linked to privacy concerns.

Knowledge Privacy knowledge, occasionally known as privacy literacy (Park & Jang, 2014) or privacy awareness (Correia & Compeau, 2017), potentially influences people's level of privacy concerns. In social psychology, this type of knowledge is the construct of *attitude-relevant knowledge*, which is defined as "the number of attitude-relevant beliefs and experiences that come to mind when encountering an attitude object" (Fabrigar et al., 2006). Here, privacy knowledge can be categorized into declarative knowledge, such as privacy rights and risks, and procedural knowledge, such as skills about privacy-preserving functions on the Internet (Debatin et al., 2009; Park, 2013; Park & Jang, 2014). Further details regarding privacy knowledge will be discussed in Chapter 5.

Perception Psychologists view perception as a subset of cognition. Individuals perceive the world through their senses (i.e., touch, smell, hearing, and sight) by receiving stimulus input

(Golledge & Stimson, 1997). This inferential process interprets, categorizes, and transforms information signals into perception (Werner & Kaplan, 1963). Not all senses play an equal part in perception formation. Environmental information, for example, can be primarily acquired secondarily through sources like social media or human conversations. This action also constitutes a form of perception. *Simultaneity* is a key property of perception (Ittelson, 1960). In geography, perception can be viewed as "the immediate apprehension of information about the environment by one or more of the senses" (Golledge & Stimson, 1997). The immediacy of perception, when considering privacy, is associated with privacy violations in the immediate surroundings and can prompt immediate privacy protection behaviours.

Attitude According to Golledge & Stimson (1997), attitude is "a learned predisposition to respond to a situation in a consistent way". Compared to perception, the distinction between the two is that attitude is relatively permanent. In other words, the mental structure persists even without stimuli. Geographers have evaluated perception in a broader context (Downs, 1981), essentially treating the term as attitude. The two concepts are, therefore, used interchangeably in this dissertation, although their meanings are not precisely identical. Individuals' attitudes are reflected through their behaviours. The "internal mental life" of a person, in this sense, manifests as their "overt behavioural responses" (Gold, 1980).

Behaviour Behaviour is generally defined as "observable actions ... taken by individuals" (Dienlin & Trepte, 2015). Information privacy behaviour in this context refers to the action of "limiting self-disclosure or ... withdrawing from interactions with others" (Dienlin & Trepte, 2015; Altman, 1975). Thus, the concept is relevant to information disclosure decisions (Gerber et al., 2018) that aim to *protect* and *control* personal privacy. The relationship between privacy knowledge, attitude, and behaviour will be analyzed in Chapter 5.

2.3 Privacy Concerns Across Nations

With the key concepts clearly defined, the scope of the dissertation has been identified. The next step is to demonstrate the importance of this topic. Given the variability in internet penetration rates across the globe, there exists a potential "information cocoon" effect[10] wherein we are immersed in media coverage of privacy news primarily within developed countries. This situation raises the pivotal question: *Is information privacy a universal concern that goes beyond geographical boundaries?* As a result, in this section, we compare privacy concerns among global citizens to give prominence to the urgency of studying privacy concerns in the present time. The section starts from a North American perspective, summarizing the survey results from Americans and Canadians. Subsequently, a global review illustrates the varied privacy concerns across nations[11].

2.3.1 Americans and Privacy

Pew Research Center conducted a survey in June 2019, shedding light on the prevailing privacy concerns among American adults (Auxier et al., 2019). More than 60% of respondents believed that it was impossible to lead their daily lives without having their data collected, irrespective of whether it was by enterprises or government authorities. A similar sentiment was observed regarding data usage, where the majority expressed worries (79% for companies and 64% for government).

In terms of trust, 79% of respondents lacked confidence in companies' ability to take responsibility when their personal information was misused or compromised. Moreover, com-

[10] An *information cocoon* arises from a combination of active user choices and passive algorithmic decisions. It is formed by platforms' selective display of information to their users, where the content is tailored based on users' expressed interests and preferences (Sunstein, 2006).

[11] I chose to survey the opinions of individuals from both the United States and Canada given the location of my institution. Put differently, the readers of the dissertation are likely to be interested in learning more about the privacy attitudes of their neighbours. After establishing a common understanding toward privacy in North America, the subsequent section introduces fresh perspectives from other nations.

pared to five years ago, 70% of respondents felt that their personal data was now less secure. Despite these high levels of privacy concerns, a large portion of the sample demonstrated a lack of interest in reading privacy policies and terms of service. Only 22% of respondents claimed that they "always" or "often" read a company's privacy policy before agreeing to it, while an additional 38% said they sometimes check it. Among those who do read, merely another 22% thoroughly review the terms and conditions.

Regarding declarative knowledge, the majority (63%) of respondents stated that they understand "very little" or "nothing at all" about privacy laws and regulations. Despite this lack of awareness, some respondents acknowledged the benefits of pervasive data collection in some scenarios, such as sharing students' data for educational improvements or collecting citizens' data for terrorism prevention.

The survey also revealed interesting variations across demographic groups. For example, regarding age, older Americans felt they had less control over their personal data, perceived fewer benefits from data collection, and paid closer attention to privacy news than their younger counterparts. In terms of race, Black Americans displayed greater sensitivity to governmental surveillance and reported encountering identity theft more frequently (20%) compared to Hispanic (7%) or White (6%) respondents.

2.3.2 Canadians and Privacy

The Office of the Privacy Commissioner of Canada conducts a biennial survey to gain insights into privacy issues and awareness of privacy rights among Canadians. The most recent survey, conducted in 2022 (Phoenix SPI, 2023), shows high privacy concerns among Canadian respondents. A notable 93% of participants expressed varying degrees of concern, with 38% stating they were extremely concerned. The primary worry centred around the tracking of online activities and mobile communications by companies or organizations (91%), with a

specific focus on how this information is utilized for profiling (89%) and decision-making (87%) purposes, such as insurance claims or health coverage.

Regarding respect for privacy rights, 39% of respondents demonstrated a lack of confidence in companies, aligning with the findings from the American survey. However, more than half of the respondents (58%) expressed trust in the federal government. Social media companies received the lowest trustworthiness rating (10%) in terms of personal information protection, followed by big tech (34%), retailers (36%), and internet service providers (41%). The government (80%), banks (76%), and law enforcement (76%) received the highest ratings for their efforts in safeguarding personal information.

Regarding privacy-related behaviours, the majority of respondents exhibited proactive measures to protect their privacy. These include adjusting privacy settings on social media accounts (75%) and refraining from providing personal information to businesses or organizations due to privacy concerns (74%). A smaller percentage reported deleting or discontinuing the use of a social media account due to privacy concerns (50%) or ceasing transactions with companies that experienced privacy breaches (38%). About one-third of respondents (32%) stated that they had "raised a privacy concern with a company or organization."

In comparison to the American survey (Auxier et al., 2019), the Canadian respondents displayed higher levels of privacy awareness and an increased tendency to implement privacy protection practices. Approximately half of the Canadian respondents (51%) reported having "good" or "very good" knowledge of their privacy rights, and a noteworthy 70% indicated that they "sometimes" or "always" read privacy policies, surpassing the corresponding figures from the American survey. Among those who only sometimes read privacy policies, the most frequently cited reason (46%) was that the policies were excessively lengthy.

2.3.3 Global Review of Privacy Concerns

The summary of the following three surveys expands the scope of the analysis from North America to the global south [12]. The Centre for International Governance Innovation (CIGI), in collaboration with Institut Public de Sondage d'Opinion Secteur (Ipsos), conducted five waves of surveys about internet security and trust involving more than 25,000 internet users. The latest wave, concluded in 2019 (Ipsos, 2019), indicates a rising trend in global citizens' privacy concerns. Overall, 78% of the respondents expressed at least some degree of concern about their online privacy. Figure 2.1 displays the diversity of privacy concerns worldwide. Notably, developing economies such as India, Nigeria, and Mexico displayed the highest concerns, with Egypt and Hong Kong (China) topping the list at 96%. Counter-intuitively, European nations and members of the Five Eyes alliance demonstrated lower levels of privacy concerns compared to their developing counterparts. Mainland China, in contrast to Hong Kong, exhibited a significantly lower percentage of concerned citizens (68%). Kenya was the only economy with less than half of its citizens expressing concern (44%). The survey also reported on how distrust on the Internet influences people's online behaviours. This behavioural change ranged from decreased information disclosure and increased device security measures to self-censorship of online speech and selective usage of online applications (Ipsos, 2019).

The World Values Survey captures public opinions from another perspective. Evolving from the European Values Study[13], the international research collaboration aims to investigate social values among citizens in different countries. In its latest wave (Haerpfer et al., 2022), conducted between 2017 and 2022, the survey introduced surveillance-related ques-

[12] Although China is in the title of the dissertation, this section examines a global context and only mentions China when relevant statistics are present in the surveys. This is because the discussion in Chapter 3 does not exclusively centre on the Chinese population. The justifications for selecting China as the study area are included in Chapters 4 and 5.

[13] `https://europeanvaluesstudy.eu/`

tions in the section dedicated to ethical values and norms. Specifically, question 197 inquired whether respondents believe that their "country's government should or should not have the right to ... monitor all e-mails and any other information exchanged on the Internet," thereby touching upon information privacy concerns. Figure 2.2 illustrates the percentage of respondents who at least somewhat disagree with governmental access to personal information online, indicating a distinctive trend compared to general concerns of online privacy (Figure 2.1). Here, European and North American regions exhibit the highest concentrations of dissent, with Andorra topping the list with 90% disagreements. Within North America, Canadians expressed a higher rate of disagreement (85%) than their neighbours, the United States (75%) and Mexico (74%). In South America, North Asia, and Oceania, although the number of dissenting opinions was relatively lower, the percentage of respondents who believed that the government should not have the right was still more than half. On the other hand, countries in the tropical and subtropical regions, such as the Middle East and Southeast Asia, demonstrated the highest approval rates on this topic, with Myanmar at the bottom with only 11% dissent. Again, polarized opinions were observed within China, with Hong Kong exhibiting a higher level of disagreement (75%) and mainland China displaying a lower level of concern (39%).

We learned from sections 2.3.1 and 2.3.2 that users adapt their online behaviours to protect their privacy. However, the extent of these adaptations may vary between nations. Figure 2.3 provides insights into the percentages of "privacy actives" who had switched organizations they do business with because of privacy concerns (Cisco, 2022). Developing countries demonstrated higher percentages of privacy actives, with India leading at 68%, followed by China at 53%. In contrast, the United Kingdom stood out with the most loyal customers, as only 21% of them switched organizations due to privacy concerns. Similarly, its European neighbours display a similar trend with a lower percentage of privacy actives. Overall, the survey indicates that only 37% of the respondents had taken action.

In conclusion, the question posed at the beginning of this section has been answered: information privacy is indeed a universal concern, and, notably, the level of distress has been soaring over the years. However, as we delve deeper into the data and explore different aspects, variations in privacy attitudes and behaviours emerge between different regions of the world, concerning the degree of trust towards government versus enterprise, and depending on the acceptance level of existing privacy regulations. These variations can be attributed to cultural and geopolitical influences, which will be analyzed in the next chapter. By exploring these aspects, I aim to comparatively examine the complexities surrounding privacy attitudes and to identify potential areas for further research and policy development.

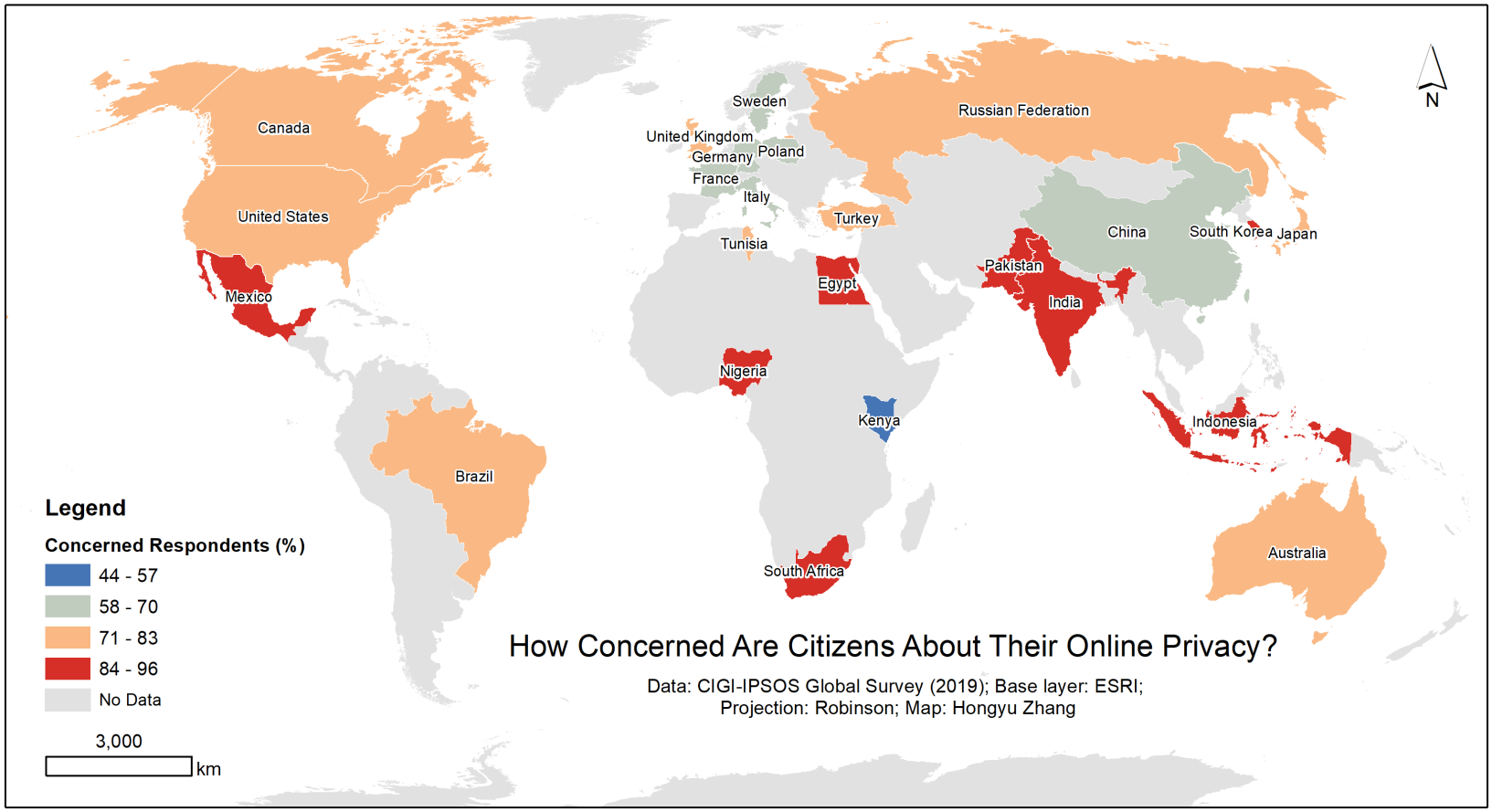

Figure 2.1: How Concerned Are Citizens About Their Online Privacy?

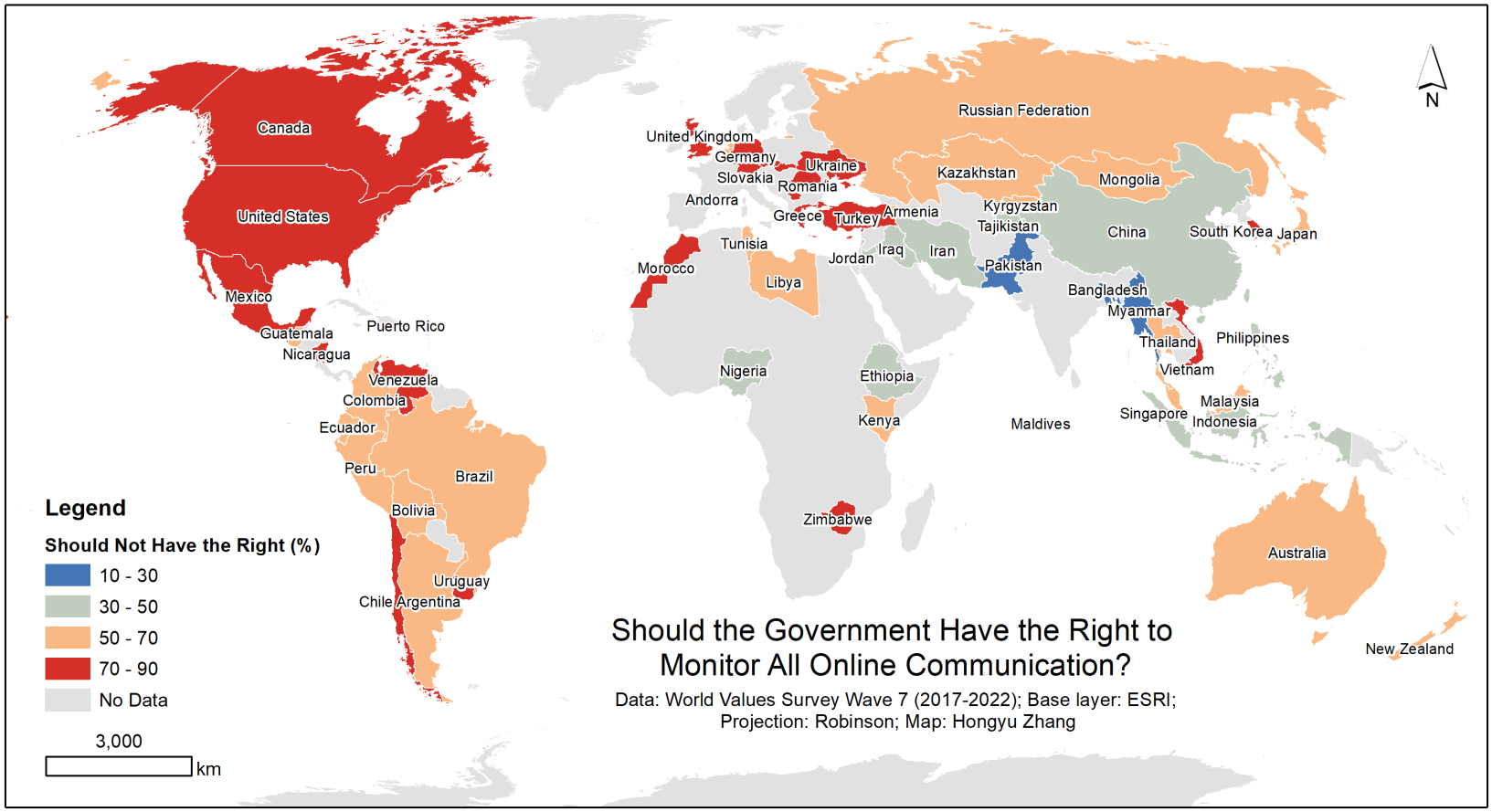

Figure 2.2: Should the Government Have the Right to Monitor All Online Communication?

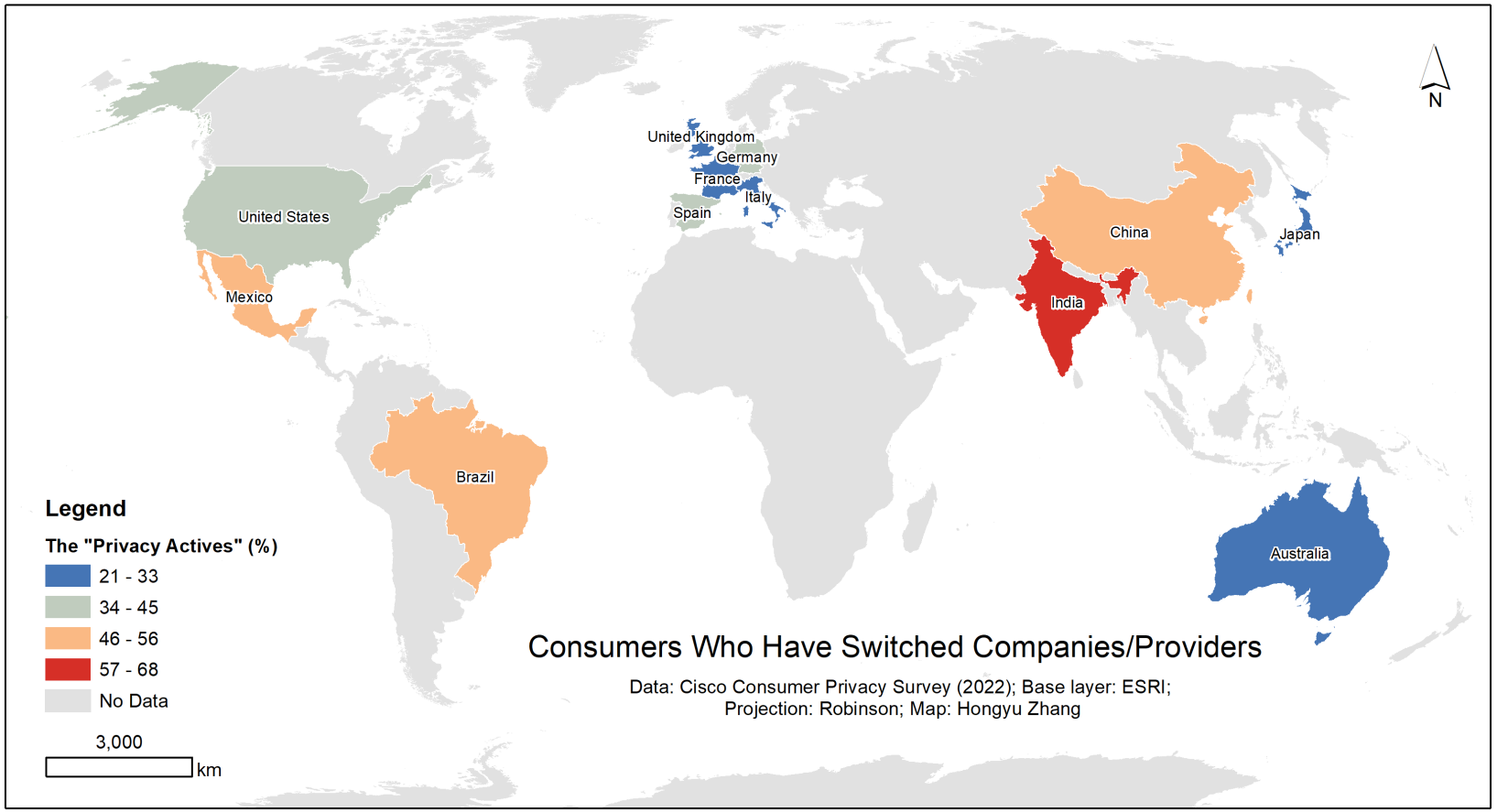

Figure 2.3: Consumers Who Have Switched Companies/Providers

Preamble to Chapter 3

The concept of geoprivacy was defined in Section 2.2. Within the ambit of this chapter, I argue that geoprivacy possesses a uniqueness owing to its ever-changing and context-sensitive nature. While there is a necessity for standardized computational privacy preservation techniques, it is essential to acknowledge that these techniques might not comprehensively address the privacy concerns of all users. Numerous factors, including time, culture, demographics, spatial granularity, and trust, influence individuals' decisions regarding location disclosure. This chapter further advances the exploration of geoprivacy from a cognate-based standpoint. The objective is to rehumanize this field by emphasizing its contextual, cultural, and economic dimensions, thereby highlighting the distinctiveness of geodata in privacy studies. The outcomes of this chapter acknowledge spatially nuanced perceptions regarding geoprivacy, with the human-centred approach emerging as an essential mechanism for preserving geoprivacy.

Chapter 3

Rehumanize Geoprivacy[14]

Abstract

Traditional boundaries between people are vanishing due to the rise of Internet of Things technology. Our smart devices keep us connected to the world, but also monitor our daily lives through an unprecedented amount data collection. As a result, defining privacy has become more complicated. Individuals want to leverage new technology (e.g., making friends through sharing private experiences) and also avoid unwanted consequences (e.g., targeted advertising). In the age of ubiquitous digital content, geoprivacy is unique because concerns in this area are constantly changing and context-dependent. Multiple factors influence people's location disclosure decisions, including time, culture, demographics, spatial granularity, and trust. Existing research primarily focuses on the computational efforts of protecting geoprivacy, while the variation of geoprivacy perceptions has yet to receive adequate attention in the data science literature. In this work, we explore geoprivacy from a cognate-based perspective and tackle our changing perception of the concept from multiple angles. Our objectives are to rehumanize this field from contextual, cultural, and economic dimensions and highlight the uniqueness of geodata under the broad topic of privacy. It is essential that we understand the spatial variations of geoprivacy perceptions in the era of big data. Masking geographic coordinates can no longer fully anonymize spatial data, and targeted geoprivacy protection needs to be further investigated to improve user experience.

3.1 Introduction

While the concept of a location-based service (LBS) existed prior to the emergence of global positioning systems (GPS), it was only after the launch of these technologies, and subsequent discontinuation of selective availability, that these services emerged as the robust technologies that we know them to be today. Realizing the limitations of GPS, such as slow transmission rates (Wicker, 2012), researchers developed alternative methods such as cellular trilateration and Wi-Fi positioning to determine an individual's locations. A plethora of research went into developing more precise location-identification methods to provide contextually relevant information for services such as navigation, restaurant recommendations, etc. The emergence of Web 2.0 had a significant impact on location-identification, encouraging users themselves to *participate* by contributing location information back to location-based services. Developers quickly discovered that the inclusion of *user-generated content* (UGC), along with sensor-based technologies, substantially improved the precision and response speed of LBS. While participatory mapping and the subsequent use of volunteered geographic information have undoubtedly contributed additional data to improve the quality of LBS (e.g., the case of OpenStreetMap (H. Zhang & Malczewski, 2019)), it has led to considerable privacy concerns. Over the past few decades, we have become more aware of the underlying privacy risks associated with location technologies and the adverse societal and personal effects. As Wacks (2015) suggests, it is the possibility that "I am being watched" that makes people worry about their privacy. This concept of being watched is a topic that we will return to throughout this manuscript, as well as some of the behavioural changes that have emerged because of these privacy concerns.

Why is the privacy of our *location* information unique, though? Our location is inherently tied to our identity. Socio-demographic properties such as race, income, education, and many

[14] A version of this chapter appears in Zhang, H., & McKenzie, G. (2023). Rehumanize geoprivacy: from disclosure control to human perception. *GeoJournal*, *88*(1), 189–208.

others correlate significantly with location (Zhong et al., 2015). Most would agree that a malicious actor gaining access to one's credit card information or government identification number is a substantial breach of privacy with lasting impacts. However, public exposure of how, when, and where one's child goes to school is arguably more valuable and likely of greater concern to a parent. In a similar vein, while knowledge of one's visit to a gay bar in a major U.S. city may not be of concern to many, to those in regions where people with specific sexual preferences may be discriminated against, the privacy of this information is of paramount concern. Compared to privacy defined more broadly, geoprivacy is unique in that it involves a specific set of characteristics. Location data and privacy requirements are always changing and context-dependent. A high degree of geoprivacy preservation is also often contradictory to high quality of service (QoS) (Wang & Liu, 2009). Commercial entities and government agencies increasingly view location data as a commodity to be traded (often for financial gain or national security), and legal developments are already falling behind technological advancements (Keßler & McKenzie, 2018). At the time of writing, we are observing a privacy battle playing out in the media, the courts, and public opinions, with large corporate entities such as Apple, Google and Facebook attempting to balance user privacy with advertising revenue (B. Chen, 2011). All of these facets indicate that now is a necessary time to revisit the topic of geoprivacy and think beyond data-centric anonymization approaches. With this in mind, the objectives of this paper are to

- Provide an overview of the recent literature pertaining to the broad topic of privacy, framed from a big spatial data perspective,
- Examine and identify what makes geoprivacy unique, from a human geography perspective, and
- Discuss how our perceptions of geoprivacy have substantively changed nowadays and how they vary around the globe.

The remainder of this article is organized as follows. Section 3.2 identifies people's geoprivacy concerns, elaborates recent anti-geosurveillance attempts, and redefines geoprivacy from a *platial* perspective. Section 3.3 discusses the current context behind geoprivacy perceptions and how people's behaviour is impacted in this revolutionary environment. Section 3.4 examines spatial variations of geoprivacy from cultural, demographic, and legal perspectives, while Section 3.5 presents geoprivacy from an economic view and explores how geoprivacy is priced. Finally, Section 3.6 concludes the article and provides an outlook of future trends.

3.1.1 What Is Privacy?

A consensus on the definition of privacy has proved difficult to achieve (Solove, 2005) even though the notion has been extensively examined in many social science fields such as philosophy, psychology, sociology, and law (Smith et al., 2011). Broadly stated, privacy involves either a *value* or *cognate*-based definition. A value-based definition refers to privacy as a *human right* or a *commodity*. For example, Warren & Brandeis (1890) stated that privacy is "the right to be let alone", while Davies (1997) viewed privacy as merchandise to be traded in information markets. On the other hand, a cognate-based definition categorizes privacy as a *state* of mind or *control* of private information (Westin, 1967). One example is that psychologists and cognitive scientists linked privacy to personal perceptions and cognition (Miltgen & Peyrat-Guillard, 2014). Though many have attempted to develop a succinct definition, Johnson (1992) argued that "contexts and situations" are essential conditions of privacy. Johnson's opinion aligns with our view of geoprivacy, that the privacy of one's location information is almost entirely dependent on the context in which it is collected and shared. Past work has identified specific features of our environment that influence an individual's perception of privacy such as time, location, occupation, culture, and rationale (Bansal & Zahedi, 2008). Additional factors impacting people's privacy concerns are summarized in

Figure 3.1 (Smith et al., 2011; Li, 2011; Miltgen & Peyrat-Guillard, 2014).

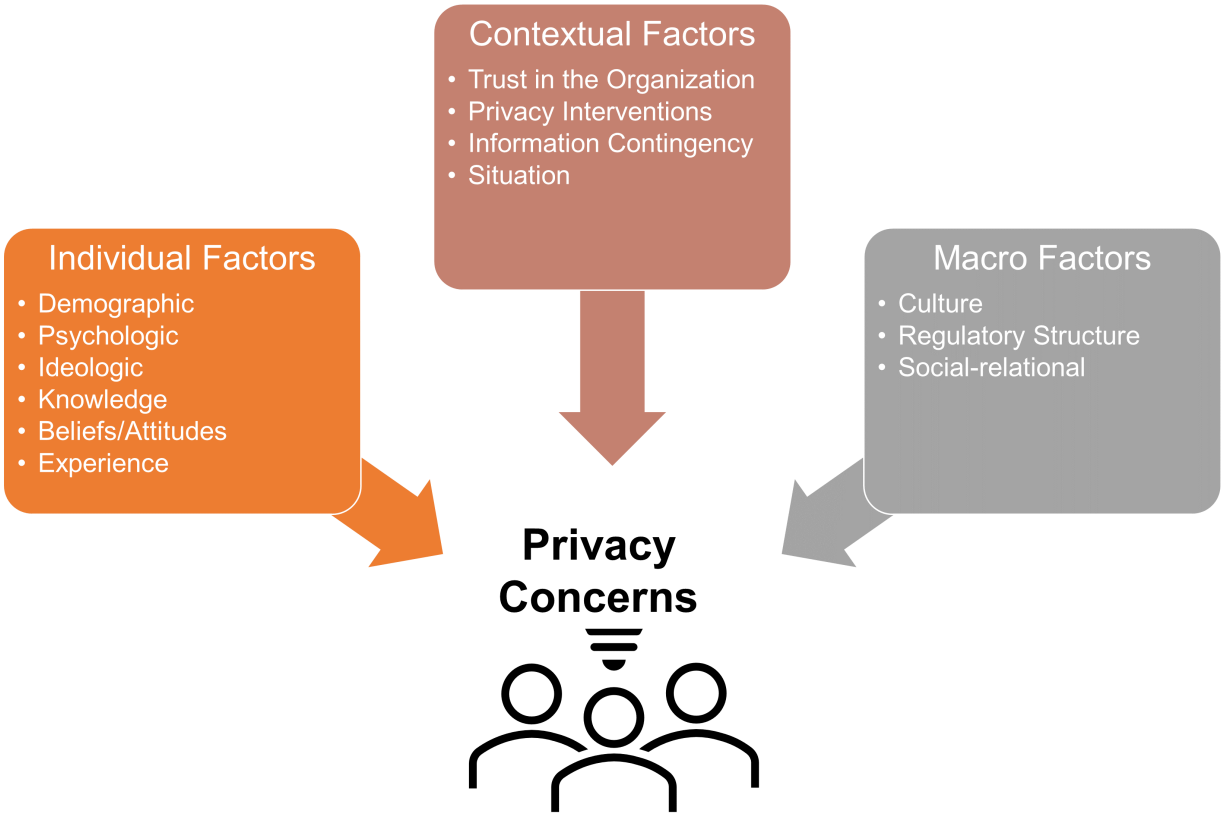

Figure 3.1: Factors That Influence an Individual's Perception of Privacy (Adapted from Smith et al., 2011; Li, 2011; Miltgen & Peyrat-Guillard, 2014)

The concept of privacy continues to evolve due to its fundamental basis in personal perceptions and potential threats (Wacks, 2015). Essentially, privacy entails possessing anonymity (remain secret) and autonomy of actions (which are not influenced by external forces) (Crampton, 2015). Historically, we viewed privacy as a "property of the built environment" (Georgiou, 2006, p. 13), believing that walls and borders preserved privacy and shielded us from outsiders. This is reflected in the now outdated mantra, "a man's house is his castle" (Coke, 1979). This primitive concept of privacy has drastically changed with technological advances, as contextually-aware devices connected to the Internet no longer respect physical boundaries.

The rise of big data has also shifted our definition and understanding of privacy. As Rzeszewski & Luczys (2018) point out, every piece of personal identifiable information is already in a database somewhere in the world. This knowledge, in conjunction with the "privacy paradox" (to be discussed in the next section), has led to a high level of anxiety concerning big data (Leszczynski, 2015; Crawford, 2014). First, how big data is processed is not transparent (Richards & King, 2013). Users are often captivated by elegant user interfaces and convenient service applications (Kaasinen, 2003; Kitchin & Dodge, 2014; Thrift, 2004) without paying attentions to terms of service and their rights of personal location information. The events and actions taken behind the scenes typically occur in a "black box" involving proprietary algorithms and datasets. It is only when this process fails that users are provided a glimpse behind the curtain. Second, big data "constitutes identity" (Richards & King, 2013). While people try to remain anonymous, the sheer magnitude and coverage of big data enable researchers, advertisers, and attackers to make personal identifiable conclusions. Third, control of big data lies with influential organizations instead of average citizens. As a result, users often feel coerced when it comes to necessary changes of terms and conditions in the services they rely on. This ubiquitous data collection, unsurprisingly, has led to an increase in public discussion over our data privacy.

3.1.2 The Privacy Paradox

The privacy paradox describes the inconsistent nature between privacy attitudes and behaviour (Kar et al., 2013; Kokolakis, 2017). People both worry about their privacy and are eager to experience new services simultaneously; they want to have control of their personal information but also want to engage in social interaction through sharing private matters (Nakada & Tamura, 2005). The quintessential example of this is that although users are anxious about their privacy, the vast majority of users never even skim the End User License

Agreement (EULA) of an application or service before choosing "Yes" (Lin et al., 2012). This phenomenon reflects what is colloquially referred to as "Fear of Missing Out" (FoMO) (Przybylski et al., 2013), choosing to benefit from a service while actively ignoring the privacy costs. When it comes to location sharing, the incentives of Quality of Service (QoS) improvements frequently outweigh privacy concerns (Keßler & McKenzie, 2018).

The privacy awareness gap is also a concern. On the one hand, people often share their locations unknowingly and can be unaware of the potential risks of personal location disclosure (Keßler & McKenzie, 2018). On the other hand, users are often data consumers and producers at the same time and possess limited technical knowledge to make the correct decision about their privacy settings (Rzeszewski & Luczys, 2018). While many people fit into one of the categories above, some are only worried about geoprivacy as data creators (their own privacy) but not consumers (other's privacy). In simple terms, the privacy paradox can be explained by our humanity: the desire for new experiences and the ignorance of unknown risks, push individuals to behave contradictorily from their attitudes.

3.2 Dimensions of Geoprivacy

3.2.1 What Are We Afraid of?

Why do we care about geoprivacy, and what exactly are we afraid of? According to Culnan & Armstrong (1999), Milberg et al. (2000), and Malhotra et al. (2004), information privacy concerns are individual's subjective beliefs of possible invasions of privacy in the future. Citizens prefer to remain anonymous, unidentifiable, and unfollowed. Most prefer a visible background processing service and control of their personal data. Instead, increased occurrences of data breaches over the past few years (e.g., the data leak of 533 million Facebook users in March 2021 (McCandless et al., 2021)) have led to lower expectations and lack of

trust. Here, *trust* is defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (Rousseau et al., 1998, p. 395). Trust has been found as a mediator (Malhotra et al., 2004; Metzger, 2004) or argued as a moderator (Joinson et al., 2010) between people's privacy attitudes and self-disclosure intentions. In a low-trust environment, privacy concerns are one of the determinants of people's behaviours of sharing personal information online, whether voluntarily (Sui et al., 2012), coercibly (McKenzie & Janowicz, 2014), or unknowingly.

Nowadays in the digital age, people's privacy concerns are influenced by factors such as personal identification, tracking and profiling, transparency, controllability, and data leaks (Alrayes et al., 2020; Clarke, 1994). User identification and targeted profiling have unavoidably become much easier with the emergence of big data. For instance, research has demonstrated that with access to only a 5-digit ZIP code, one's gender, and date of birth, 87% of Americans can be uniquely identified (Sweeney, 2000). Using the same identifiers, the percentage of uniqueness is about 98% for Montrealers in Canada (El Emam et al., 2011). The identification is accomplished by linking information across multiple data sources and inferring user interests. Not only is this shocking to most, but the process of inference can also be dangerous, leading to erroneous assumptions and attribute assignments. The practice of a company or agency secretly sharing a user's locations is also prevalent. Users typically have few methods for confirming the privacy compliance statuses of location-based services (Keßler & McKenzie, 2018). Using spatial information collected through applications, attackers can infer sensitive data such as gender, educational background, age, and sexual orientation (Rossi & Musolesi, 2014; Zhong et al., 2015). Additionally, researchers have demonstrated the ability to estimate a user's home locations (Gu et al., 2016), social relationships (Sadilek et al., 2012), as well as probabilities of returning to a venue (Preoţiuc-Pietro & Cohn, 2013) based solely on geotagged social media contents.

Alrayes et al. (2020) summarized the issue of location disclosure through three dimen-

sions (Figure 3.2): what's being shared (data), who has access (visibility), and how much does a user know (awareness)? Today, data include various attributes ranging from spatial location information (e.g., geographic coordinates, regions, places) to social-semantic data such as social relationships and shared media (e.g., text, images or videos). Temporal data is also highly indicative, containing information related to trajectories, frequency of visits, the sensitivity of places, and co-location of users. With respect to visibility, Smith et al. (2011) classified this dimension into social privacy (e.g., visible to public or restricted groups) and information privacy (e.g., privacy policies). Awareness can be delineated by what are referred to as *modes*: *Realistic Mode*, where users are only aware of what they have chosen to share, and *Attacker Mode*, where information is inferred based on additional content and attributes. Together, it is easy to realize that we are living in an omni-connected world: the pervasive surveillance technologies and the lack of mental boundaries make people question their individuality or whether "self" still holds its integrity. In fact, fear from geosurveillance has forced advocates and minority groups to change their behaviours (Clarke & Wigan, 2011), which can be argued that parts of their "selves" have been lost in the process of anti-geosurveillance.

3.2.2 Anti-geosurveillance Attempts

Our digital environment is designed with convenience but not privacy in mind, which serves to exaggerate people's fear of privacy loss. Due to many factors, most notably outdated laws and limited penalties (Surden, 2007), user privacy is not a top priority for many service providers. Moreover, when outsourcing proves to save development costs, the security of a product becomes more difficult to monitor (Crampton, 2015). Provided that someone is concerned about the risks associated with personal location data, how should one protect their geoprivacy in this context?

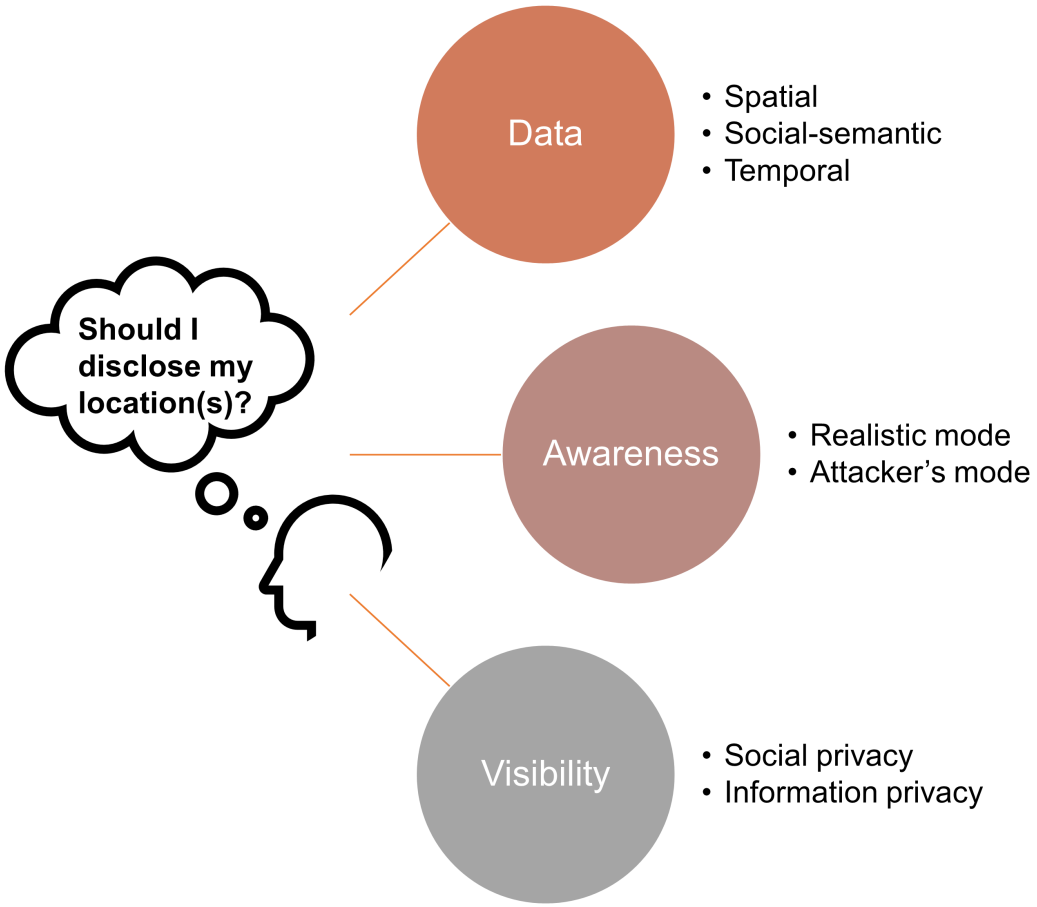

Figure 3.2: Dimensions of the Location Disclosure Problem (Adapted from Alrayes et al., 2020)

Swanlund & Schuurman (2019) provide a set of short-term tactics and long-term strategies to resist geosurveillance. The tactics being proposed include *data minimization*, *obfuscation*, and *manipulation* (Table 3.1). Data minimization is the most straightforward method (e.g., cash transactions), where this minimization effort is similar to suppression in statistical disclosure control where data are not released (Sweeney, 2002). Caching-based mechanisms used a comparable logic to reduce the number of communications with (untrusted) LBS servers (Niu et al., 2015; Amini et al., 2011). While obfuscation and manipulation sound similar, they are different as obfuscation adds random noise (e.g., the Tor network), and manipulation creates specific patterns (e.g., Virtual Private Network (VPN) or fake GPS

location applications). Cloaking based on k-anonymity (Sweeney, 2002), differential privacy (Dwork, 2011), and dummy data (Kido et al., 2005) are three popular obfuscation techniques for LBS. The three techniques are sometimes referred to as location generalization, location perturbation, and location spoofing respectively (Jiang et al., 2021). For continuous LBS (e.g., tracking of vehicle trajectories), mix zones (Beresford & Stajano, 2003) is another widely cited obfuscation technique. We added *encryption* as the fourth type of anti-geosurveillance tactic because encryption algorithms can hide private information from adversaries. Table 3.1 lists notable examples of cryptography-based privacy-preserving mechanisms for LBS. In terms of long-term solutions, the usability of the proposed strategies is debatable. Swanlund and Schuurman's first strategy, destabilizing assumptions behind geosurveillance, cannot be universally applied as privacy is a personal perception. Secondly, alternative private applications are available on the market, but companies face the challenges of small user numbers and subpar service quality. Finally, in addition to strengthening activism, one could argue that it is more important to rebuild trust between individuals and data collectors as high trust may dismiss the impact of privacy concerns on self-disclosure behaviours (Joinson et al., 2010).

Recent studies have found that traditional masking and obfuscation methods may not be enough to protect users' geoprivacy (Keßler & McKenzie, 2018). The digital exhaust from individuals' daily lives contributes additional information that can be used to identify their location information based on non-spatial factors. For instance, research has shown that one's location can be identified based on the textual content and timing of a social media post (McKenzie et al., 2016). Additional studies on user profiling also explored home (Gu et al., 2016) or current location identification (Bellatti et al., 2017; Pontes et al., 2012), future check-in location prediction (H. Gao et al., 2012), social relationship inference (Sadilek et al., 2012), returning probability computation (Preoţiuc-Pietro & Cohn, 2013), and sensitive personal information calculation (e.g., gender, educational back-ground, age and sexual ori-

Table 3.1: Types of Anti-geosurveillance Tactics (Reassembled from Swanlund & Schuurman, 2019; Jiang et al., 2021)

Types	Descriptions	Examples
Minimization	Transfers less data	Cash transactions Caching (Niu et al., 2015)
Obfuscation	Adds random noise	Cloaking (Chow et al., 2011) Differential privacy (Dwork, 2011) Dummy data (Kido et al., 2005) Mix zones (Beresford & Stajano, 2003)
Manipulation	Creates specific patterns	VPN Fake GPS locations
Encryption	Converts plaintext to ciphertext	Space transformation (Khoshgozaran & Shahabi, 2007) Secure multiparty computation (Cramer et al., 2015) Private information retrieval (Chor et al., 1995)

entation) (Rossi & Musolesi, 2014; Zhong et al., 2015). Weiser & Scheider (2014) therefore suggest building a civilized cyberspace to prevent misuse of personal location information. However, a fully self-regulated society is a utopia even in the physical world. Hence, alternative geoprivacy preservation techniques that consider more than geographic coordinates need to be further studied.

3.2.3 Beyond Locations: A *Platial* Perspective on Geoprivacy

Previous researchers have traditionally used the terms *geoprivacy* and *location privacy* synonymously (Keßler & McKenzie, 2018). The concept particularly concerns the control of what spatial data one person shares with others (Duckham & Kulik, 2006; Weiser & Scheider, 2014). This often means that individual locations are categorized into public (e.g., campaign trails) and private (e.g., home addresses) spheres, with precision of locations either being approximate (e.g., city-level) or exact (e.g., coordinates). However, the tradition

of using the two terms interchangeably is perplexing as the prefix "geo" covers a broader domain than "location". When we acknowledge spatial data in this conversation, do we mean a location, a place, or a space? If we refer to location(s), is it a spatial relation, a region, a pair of coordinates, or a trajectory (Purves et al., 2019)? We will try finding answers in the key concepts of human geography in the next paragraphs.

In recent decades a substantial body of literature has emerged comparing the concepts of *space* and *place* (Hamzei et al., 2020). Space is used to describe a geographic region or location. The concept is often "abstract, formalizable, and context-free" (Tenbrink, 2020, p. 5). Places, contrastingly, can be experience-based and have vague boundaries (Tenbrink, 2020). In a modern geographic information system (GIS), space can be referenced by geometric systems such as coordinates, distances, topology, and directions, while places are represented by names, descriptions, and semantic relationships (S. Gao et al., 2013). Table 3.2 lists different properties and metaphors of the two concepts from multiple perspectives. A salient overlap in each column is the divide between public and private. It seems scholars felt a sense of belonging when talking about places, which corresponds to its cognate-based definition. According to Tuan (1990), perception, attitude, and world view all shape people's experience in their surrounding environment or the places in which they exist. While perception is a human's biological feedback from external stimuli, attitude is based on the accumulation of perceptions and cultures in a society. World view, the last impacting factor on the list, is systematic attitude and belief. In short, places are spaces instilled with meaning by those that inhabit or visit locations.

As a result, the notion of *place* is more relevant to our discussion of *geoprivacy* because of its subjective, qualitative, and emotional aspects (Cloke et al., 2013). Yet, the concept is loaded with a wide range of explanations (Goodchild, 2011), so it is better to categorize these related meanings. Agnew (2014) summarized three core meanings of the concept, and his categorization is not obsolete despite of recent technological developments. Place, in Agnew's

Table 3.2: Space vs. Place (S. Gao et al., 2013; Harrison & Dourish, 1996; Tuan, 1977; Hillier, 2007)

Space	**Place**
Accuracy, Precision	Ambiguity, Vagueness
Heterogeneity	Homogeneity
Proximity	Similarity
Absoluteness	Relatedness
Multi-dimension	Order, Hierarchy
A house (the abstract)	A home (the personal)
Freedom (openess)	Security (stability)
Raw material	Decorated space

words, can be a *location*, a *sense of place*, or a *locale*. Here, a *location* is narrowly defined as a pair of coordinates on the earth's surface. A *sense of place* represents people's emotional attachments with places, as well as the role of place in shaping people's identities. A *locale* is a "scale" that sketches people's everyday actions and social interactions (Agnew, 2014; Castree, 2003). Both the second and the third meanings indicate that there are no places without people's activities (for nearby places) or imaginations (for distant or unpopulated places). On the other hand, it is the imaginative and affective dimension of place (Castree, 2003), in addition to the physical dimension, links our social relationships. This interdependency between people and place shows the humanistic value of this concept. Though places are different, their interconnectivity reinforces the effect of globalization (Harvey, 2018). Not only could what happened in one place have significant impacts on another far away, when it comes to people's identity, "routes" can also tell more personal stories than "roots" (Massey, 1997). This time-dependent nature leads us to the durability of place (Anderson, 2008). Purves et al. (2019) argued that "time is inherent to any definition of places" (p. 1175). A "progressive sense of place" (Massey, 2012), as a result, needs to be advocated as it reflects changes in the physical space and personal journeys, and opens people's minds to a wider world.

The word "platial" first appeared in Casey (1993), referencing place-based geographic methods. The field of research is focused on connecting precise locations with human feelings, behaviours, and perceptions. Language is an important medium for expressing one's platial experience, and a considerable amount of research has emerged in this area in recent years (S. Gao et al., 2013; Tear, 2020). Although place-specific language has been examined in the cognitive sciences, human geography, environmental psychology, and the broader humanities, it is a complex phenomenon that has only recently developed as an area of study for data-driven and computational sciences (Tenbrink, 2020). Early work in this area has demonstrated that the influential dimensions to one's platial experience also play a role in identifying one's location. Information such as time of the day, day of the week, and weather all contribute to the probability of someone being at a specific location. Preserving one's geoprivacy thus involves more than simply masking geographic coordinates: attention also must to be paid to non-explicitly spatial data that can be used to identify someone's location (McKenzie et al., 2016). When we look at geoprivacy through the lens of place, the scope of this concept goes beyond locations. As a unique concept, which is comparable to places (Castree, 2003), geoprivacy is emotional, contextual, changing, and profound. People have different level of geoprivacy concerns, but these concerns are never singular and are often shared by a community. In this sense, geoprivacy is not only personal: a group-level investigation is a research direction that is waiting to be explored (Taylor et al., 2016). The consideration of group privacy also implies cultural influences on spatial variations of privacy perceptions.

To conclude our analysis from the platial perspective (Goodchild, 2011), geoprivacy is time-variant, people-centered, and culturally situated. The difference between *location privacy* and *geoprivacy* can be referenced from the comparison between *space* and *place*, where the former is data-centric and the latter is human-centric. We add here that geoprivacy diminishes the moment a location is shared with a third party because an individual has

lost control of the spatial information linked to themselves, and their location is no longer a secret. Any auxiliary information (e.g., social media posts) that aid in probabilistically identifying someone's private places also serves to compromise their geoprivacy. In the next three sections, we will deconstruct this unique concept from contextual, cultural, and monetary facets.

3.3 Contemporary Conditions Behind Geoprivacy

Technological advancement, security, and health concerns are changing our experience of space and our interaction with the world (Evans, 2011). The fast iterations and the constant needs of catching up create not only generation gaps but also the need of revisiting geoprivacy in the current context. In this section, we first discuss the privacy implications of surveillance technologies and big data, then investigate how location-aware technologies have influenced and changed our behaviours.

3.3.1 Surveillance Technologies and Privacy Lost

Security is an obsession in much of the developed world. Constant monitoring and profiling aim to "stop crimes in their cradles," but at the cost of citizens living in what is often referred to as "surveillance societies" (Gilliom, 2001). One might reasonably argue that those of the millennial generation understand they live in an *omniopticon*, which allows "the many to watch the many" (Rzeszewski & Luczys, 2018). The concept is derived from a panopticon, a round-shape prison that simplifies prisoner monitoring. Our willingness to share our personal location information has led to a society of "participatory panopticism" (Rose-Redwood, 2006; Elwood & Leszczynski, 2011), which may be the first time in history that participation benefits both the watchers and the people being watched (Dobson & Fisher, 2007). If we apply this concept of omniopticon to the geography domain, we discover

that emerging technologies have changed the way people perceive their spatial and platial environments. When it comes to sensitive places, even extroverts might be hesitant to share their locations. In response, geographers and sociologists developed the following terminologies and metaphors, namely *geoslavery* (Dobson & Fisher, 2003), *dataveillance* (Clarke, 1988), *geosurveillance* (Crampton, 2003), and *data colonialism* (Thatcher et al., 2016) to emphasize the lack of control of personal location data in the 21st century. Table 3.3 lists the definitions of these concepts.

Table 3.3: Related Concepts in Geoprivacy and Surveillance

Terminologies	**Definitions**
Geoslavery	A practice of master(s) "coercively or surreptitiously" control slave(s) through physical locations (e.g., time of presence and movement trajectories) (Dobson & Fisher, 2003, p. 47).
Dataveillance	"the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988, p. 499).
Geosurveillance	A surveillance action in which space and people are "resources" that need to be politically normalized in security and risk management (Crampton, 2003, p. 137).
Data Colonialism	A metaphor from capitalist expropriation that describes data commodification as "accumulation by dispossession" (Thatcher et al., 2016).

Surveillance societies were a leading contributor to the rise of "big data". Crawford & Schultz (2014) describe three perspectives on big data, which are: A technology that utilizes high-performance computing; an analytical process of data cleaning and comparison; and a "mythology" that more data is better on the road of pursuing "truth, objectivity, and accuracy". Online privacy, as a result, is often violated through (secretly) collecting, trading, and redeveloping personal information (Wu et al., 2011) and was argued to be a major obstruction of location-based services (LBS) dissemination (Gupta et al., 2011). Data mining makes personal data transmission impossible to track and aggravates electronic

surveillance to some extent due to the ability of the watchers to remain anonymous (Wu et al., 2011). What is of increasing concern is the limited control over recent biometric mechanisms such as face recognition and DNA testing (Swanlund & Schuurman, 2019). Compared to fingerprints which require active participation, facial images can be passively collected (Bowyer, 2004). The ability of a malicious actor to remain secret increases its possibility of being abused. DNA testing is also becoming ubiquitous as many customers are paying private enterprises for ancestry tests, in which the practice exposes sensitive genetic data in semi-regulated environments (Naveed et al., 2015). As a fringe area in geoprivacy research, we must realize that biometric data contain numerous regional characteristics of people, and the underlying risks require further scrutiny as related concerns continue rising.

3.3.2 Deception and Behavioural Influences

Access to public location information about friends and strangers influences our behaviour and daily interaction with others (Michael & Michael, 2011; Dearman et al., 2005). Our relationships, our identities (e.g., sexual preference), and our seemingly private decisions (e.g., abortion) may be altered based on the fear of losing geoprivacy (Wacks, 2015). In the early days of social media, you either shared content with everyone on a platform or kept it to yourself. The amount of publicly available content has since declined dramatically after the launch of visibility settings in, for example, Facebook (Stutzman et al., 2013). In recent years we have seen a rise in social media users deleting connections, comments, or even their applications (Alrayes & Abdelmoty, 2014; Boyles et al., 2012), citing anxiety of location privacy (Rzeszewski & Luczys, 2018). In fact, in a recent study of location disclosure based on respondents' willingness to share, privacy-related concerns are at the top (86%). In contrast, only 14% of concerns are about social capital (e.g., whether others like me) (Alrayes et al., 2020). The sensitivity of the place type (public vs. personal places) also plays a vital

role in the justification process with a 31% drop in willingness to share at personal places. In comparison, co-location with a friend has a slight impact (8% increase compared to alone) (Alrayes et al., 2020).

The decision process of location sharing has been explained by the privacy calculus model, which calculates the perceived benefits and privacy risks on user adoption (Culnan & Bies, 2003; Xu et al., 2011; Naous et al., 2019; Hassandoust et al., 2021). Only when benefits from service providers exceed the cost of potential privacy threats will users opt to disclose personal (location) information (Culnan & Armstrong, 1999; Hassandoust et al., 2021). Because the concept of privacy is all about the "beliefs" (rather than the actual safety of information; see Section 1) (Wacks, 2015), service providers can manipulate user perceptions to increase their intention to share. Several ethical concerns have been exposed through researchers studying human-computer interaction. For example, Kummer et al. (2018) suggest the followings for Check-in Services practitioners:

1. integrating features and redesigning user interface;
2. implementing visibility settings and offering incentives to publicly shared contents;
3. recommending locations with "a high hedonic nature (e.g., tourist attractions)" to new users;
4. creating personalized privacy settings (e.g., less restrictive default settings for extroverts and males);
5. reducing the appearance of frequently visited locations.

The above deceptive strategies may have already been implemented because of the Key Performance Indicators (KPIs) in software development, such as install penetration, active users, and data accumulation. We suggest that LBS developers focus on creating a safer data-exchange environment (e.g., enhancing securities and limiting third-party data transfer) to

dismiss most users' privacy concerns rather than choosing an easy path that only attracts a group of people.

3.4 Cultural Differences of Geoprivacy

People from different cultural backgrounds have differing opinions and experiences with LBS. Depending on heavy users' familiarities with LBS, some view LBS as a tool for a specific set of needs, while others see LBS as recreational services without many concerns (Rzeszewski & Luczys, 2018). The distinction is that, in the eyes of the first group, LBS has the power to change the real world. However, the second group believes LBS (and its augmented reality feature) has already integrated with actual space/place (Rzeszewski & Luczys, 2018). When discussing geoprivacy concerns, culture cannot be ignored because of its effects on our decisions (Kummer et al., 2012, 2017). This section first discusses the cultural and demographic variables that influence individuals' location disclosure choices and then presents the range of privacy protection laws worldwide.

3.4.1 Cultural Impact on Privacy Perceptions

One's culture profoundly impacts on one's ideas through concepts such as ideologies, beliefs, rudimentary assumptions, core values, and "collective will" (Miltgen & Peyrat-Guillard, 2014). One definition states that a national culture is the "collective programming of the mind which distinguishes the members of one group or category of people from another" (Hofstede et al., 2010, p. 6). Hofstede (1984) defined five dimensions of a national culture: power distance, individualism, masculinity, uncertainty avoidance, and long-term orientation. Among the cultural dimensions, power distance and individualism are the critical determinants of privacy perceptions. Power distance denotes the degree of inequality in a superior-subordinate relationship (Hofstede, 1984), influencing people's acceptance level

of control, trust, and regulations (Miltgen & Peyrat-Guillard, 2014). Individualism, which describes a person's separate entity from the others, is dominant in western culture in contrast to collectivism, in which a self-concept includes "their social and cultural surroundings" (Bochner & Hesketh, 1994, p. 237). Although there is no true consensus (e.g., Ting-Toomey, 1991), several studies have reported a positive correlation between individualism and privacy concerns (e.g., Milberg et al., 2000; Posey et al., 2010; Bellman et al., 2004). Masculinity and uncertainty avoidance are the other two potential impact factors. When masculinity is high, a society focuses more on wealth and material success instead of emotions and connections with others (Hofstede et al., 2010). As a result, surplus values of private information are drained for economic benefits, increasing people's privacy concerns (Milberg et al., 1995, 2000). Finally, uncertainty avoidance has a negative association with privacy concerns. This hypothesis assumes that high uncertainty avoidance embraces a higher level of privacy regulations (Milberg et al., 1995, 2000). Privacy concerns, therefore, decrease with trust in the more robust legal system. Geoprivacy concerns and their relationships with the above cultural dimensions are no different in this case.

3.4.2 When East Meets West: The Hidden Social Norms Behind Location Disclosure Behaviours

The degree to which one is concerned about geoprivacy varies considerably between populations in western societies. Compared to selected European countries (e.g., Italy (Dinev et al., 2006) and Germany (Krasnova & Veltri, 2010)), Americans showed a higher level of internet privacy concerns. However, Americans were also more willing to self-disclose on social networks such as Facebook, which is another example of the privacy paradox. The misalignment between privacy attitudes and self-disclosure behaviours can be explained by a higher level of perceived benefits, trust, and control in the U.S. (Krasnova & Veltri, 2010).

The variation of privacy attitudes is also evident within Europe. Individualistic countries in the Western (e.g., France) and Northern (e.g., Poland and Estonia) Europe are more concerned with responsibility (i.e., public intervention). However, collectivist nations in Southern (e.g., Greece and Spain) and Eastern Europe place more trust in their government and regulations (Miltgen & Peyrat-Guillard, 2014). Many factors, including national histories, economic developments, and political environments, all contribute to the various levels of privacy concerns (Miltgen & Peyrat-Guillard, 2014). More profound understandings of the regional differences require additional knowledge of local affairs.

The right to privacy has gradually gained popularity in many Asian countries. Traditional eastern Asian cultures prioritize harmony (Nakada & Tamura, 2005), politeness (Kitiyadisai, 2005), and trusted human relationships (Nakada & Tamura, 2005) as their core values, which suggests that "privacy" is a foreign concept that requires time to be accepted (Lü, 2005). Depending on the level of intimacy, East Asians' attitudes towards privacy change in the opposite directions. In general, eastern Asians are more reluctant to disclose sensitive personal information with strangers compared to westerners (G.-M. Chen, 1995; Asai & Barnlund, 1998). Different coping mechanisms related to private information may be related to the definition of "shame" in different cultures (Capurro, 2005). The face-saving tradition in Asia prevents people from freely disclosing their private lives (Kitiyadisai, 2005). Other situational factors such as collectivism (e.g., "being selfless" (Lü, 2005)), tightly centralized regulators, and crowded living space foster the notion of "group privacy", which private matters can be communal (e.g., within a family or a company) instead of personal (Capurro, 2005; Lü, 2005). Although Asian scholars and media have discussed privacy protection, the arguments of privacy protection focused on instrumental benefits rather than an intrinsic human right and a foundational component of democracy (Lü, 2005; Nakada & Tamura, 2005). Political ideologies (e.g., Marxist), religions (e.g., Buddhism), and the collectivist culture have profound influences on the formation of privacy perceptions in East Asia.

Lin et al. (2013) identified some interesting differences in location privacy preferences between university students in the United States and China. In terms of sensitivity of places, U.S. students worried less about sharing their work locations than their homes, while Chinese students viewed the two types of places equally private. When it comes to the time of the day, both groups demonstrated less interest in sharing at night on weekdays (from 6 pm to 8 am), but the fluctuation of sharing interests was more evident among Chinese students. The sudden changes in Chinese students' behaviours continued on weekends, with spikes observed during lunch, dinner, and party times, unseen in their American counterparts. When given the option to fine-tune the granularity of shared locations (e.g., province vs. address level), American students were more conservative about the precision of locations. However, they were more open to sharing when the option was unavailable. Finally, both groups demonstrated significant variations of location sharing intents depending on who were the recipients (e.g., friends or advertisers). The findings indicate the impacts of cultural differences on location sharing preferences in the two countries.

3.4.3 Demographic Factors

Although social norms (Venkatesh et al., 2012) have an impact on people's privacy attitudes, subjective norms (Chang & Chen, 2014) also play an important role in influencing individuals' privacy concerns. Demographic factors such as age, gender, and internet experience differentiate subjective norms. Cho et al. (2009) concluded that privacy concerns are more serious among senior, female internet users from an individualistic country. Specifically, the gender difference was observed by Tifferet (2019). Lin et al. (2013) also concluded that Chinese females were more hesitant than males to share their locations, although the level of concerns decreased when the recipients became friends. The influence of age is debatable, in any case. While some surveys found that younger generations are more reckless to exchange

privacy for free services (e.g., Canares, 2018), others found the opposite (e.g., Madden et al., 2013) or no difference (e.g., Hoofnagle et al., 2010). It is worth noting that age itself is not a deciding factor, but what age brings are: adolescents may have fewer privacy concerns because of the privacy awareness gap (Hoofnagle et al., 2010), while older adults may not know how to maneuver through the complicated privacy settings (Caverlee & Webb, 2008). If young and old generations have the same level of privacy knowledge and technical skills, a significant difference may not be present. Additional age-dependent background such as levels of education (M. Zhang et al., 2020) and internet experience (Hong et al., 2021) also have associations with privacy concerns because experienced users are more knowledgeable about potential privacy issues. The individual (e.g., age and gender) and the situational factors (e.g., culture) together shape people's subjective and social norms, which in turn reflect individuals' privacy attitudes and behaviours (e.g., avoidance, opt-out, and proactive protection) (Cho et al., 2009).

3.4.4 Legal Variances

How strict a country's privacy regulations are positively correlated with the level of privacy concerns among its citizens (Milberg et al., 1995, 2000), which is influenced by cultural values and regulatory regime (Bellman et al., 2004). The European Union takes an omnibus approach (Bellman et al., 2004) and can be argued to have the tightest privacy protection law in the world. The implementation of the General Data Protection Regulation (GDPR) requires geosocial networks (GeoSNs) to be transparent about their data collection and processing services and be responsible for getting user consent on data sharing (Alrayes et al., 2020). However, the law may not be enough to protect users' location privacy. Instead, the updated privacy policy acts as an umbrella from service providers to shield them from legal liability while users remain uncertain about the background processing of their data (Alrayes

et al., 2020). This situation can be reflected with Capurro (2005)'s "privacy displacement", in which he believed being transparent alone is not enough to protect privacy. For example, Facebook's privacy policy states that "Location-related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend)."[15] In this case, even if we turn off precise location sharing, Facebook can still estimate our locations based on IP addresses and our interactions with the GeoSN. Even with a Virtual Private Network (VPN, which allows data transmission on another network) or Tor (an anonymous communication software), location information can still be indicative in a non-georeferenced text (B. Adams & Janowicz, 2012).

Countries like the United States, Canada, and Australia have sectoral regulations on information privacy, mainly focusing on the public sector (Bellman et al., 2004). The legislative actions in the United States have several unique characteristics. First, the concept of privacy has ambiguous explanations in the constitution (Margulis, 1977, 2003). The consideration of "a reasonable expectation of privacy" (L. T. Lee, 2007, p. 507) triggers eternal debates in courts but also guarantees the definition of privacy keeps up with the times (Wu et al., 2011). Second, the U.S. adopts a self-regulatory model because it trusts in the freedom and honour system (Wu et al., 2011). This voluntary approach contrasts with the omnibus approach in Europe, where the European regulations cover both public and private sectors (Bellman et al., 2004). Third, the lack of uniform federal legislation causes regional differences in privacy protection in the U.S (Wu et al., 2011). For instance, California, with its California Consumer Privacy Act (CCPA), has become a leader of personal data protection. At the same time, other states take different approaches, often falling behind in the competition to help prepare local companies to adapt to future-proof privacy requirements.

Other countries, such as China, have minimal legislation when it comes to information

[15] `https://www.facebook.com/policy.php`

privacy. In China, public security takes precedence over personal privacy; only scattered legal clauses mention "privacy" (Wu et al., 2011). The judiciary is also part of the government in China while independent in the U.S. (Wu et al., 2011). However, if the centralized regime opts to enhance privacy protection, the enforcement would have better efficiency than its western counterparts (Wu et al., 2011). The recently implemented "Personal Information Protection Law" (Bracy, 2021) has informed consent as its core principle and regulates the collection, storage, usage, and sharing of personal information in China (Creemers et al., 2020). The integrity of information privacy laws, especially those targeting the private sector, will thus improve in China in the coming years.

3.5 Economic Implications of Spatial Data

The previous sections provide an overview of some of the technological and cultural reasons behind one's geoprivacy concerns. This section begins with a theoretical background of surveillance capitalism, then discusses the empirical studies of quantitative privacy valuation and participatory sensing incentives.

3.5.1 Surveillance Capitalism

Location data can be viewed as a commodity traded in exchange for services (Prudham, 2009; McKenzie et al., 2016). Schneier (2015) called this kind of surveillance "a business model". Indeed, the "privacy information markets" (Crampton, 2015; Thatcher, 2017; Keßler & McKenzie, 2018) are prosperous. Although alternative providers are available, large internet service companies such as Google and Facebook are verging on monopolies due to their breadth, existing data silos, and quality of service. Smaller, independent services are more limited in their service coverage and typically have access to a lesser amount of data to improve their products (e.g., for training machine learning models). As a result, large internet

organizations can obtain "surplus value" from compromising user privacy (Crampton, 2015), echoing Harvey (2005) "accumulation by dispossession" (which describes the expansion of capitalism through political power instead of economic rules in the late 20^{th} century). Years ago, our homes could be viewed as a "factory" when we watched television advertisements because the action of watching TV generated value for advertisers (Jhally & Livant, 1986). Today, we are actively "working" for these advertisers by playing games and socializing on our mobile devices. While users believe that geosocial check-in services, for example, are free to use, users' personal data are collected by service providers, which can be turned into revenues (in the "privacy information markets", for example, where location data can be purchased for research or marketing purposes) (Kummer et al., 2018). Everyone is a "data broker" of his or her own and does not always have the technical knowledge, time, or interests to make a critical decision about whether accepting the terms of use for an application generates greater benefits than risks (Rzeszewski & Luczys, 2018). Compared to the agricultural society, the current world is moving from "land grab" to "data grab" (Fraser, 2019). Although it is debatable that technology users are labourers "in an exploitive economic system" (Crampton, 2015, p. 521), citizens feel anxious about dataveillance and being controlled (Crawford, 2014; Leszczynski, 2015; Rzeszewski & Luczys, 2018).

3.5.2 Valuation of Privacy

The value of privacy has been explored by researchers in psychology, economics, and management. Keßler & McKenzie (2018) hypothesized that the valuation of location information depends on the level of detail (i.e., the precision of places) and use case. Locations are also often collected as auxiliary information, making the valuation of geoprivacy a challenge in a service transaction with other primary benefits. From a psychological perspective, one important finding is that people may price their privacy differently depending on how ques-

tions are asked (Acquisti et al., 2013). Survey design options such as open- vs. closed-ended questions, rating scales, and reference periods can all lead to different responses from the same participant (Schwarz, 1999). People also tend to exaggerate their privacy concerns if surveyed directly (Acquisti & Grossklags, 2005). Empirical studies also focused on individuals' willingness to accept (WTA) and seldom compared results of WTA with individuals' willingness to pay (WTP) (Acquisti et al., 2013). Grossklags & Acquisti (2007) found that the average WTA was much greater than the average WTP, meaning that while people generally have less interest in paying in exchange for their privacy, they may still value their privacy and would only sell personal information at a reasonable price. The inequivalence of WTA and WTP signifies another psychological phenomenon that needs to be addressed in the valuation of privacy, namely incentives.

The incentives to encourage participation are not always monetary, and researchers have studied different incentive mechanisms. According to Dalkir (2017), incentives can be classified into four classes, namely remunerative (e.g., material reward), moral ("the right thing to do"), natural (e.g., self-interests), and coercive (i.e., punishment). The reputation-based incentive was recommended by Y. Zhang & Van der Schaar (2012) for crowdsourcing applications. To determine the amount of (monetary) incentives, game-theoretical, or more specifically, auction-theory-based methods were popular choices (e.g., Cvrcek et al., 2006; Danezis et al., 2005). J.-S. Lee & Hoh (2010) also proposed a reverse-auction-based dynamic price (RADP) incentive mechanism because compared to random-selection-based fixed price (RSFP), RADP reduces incentive cost through auctions and attracts an adequate number of participants. In terms of non-auction-theory-based mechanisms, fixed micro-payment is still the most effective method of maintaining participation rate, followed by lottery-style payout and variable micro-payment (Khoi et al., 2018). For future research, attention should be placed on helping participants making sensible decisions and controlling the quality of collected information (Restuccia et al., 2016). Specific incentive mechanisms for location-

sensing also need to be developed because of the unique and complex nature of geoprivacy.

3.6 Conclusions and Recommendations

The study of geoprivacy requires more than technological research (e.g., algorithmic obfuscation) due to its state as a "tension field" involving numerous themes (e.g., ethical, economic, legal, psychological, and cultural studies) (Keßler & McKenzie, 2018). This article favours the cognitive-based conceptualization of geoprivacy and shows its various dimensions from underlying situation, cultural differences, to economic implications. It is necessary to re-humanize geoprivacy as it is a concept that involves flesh and blood instead of numbers alone. Protecting geoprivacy is therefore more than uniformly masking locations to a certain degree without considering perceived risks from multiple facets. Thinking from the platial perspective, we can discover shared implicit attitudes and move the discipline from analyzing individual concerns towards protecting group privacy. Geography, as an synthetic and integrative subject (Hartshorne, 1939), offers a solid foundation for researchers to study human perception of privacy in a worldly sense.

To better understand the changing perceptions of geoprivacy, we propose a number of future research directions:

- **Designing personalized questions**: Due to the subjective nature, questionnaires on geoprivacy perceptions need to have survey questions attached to personal connections (Alrayes et al., 2020). For instance, presentations of "Hospital A" and "Toronto General Hospital" may lead to dissimilar decisions of location disclosure for Torontonians. The catch is that personal information needs to be collected before displaying actual questions.

- **Revisiting cultural impacts**: Culture, as we demonstrated in Section 4, is a signifi-

cant influencer on geoprivacy perceptions (Kummer et al., 2018) and is interrelated with a nation's legal system: as cultural values shape a country's privacy regulations, the regulations in turn influence individuals' privacy concerns (Bellman et al., 2004). Along with economic levels and political environments, different cultures foster spatial variations of privacy requirements.

- **A more-than-linear privacy model**: It is important to recognize that a privacy model can be more complicated than a linear one (Alrayes et al., 2020). For example, incentives or previous negative experiences are both impactful on individuals' geoprivacy perceptions. Even so, optimism or pessimism may not last (i.e., there is no guarantee of the longevity of these impacts) (Kummer et al., 2018), just like people's "progressive sense of place" (Massey, 2012). Thus, continuous LBS, which collects real-time location data, needs to be further scrutinized (Keith et al., 2013; Pee, 2011) and take the dynamics of privacy concerns into consideration.

- **Education, education, education**: The privacy awareness gap has resulted in countless privacy information loss in the digital age. In general, the more knowledgeable people are about location-based technologies, the better decisions users can make when they share location data. Sometimes, we overestimate the risks because of mistrust in governments or techno-giants; more often, we underestimate the perils from skipping service agreements. Hence, understanding the capabilities of context-aware technologies is the first step towards making responsible decisions regarding location data sharing.

The ultimate goal of geoprivacy protection is to develop a privacy-aware system (Alrayes et al., 2020). Researchers in this area aim to take all of the important factors of privacy into account, including transparency, controllability, user feedback, informed consent, data sensitivity, information receiver, and purpose of use (A. Adams & Sasse, 1999; Friedman et al., 2005; Langheinrich, 2001). Before that happens, informing and offering users choices in

privacy settings is possibly the most effective approach as having control provides a sense of security. Depending on user sensitivity, service providers can ask users directly (Watson et al., 2015) or learn from user behaviour automatically (Bilogrevic et al., 2016), but must resist from making decisions on users' behalf secretly. Alternatively, users can be more proactive in keeping their geoprivacy. With stricter information privacy laws being proposed worldwide, privacy as a service (e.g., VPN) will become ubiquitous in the future and act as a guard of people's geoprivacy.

3.7 References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274.

Adams, A., & Sasse, M. A. (1999). Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie? In *Interact* (pp. 214–221).

Adams, B., & Janowicz, K. (2012). On the geo-indicativeness of non-georeferenced text. In *Proceedings of the international AAAI conference on web and social media* (Vol. 6).

Agnew, J. A. (2014). *Place and politics: The geographical mediation of state and society*. Routledge.

Alrayes, F., & Abdelmoty, A. (2014). No place to hide: A study of privacy concerns due to location sharing on geo-social networks. *International Journal on Advances in Security*, *7*(3/4), 62–75.

Alrayes, F., Abdelmoty, A., El-Geresy, W., & Theodorakopoulos, G. (2020). Modelling perceived risks to personal privacy from location disclosure on online social networks. *International Journal of Geographical Information Science*, *34*(1), 150–176.

Amini, S., Lindqvist, J., Hong, J., Lin, J., Toch, E., & Sadeh, N. (2011). Caché: caching location-enhanced content to improve user privacy. In *Proceedings of the 9th international conference on mobile systems, applications, and services* (pp. 197–210).

Anderson, B. (2008). For space (2005): Doreen massey. *Key texts in human geography*, 227–235.

Asai, A., & Barnlund, D. C. (1998). Boundaries of the unconscious, private, and public self in Japanese and Americans: A cross-cultural comparison. *International Journal of Intercultural Relations*, *22*(4), 431–452.

Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. In *Proceedings of the international conference on information systems (ICIS 2008)*.

Bellatti, J., Brunner, A., Lewis, J., Annadata, P., Eltarjaman, W., Dewri, R., & Thurimella, R. (2017). Driving habits data: Location privacy implications and solutions. *IEEE Security & Privacy*, *15*(1), 12–20.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, *2*(1), 46–55.

Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., Gazaki, M., & Hubaux, J.-P. (2016). A machine-learning based approach to privacy-aware information-sharing in mobile social networks. *Pervasive and Mobile Computing*, *25*, 125–142.

Bochner, S., & Hesketh, B. (1994). Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. *Journal of Cross-Cultural Psychology*, *25*(2), 233–257.

Bowyer, K. W. (2004). Face recognition technology: Security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. *Pew Internet & American Life Project*, *4*, 1–19.

Bracy, J. (2021). *China adopts national privacy law.* IAPP. Retrieved from `https://iapp.org/news/a/china-adopts-national-privacy-law/`

Canares, M. (2018). *Online privacy: will they care? Teenagers use of social media and their understanding of privacy issues in developing countries.* World Wide Web Foundation. Retrieved from `http://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf`

Capurro, R. (2005). Privacy. An intercultural perspective. *Ethics and Information Technology*, *7*(1), 37–47.

Casey, E. S. (1993). *Getting back into place: Toward a renewed understanding of the place-world*. Indiana University Press.

Castree, N. (2003). Place: connections and boundaries in an interdependent world. In N. Clifford, S. Holloway, S. Rice, & G. Valentine (Eds.), *Key concepts in geography* (pp. 165–186). Sage London.

Caverlee, J., & Webb, S. (2008). A large-scale study of myspace: observations and implications for online social networks. In *Proceedings of the international AAAI conference on web and social media* (Vol. 2, pp. 36–44).

Chang, C.-W., & Chen, G. M. (2014). College students' disclosure of location-related information on Facebook. *Computers in Human Behavior*, *35*, 33–38.

Chen, B. (2011). *Why and how apple is collecting your iphone location data.* Wired. Retrieved from `https://www.wired.com/2011/04/apple-iphone-tracking/`

Chen, G.-M. (1995). Differences in self-disclosure patterns among Americans versus Chinese: A comparative study. *Journal of Cross-Cultural Psychology*, *26*(1), 84–91.

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

Chor, B., Goldreich, O., Kushilevitz, E., & Sudan, M. (1995). Private information retrieval. In *Proceedings of IEEE 36th annual foundations of computer science* (pp. 41–50).

Chow, C.-Y., Mokbel, M. F., & Liu, X. (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica*, *15*(2), 351–380.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Clarke, R. (1994). Dataveillance by governments: The technique of computer matching. *Information Technology & People*, *7*(2), 46–85.

Clarke, R., & Wigan, M. (2011). You are where you've been: The privacy implications of location and tracking technologies. *Journal of Location Based Services*, *5*(3-4), 138–155.

Cloke, P., Crang, P., & Goodwin, M. (2013). *Introducing human geographies*. Routledge.

Coke, E. (1979). *The first part of the institutes of the laws of england. 1628*. Reprint.

Cramer, R., Damgård, I. B., et al. (2015). *Secure multiparty computation and secret sharing*. Cambridge University Press.

Crampton, J. W. (2003). Cartographic rationality and the politics of geosurveillance and security. *Cartography and Geographic Information Science*, *30*(2), 135–148.

Crampton, J. W. (2015). Collect it all: National security, big data and governance. *GeoJournal*, *80*(4), 519–531.

Crawford, K. (2014). *The anxieties of big data.* The New Inquiry. Retrieved from `https://thenewinquiry.com/the-anxieties-of-big-data/`

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, *55*(93).

Creemers, R., Shi, M., Dudley, L., & Graham, W. (2020). *China's draft 'personal information protection law' (full translation).* New America. Retrieved from `https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/` (Accessed: 2023-07-22)

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342.

Cvrcek, D., Kumpost, M., Matyas, V., & Danezis, G. (2006). A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on privacy in electronic society* (pp. 109–118).

Dalkir, K. (2017). *Knowledge management in theory and practice*. MIT Press.

Danezis, G., Lewis, S., & Anderson, R. J. (2005). How much is location privacy worth? In *Workshop on the economics of information security (WEIS)* (Vol. 5).

Davies, S. G. (1997). Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity. In P. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 143–166). MIT Press.

Dearman, D., Hawkey, K., & Inkpen, K. M. (2005). Rendezvousing with location-aware devices: Enhancing social coordination. *Interacting with Computers*, *17*(5), 542–566.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management*, *14*(4), 57–93.

Dobson, J. E., & Fisher, P. F. (2003). Geoslavery. *IEEE Technology and Society Magazine*, *22*(1), 47–52.

Dobson, J. E., & Fisher, P. F. (2007). The panopticon's changing geography. *Geographical Review*, *97*(3), 307–323.

Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. In R. Billen, E. Joao, & D. Forrest (Eds.), *Dynamic & mobile GIS: Investigating change in space and time* (pp. 35–52). CRC Press.

Dwork, C. (2011). Differential privacy. *Encyclopedia of Cryptography and Security*, 338–340.

El Emam, K., Buckeridge, D., Tamblyn, R., Neisa, A., Jonker, E., & Verma, A. (2011). The re-identification risk of Canadians from longitudinal demographics. *BMC Medical Informatics and Decision Making*, *11*(1), 1–12.

Elwood, S., & Leszczynski, A. (2011). Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum*, *42*(1), 6–15.

Evans, L. (2011). Location-based services: Transformation of the experience of space. *Journal of Location Based Services*, *5*(3-4), 242–260.

Fraser, A. (2019). Land grab/data grab: Precision agriculture and its new horizons. *The Journal of Peasant Studies*, *46*(5), 893–912.

Friedman, B., Lin, P., & Miller, J. K. (2005). Informed consent by design. *Security and Usability*, 503–530.

Gao, H., Tang, J., & Liu, H. (2012). gSCorr: Modeling geo-social correlations for new check-ins on location-based social networks. In *Proceedings of the 21st ACM international conference on information and knowledge management* (pp. 1582–1586).

Gao, S., Janowicz, K., McKenzie, G., & Li, L. (2013). Towards platial joins and buffers in place-based GIS. In *ACM SIGSPATIAL COMP'13.*

Georgiou, M. (2006). *Architectural privacy: A topological approach to relational design problems* (Unpublished doctoral dissertation). University College London.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy.* University of Chicago Press.

Goodchild, M. F. (2011). Formalizing place in geographic information systems. In L. Burton, S. Matthews, M. Leung, S. Kemp, & D. Takeuchi (Eds.), *Communities, neighborhoods, and health* (pp. 21–33). Springer.

Grossklags, J., & Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *Workshop on the economics of information security (WEIS).*

Gu, Y., Yao, Y., Liu, W., & Song, J. (2016). We know where you are: Home location identification in location-based social networks. In *2016 25th international conference on computer communication and networks (ICCCN)* (pp. 1–9).

Gupta, S., Xu, H., & Zhang, X. (2011). Balancing privacy concerns in the adoption of location-based services: an empirical analysis. *International Journal of Electronic Business*, *9*(1-2), 118–137.

Hamzei, E., Winter, S., & Tomko, M. (2020). Place facets: A systematic literature review. *Spatial Cognition & Computation*, *20*(1), 33–81.

Harrison, S., & Dourish, P. (1996). Re-place-ing space: The roles of place and space in collaborative systems. In *Proceedings of the 1996 ACM conference on computer supported cooperative work* (pp. 67–76).

Hartshorne, R. (1939). The nature of geography: A critical survey of current thought in the light of the past. *Annals of the Association of American geographers*, *29*(3), 173–412.

Harvey, D. (2005). *The new imperialism.* Oxford University Press.

Harvey, D. (2018). *The limits to capital.* Verso books.

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463–471.

Hillier, B. (2007). *Space is the machine: A configurational theory of architecture*. Space Syntax.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Sage.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. McGraw Hill.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, *168*, 539–564.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*.

Jhally, S., & Livant, B. (1986). Watching as working: The valorization of audience consciousness. *Journal of Communication*, *36*(3), 124–143.

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys*, *54*(1), 1–36.

Johnson, J. L. (1992). A theory of the nature and value of privacy. *Public Affairs Quarterly*, *6*(3), 271–288.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1–24.

Kaasinen, E. (2003). User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, *7*(1), 70–79.

Kar, B., Crowsey, R. C., & Zale, J. J. (2013). The myth of location privacy in the United States: Surveyed attitude versus current practices. *The Professional Geographer*, *65*(1), 47–64.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Keßler, C., & McKenzie, G. (2018). A geoprivacy manifesto. *Transactions in GIS*, *22*(1), 3–19.

Khoi, N. M., Casteleyn, S., Moradi, M. M., & Pebesma, E. (2018). Do monetary incentives influence users' behavior in participatory sensing? *Sensors*, *18*(5), 1426.

Khoshgozaran, A., & Shahabi, C. (2007). Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *Proceedings of the international symposium on spatial and temporal databases* (Vol. 10, pp. 239–257).

Kido, H., Yanagisawa, Y., & Satoh, T. (2005). Protection of location privacy using dummies for location-based services. In *International conference on data engineering workshops (ICDEW)* (Vol. 21, pp. 1248–1248).

Kitchin, R., & Dodge, M. (2014). *Code/space: Software and everyday life*. MIT Press.

Kitiyadisai, K. (2005). Privacy rights and protection: foreign values in modern Thai context. *Ethics and Information Technology*, *7*(1), 17–26.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences* (pp. 1–10).

Kummer, T.-F., Leimeister, J. M., & Bick, M. (2012). On the importance of national culture for the design of information systems. *Business & Information Systems Engineering*, *4*(6), 317–330.

Kummer, T.-F., Recker, J., & Bick, M. (2017). Technology-induced anxiety: Manifestations, cultural influences, and its effect on the adoption of sensor-based technology in German and Australian hospitals. *Information & Management*, *54*(1), 73–89.

Kummer, T.-F., Ryschka, S., & Bick, M. (2018). Why do we share where we are? The influence of situational factors on the conditional value of check-in services. *Decision Support Systems*, *115*, 1–12.

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on ubiquitous computing (Ubicomp)* (pp. 273–291).

Lee, J.-S., & Hoh, B. (2010). Sell your experiences: A market mechanism based incentive for participatory sensing. In *2010 IEEE international conference on pervasive computing and communications (PerCom)* (pp. 60–68).

Lee, L. T. (2007). Digital media technology and individual privacy. In C. Lin & D. Atkin (Eds.), *Communication technology and social change* (pp. 504–549). Routledge.

Leszczynski, A. (2015). Spatial big data and anxieties of control. *Environment and Planning D: Society and Space*, *33*(6), 965–984.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*, 453–496.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 501–510).

Lin, J., Benisch, M., Sadeh, N., Niu, J., Hong, J., Lu, B., & Guo, S. (2013). A comparative study of location-sharing privacy preferences in the United States and China. *Personal and Ubiquitous Computing*, *17*(4), 697–711.

Lü, Y.-H. (2005). Privacy and data privacy issues in contemporary China. *Ethics of Information Technologies*, *7*, 7–15.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). *Teens, social media, and privacy.* Pew Research Center. Retrieved from `https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/`

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261.

Massey, D. (1997). The spatial construction of youth cultures. In T. Skelton & G. Valentine (Eds.), *Cool places* (pp. 132–140). Routledge.

Massey, D. (2012). *Power-geometry and a progressive sense of place.* Routledge.

McCandless, D., Evans, T., Quick, M., Hollowood, E., Miles, C., Hampson, D., & Geere, D. (2021). *World's biggest data breaches & hacks.* Information is Beautiful. Retrieved from `https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`

McKenzie, G., & Janowicz, K. (2014). Coerced geographic information: The not-so-voluntary side of user-generated geo-content. In *Proceedings of the international conference on geographic information science* (Vol. 8).

McKenzie, G., Janowicz, K., & Seidl, D. (2016). Geo-privacy beyond coordinates. In T. Sarjakoski, M. Y. Santos, & L. T. Sarjakoski (Eds.), *Geospatial data in a changing world* (pp. 157–175). Springer.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4).

Michael, K., & Michael, M. (2011). *The social and behavioural implications of location-based services.* Taylor & Francis.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65–74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125.

Nakada, M., & Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology*, *7*(1), 27–36.

Naous, D., Kulkarni, V., Legner, C., & Garbinato, B. (2019). Information disclosure in location-based services: An extended privacy calculus model. In *Proceedings of the international conference on information systems* (Vol. 40).

Naveed, M., Ayday, E., Clayton, E. W., Fellay, J., Gunter, C. A., Hubaux, J.-P., ... Wang, X. (2015). Privacy in the genomic era. *ACM Computing Surveys*, *48*(1), 1–44.

Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2015). Enhancing privacy through caching in location-based services. In *2015 IEEE conference on computer communications (INFOCOM)* (pp. 1017–1025).

Pee, L. G. (2011). Attenuating perceived privacy risk of location-based mobile services. In *Proceedings of the European conference on information systems (ECIS)* (Vol. 19).

Pontes, T., Vasconcelos, M., Almeida, J., Kumaraguru, P., & Almeida, V. (2012). We know where you live: Privacy characterization of foursquare behavior. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 898–905).

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*(2), 181–195.

Preoţiuc-Pietro, D., & Cohn, T. (2013). Mining user behaviours: A study of check-in patterns in location based social networks. In *Proceedings of the 5th annual ACM web science conference* (pp. 306–315).

Prudham, S. (2009). Commodification. In N. Castree, D. Demeritt, D. Liverman, & B. Rhoads (Eds.), *A companion to environmental geography* (pp. 123–142). Wiley.

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, *29*(4), 1841–1848.

Purves, R. S., Winter, S., & Kuhn, W. (2019). Places in information science. *Journal of the Association for Information Science and Technology*, *70*(11), 1173–1182.

Restuccia, F., Das, S. K., & Payton, J. (2016). Incentive mechanisms for participatory sensing: Survey and research challenges. *ACM Transactions on Sensor Networks (TOSN)*, *12*(2), 1–40.

Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review*, *66*, 41.

Rose-Redwood, R. S. (2006). Governmentality, geography, and the geo-coded world. *Progress in Human Geography*, *30*(4), 469–486.

Rossi, L., & Musolesi, M. (2014). It's the way you check-in: Identifying users in location-based social networks. In *Proceedings of the second ACM conference on online social networks* (pp. 215–226).

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404.

Rzeszewski, M., & Luczys, P. (2018). Care, indifference and anxiety—attitudes toward location data in everyday life. *ISPRS International Journal of Geo-Information*, *7*(10), 383.

Sadilek, A., Kautz, H., & Bigham, J. P. (2012). Finding your friends and following them to where you are. In *Proceedings of the fifth ACM international conference on web search and data mining* (pp. 723–732).

Schneier, B. (2015). *Data and goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Schwarz, N. (1999). Self-reports: How the questions shape the answers. *American psychologist*, *54*(2), 93.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Stutzman, F. D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 2.

Sui, D., Elwood, S., & Goodchild, M. (2012). *Crowdsourcing geographic knowledge: volunteered geographic information (VGI) in theory and practice*. Springer.

Surden, H. (2007). Structural rights in privacy. *Southern Methodist University Law Review*, *60*(4), 1605–1629.

Swanlund, D., & Schuurman, N. (2019). Resisting geosurveillance: A survey of tactics and strategies for spatial privacy. *Progress in Human Geography*, *43*(4), 596–610.

Sweeney, L. (2000). Uniqueness of simple demographics in the US population. *LIDAP-WP4, 2000*.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies*. Springer.

Tear, A. (2020). Geotagging matters? The interplay of space and place in politicized online social media networks. In *Proceedings of the 2nd international symposium on platial information science* (pp. 61–72).

Tenbrink, T. (2020). The language of place: Towards an agenda for linguistic platial cognition research. In *Proceedings of the 2nd international symposium on platial information science* (pp. 5–12).

Thatcher, J. (2017). You are where you go, the commodification of daily life through 'location'. *Environment and Planning A: Economy and Space*, *49*(12), 2702–2717.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990–1006.

Thrift, N. (2004). Remembering the technological unconscious by foregrounding knowledges of position. *Environment and Planning D: Society and Space*, *22*(1), 175–190.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1–12.

Ting-Toomey, S. (1991). Intimacy expressions in three cultures: France, Japan, and the United States. *International Journal of Intercultural Relations*, *15*(1), 29–46.

Tuan, Y.-F. (1977). *Space and place: The perspective of experience*. University of Minnesota Press.

Tuan, Y.-F. (1990). *Topophilia: A study of environmental perceptions, attitudes, and values*. Columbia University Press.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157–178.

Wacks, R. (2015). *Privacy: A very short introduction*. Oxford University Press.

Wang, T., & Liu, L. (2009). From data privacy to location privacy. In P. Yu & J. Tsai (Eds.), *Machine learning in cyber trust* (pp. 217–246). Springer.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Watson, J., Lipford, H. R., & Besmer, A. (2015). Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *22*(6), 1–20.

Weiser, P., & Scheider, S. (2014). A civilized cyberspace for geoprivacy. In *Proceedings of the 1st ACM SIGSPATIAL international workshop on privacy in geographic information collection and analysis* (pp. 1–8).

Westin, A. (1967). *Privacy and freedom*. Athenum.

Wicker, S. B. (2012). The loss of location privacy in the cellular age. *Communications of the ACM*, *55*(8), 60–68.

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the US and China. *Telecommunications Policy*, *35*(7), 603–616.

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*(1), 42–52.

Zhang, H., & Malczewski, J. (2019). Quality evaluation of volunteered geographic information: The case of OpenStreetMap. In M. Khosrow-Pour (Ed.), *Crowdsourcing: Concepts, methodologies, tools, and applications* (pp. 1173–1201). IGI Global.

Zhang, M., Zhao, P., & Qiao, S. (2020). Smartness-induced transport inequality: Privacy concern, lacking knowledge of smartphone use and unequal access to transport information. *Transport Policy*, *99*, 175–185.

Zhang, Y., & Van der Schaar, M. (2012). Reputation-based incentive protocols in crowdsourcing applications. In *IEEE INFOCOM 2023 - IEEE conference on computer communications* (pp. 2140–2148).

Zhong, Y., Yuan, N. J., Zhong, W., Zhang, F., & Xie, X. (2015). You are where you go: Inferring demographic attributes from location check-ins. In *Proceedings of the eighth ACM international conference on web search and data mining* (pp. 295–304).

Preamble to Chapter 4

Geoprivacy has been examined from the platial perspective in Chapter 3, underscoring the importance of the human-centred approach. In this chapter, I continue exploring human perception and geoprivacy, specifically by investigating concerns related to the involuntary disclosure of geodata on Chinese social media platforms. Since April 2022, major Chinese social media platforms have begun displaying local users' provincial locations based on their internet protocol (IP) addresses. A fiery debate on Weibo, a Chinese microblogging platform, offers an unprecedented opportunity to gain insights into the geoprivacy attitudes of Chinese netizens. Through a combination of natural language processing and thematic analysis, we extracted implicit topics from the collected Weibo posts and comments about IP location disclosure. The results, capturing both positive and negative sentiments, illustrate the specific landscape of geoprivacy concerns within the communitarian state. The revelations regarding public opinions on involuntary location disclosure hold the potential to broaden the understanding of geoprivacy attitudes in contemporary China.

Chapter 4

Geoprivacy Attitudes on Chinese Social Media

Abstract

In April of 2022, one of the largest Chinese social media platforms, Weibo, implemented a new feature that automatically adds a user's location to all microblog posts and comments. Released to combat disinformation, a user's location is identified based on their device's internet protocol (IP) address. Almost immediately, a heated debate over the implementation of this feature and user privacy took place on the platform. In this work, we analyze users' reactions to this implementation based on 59,051 microblogs and 113,175 comments about IP location disclosure collected from March to May 2022 on Weibo.com. Spatial and temporal patterns in the data were first identified. Deep reading was then guided by the output of a Latent Dirichlet Allocation (LDA) topic model to extract implicit topics from the discourse. Results indicate that both supporters and opponents of the involuntary location disclosure participated in the discussion, with females more involved than males. Theories of location privacy concerns were also proposed according to the related literature and the online discourse. The ambivalent attitudes of some users revealed the unique landscape of data privacy concerns in the communitarian state. The findings of this study will aid policymakers in understanding public opinions about involuntary location disclosure and help software developers implement privacy-aware designs in contemporary China.

4.1 Introduction

China owns one of the world's largest databases of human digital footprints due to its population of 1.4 billion people. Described by Kai-Fu Lee (2018) as the "Saudi Arabia of data," the country's physical and digital worlds are deeply integrated, from mobile payment systems (e.g., Alipay) to social networking platforms (e.g., WeChat). China also boasts the world's largest surveillance camera network and has expanded the use of facial recognition technology in recent years (Cosgrove, 2019). The unparalleled access and amount of citizen data have allowed the Chinese government to launch the social credit system (Aho & Duffield, 2020). While the measure is viewed as a "new digital Leninism" (Heilmann, 2016), the system is largely accepted among Chinese individuals as a means towards an "honest and harmonious society" (Kostka, 2019). In light of these facts, a discussion on surveillance and personal data control in China must consider the cultural and political context to better understand public opinions toward specific policies.

By April 2022, all major online platforms in China had implemented functionality for displaying user locations based on IP addresses. This measure was in addition to already tightened censorship measures such as real-name registration (Shen, 2022). The feature was first added by Weibo, commonly regarded as the Chinese version of X (Twitter), on March 4, 2022.[16] The stated reason was to combat disinformation about the Russia-Ukraine crisis. Initially, the function was only tested on selected users and microblogs with keywords such as Russia, Ukraine, and Kyiv. Chinese provinces/regions or overseas countries were displayed when users posted or commented on Weibo. The announcement initially received limited attention on the platform due to the small-scale implementation. A much larger-scale reaction was captured on the *hot search list* when the feature was fully implemented on Weibo and other social media platforms such as *WeChat* and *Douyin* in late April.

[16] `https://weibo.com/1934183965/Liait9YAp`

While the state media argued that no personally identifiable information is revealed by the feature with published locations at the regional level[17], some netizens still expressed concerns about users' location privacy being compromised. Mixed with voices of support to increase transparency on online platforms (Shen, 2022), it has been challenging to determine Weibo users' level of location privacy concerns by simply glancing at the related microblog posts and comments. The implementation of this feature and subsequent response offer an unprecedented opportunity to investigate how, what, and who is impacted by this feature. What are the spatial-temporal trends of Weibo users' discussion on this new feature? What major themes and opinions can be extracted from the social media posts and comments? Do Weibo users believe this is a practical approach to counter dis/misinformation? This paper investigates these questions through computer-assisted text analysis. After determining the spatial-temporal characteristics of the data, keywords were extracted using a Latent Dirichlet Allocation (LDA) model to lead the deep reading and manual coding of the Weibo discourse. This mixed-method approach is suited for this analysis as the LDA model identifies patterns and reduces the volume of the data, while manual coding increases the interpretability and accessibility of the results. To the best of our knowledge, this is the first study that analyzes public concerns over involuntary location disclosure on Chinese social media. The outcomes of this study shed light on the geoprivacy attitudes held by Chinese netizens. Integrated with the literature review and the discussion, this article suggests the underlying factors contributing to the divergent privacy attitudes exhibited by Weibo users.

[17] e.g., `https://weibo.com/2087169013/LCQJJtYEz`

4.2 Literature Review

4.2.1 Evolution of the Right to Privacy in China

Given the implementation of the IP location feature in China, comprehending the information privacy legislations and practices within the country becomes crucial. Drawing lessons from the West, China has developed its own rules on privacy. This section reflects on the ethical considerations from a cultural perspective and analyzes the recent legal advancement of privacy rights in mainland China.

China has been traditionally built on the concepts of nation and family. In this sense, individual and individual rights have been ignored since ancient China (Cao, 2005; Pye, 1991). Instead of being regulated by legislation, civil conduct was bound by morals and ethics from Confucianism and Taoism in feudal China. Privacy is, therefore, a foreign concept as a direct translation is rarely found in classical scriptures. With economic reform and globalization, modern privacy began gaining in popularity in 1979. The need for trust and a stable environment for the market economy encouraged the development of *right to privacy* in the legal sector (Yan & Wang, 1996). However, privacy was often mischaracterized as "shameful secrets" (e.g., sexual affairs and indecent behaviours) even in law dictionaries (Cao, 2005). This negative perception of privacy is still impacting modern Chinese society.

The privacy protection landscape in China has drastically changed in recent years. Latest legal analysis has focused on the Cyber Security Law (Qi et al., 2018), the Civil Code of the People's Republic of China (Cui & Qi, 2021), and the Personal Information Protection Law (PIPL) (Pernot-Leplay, 2020). Critiques of the regulations typically centre around public vs. private or state vs. individual. The absence of coverage of privacy issues in government is evident, as data privacy rights, for example, only apply to consumers based on the principle of national sovereignty in the Cyber Security Law (Pernot-Leplay, 2020). However, competing legal interests exist within capitalist systems, not only in paternalistic

societies (Westin, 2003).

4.2.2 Anonymity on Social Media: The Root of Disinformation?

Just as information privacy rights receive additional legal protection, fake news has also caught the attention of the state due to its extraordinary speed of dissemination. Lazer et al. (2018) defined *fake news* as "fabricated information that mimics news media content in form but not in organizational process or intent". As a result, "the accuracy and credibility of information" is in question. Egelhofer & Lecheler (2019) used a flow chart to demonstrate the relationship between fake news and other concepts (p. 103). Strictly speaking, *misinforation* is unintentional, and *disinformation* is deliberate. Only journalistically-formatted disinformation is referred to as *fake news*. We use the term "disinformation" to refer to the microblogs targeted by the IP location feature, as most of them are individual posts written in layman's style.

One question posed by regulators is whether or not anonymity on social media leads to the proliferation of disinformation. Opposing behaviours have been observed in different interaction scenarios. For instance, in an experiment involving American undergraduate students, K. Zhang & Kizilcec (2014) discovered that most participants preferred anonymous information sharing, especially for controversial content. By comparison, Jaidka et al. (2022) found no support for the assumption that anonymity reduces civility or discussion quality in a simulated online discussion about gun rights. Even if anonymity has a substantial impact, it is essential to note that people use social media for entertainment, relaxation, and expression of opinion (Whiting & Williams, 2013), and being identifiable in the virtual environment might take the enjoyment away as privacy concerns arise. The recommended use of avatars and usernames indicates that social media platforms want their users to enjoy the availability of pseudonyms. Thus, transparency is a double-edged sword: real identities

may limit the spread of disinformation, but privacy concerns may turn users away from continued usage (Zhou & Li, 2014).

Thus, what are common approaches to countering disinformation? According to Alemanno (2018), state intervention is the first solution. Organizations such as the *Global Engagement Centre* in the United States and the *Disinformation Review Office* in the European Union fall into this category. Online portals have also been set up in countries such as Canada and China for correcting dis/misinformation (Helm & Nasu, 2021). The issue is that the criteria for determining disinformation can be vague and subjective by the so-called "Ministries of Truth" (Alemanno, 2018). Another regulatory solution is to impose criminal sanctions to deter the "initial creation and sharing" of disinformation (Helm & Nasu, 2021). The challenges are that not every user is afraid of criminal sanctions, and policing this cybercrime is technically difficult (Europol & Eurojust, 2018).

Public authorities could also intervene indirectly through intermediary liability (Kaye, 2018) and require social media platforms to police user-generated content (e.g., the German Network Enforcement Act) (Alemanno, 2018). The problem is that the label of disinformation or the action of content removal may attract additional public attention (also known as the Streisand effect (Jansen & Martin, 2015)). The potential impact on freedom of expression is also a concern. A counter-intuitive approach is to swamp disinformation with the truth (e.g., the related articles feature on Facebook). Whether "exposure to alternative viewpoints" contributes to dissipating misperceptions remains to be proved, and social media platforms have few incentives to act as guardians of truth due to their reliance on advertising revenue (Alemanno, 2018).

4.2.3 Social Media, the Spatial Self, and Private Locales

Although disinformation exists, social media platforms are still popular. One explanation could be that individuals employ social media platforms as tools for online self-expression. Within this process, the concept of the "spatial self" comes to the fore, as users document, archive, and showcase their spatial experiences to construct their identities for others (Schwartz & Halegoua, 2015). This presentation transcends individual messages or images; it constitutes a cohesive narrative comprised of geocoded digital traces and mobility patterns mapped out (Schwartz & Halegoua, 2015). As a collective representation, private locations within these narratives are at risk of unintended exposure to the public domain.

The IP location feature heightens the risk of uncovering users' private spatial selves. As Humphreys (2012) pointed out, individuals' decisions regarding location disclosure are influenced by a spectrum of motivations and contexts, ranging from showcasing achievements, self-promotion, crafting inside jokes, memorizing life events, to earning points or rewards. These personal narratives are carefully curated, with specific locations excluded while others are accentuated (Mendelson & Papacharissi, 2010). This desire for "...more controlled and more imaginative performances of identity online..." reflects the calculated yet imprecise portrayal of life experiences that support intimate social connections (Papacharissi, 2011). Users are therefore interested in maintaining control over their spatial selves, safeguarding the curated projection of their online identities. Specific locales bear a sense of privacy and should not become public. With the introduction of the IP location feature, users' provincial locations have become readily available in microblog metadata, bypassing the need for location data mining and validation through sources such as user profiles, microblog contents, or relationships among microblogs (Stock, 2018). These trajectories of provincial locations can render private locales more vulnerable in the absence of appropriate countermeasures. As users progressively grow reliant on social media platforms to cultivate their digital presence

(Schwartz & Halegoua, 2015), the IP location feature has the potential to alter individuals' spatial practices and reduce sociability on online platforms.

4.2.4 Digital Surveillance Measures in China

While IP location and its comprehensive implementation are unprecedented, China has a history of developing innovative tools that go beyond the control of disinformation. The social credit system (SCS), a widely-discussed digital surveillance and control platform, is often regarded as a modern reflection of "Confucian bureaucracy" (Aho & Duffield, 2020). Indeed, having gentility is one of the Confucian doctrines. The SCS follows the same logic and aims to promote "self-discipline" of individuals and enterprises to simplify regulations and cut social costs (State Council, 2014, 2017). The "creative and novel enforcement mechanism" (Aho & Duffield, 2020) improves the efficiency of state institutions and reduces the need for institutional personnel (Kostka, 2019). However, the dystopian approach can also be challenged for algorithmic accuracy, equal access, and data privacy. Aho & Duffield (2020) argued that the SCS functions as a "coerced self-regulation" system of behavioural control. The psychological manipulation mirrors the idea of panopticon, in which the perception of ubiquitous surveillance changes people's behaviours without the need to use force (Bentham, 1791). The difference is that the SCS offers both rewards and punishments through the measures of "trustworthiness." The balance of carrots and sticks is one of the reasons for the system's high levels of approval in the country (Kostka, 2019).

Domestic censorship is another method of control which suppresses public communication. The database of prohibited keywords is only expanding as new slang is invented to discuss sensitive topics on the internet. Standard filtering practices in China include cyber-attacks, network controls, domain-name controls, localized disconnection, surveillance, and astroturfing (MacKinnon, 2011). Bamman et al. (2012) discovered that "search prohibition"

is more widely used than content deletion on Chinese social media. Geographic bias was also observed as inland provinces on the west (e.g., Tibet and Qinghai) experienced higher rates of deletion compared to coastal provinces on the east. The government also relies on domestic companies to self-censor third-party speeches, which results in a "fragmented and decentralized" censorship network (Bamman et al., 2012).

Despite the surveillance measures mentioned above and the ubiquity of closed-circuit television cameras, political trust in governmental institutions remains high in China (Wang & You, 2016)[18]. The guardianship model of governance, the paternalistic style of leadership, and the communitarian culture of shared value all shape the reliant attitudes towards the central government (Liu & Zhao, 2021). Critiques of constant digital surveillance have become background noise that is often ignored.

4.2.5 Computer-Assisted Text Analysis

Social media provides a unique source of information for investigating public sentiments towards digital surveillance and trust. Dong & Lian (2021) reviewed social-media-based public opinion analyses and identified the prevalent use of machine learning algorithms in related works. Among those, unsupervised machine learning (UML) algorithms were found to be effective in exploring new patterns of textual data (Nelson et al., 2021). Multiple studies have successfully implemented UML algorithms with Weibo data (e.g., An et al. (2018); Chen et al. (2022); Han et al. (2020); Li et al. (2021)). The majority of the related literature used an LDA approach to cluster and explore public opinions (e.g., Chen et al. (2022); Li et al. (2021); Pu et al. (2022); Xie et al. (2021)). As a generative Bayesian probabilistic model (Blei et al., 2003), LDA can discover implicit topics from text sets.

Computational methods are also being combined with grounded theory (Nelson, 2020). In

[18]With the influx of liberal values from globalization, researchers have found that the level of political trust has dwindled in recent years, but the majority still support the central regime (Wang & You, 2016; Wang & Yu, 2015).

contrast to deductive research, where data is collected for hypothesis testing, grounded theory is "an inductive process whereby theoretical insights are generated from data" (Chapman et al., 2015, p. 201). Thematic analysis is a frequently used analytical tool associated with grounded theory (e.g., Anstead & O'Loughlin (2015); Ekenga et al. (2018); Mollema et al. (2015)). Guest et al. (2011) listed four steps in performing thematic analysis: getting familiar with transcripts, identifying potential themes, analyzing structures of themes, and constructing theoretical models with new data. Together, computational grounded theory connects qualitative reasoning with quantitative tools, enabling big data research in social science.

4.3 Data

To analyze public opinions, we accessed a total of 59,051 microblogs and 113,175 comments related to IP location from March 4 through May 8, 2022, using modified Python scripts[19] through the search function and cookies on Weibo.com. Keywords such as *IP location*, *IP proxy*, and *real geographic location* were used to filter the related content. Attributes such as publication time, username, posted content, self-disclosed location[20], IP location, gender, and birthday were collected.

Basic spatial-temporal analysis was conducted to understand whether the sample was representative, whether gender bias existed, and how the discussion evolved over space and time. Figure 4.1 shows the spatial distribution of public participation in China. An east-west divide by the Heihe-Tengchong line can be observed, with more participation along the east coast and Guangdong province at the top of the list. Taking population[21] into account, a moderately strong R^2 value (0.591) shows that areas with higher economic development

[19]See the original scripts at `https://github.com/Python3Spiders/WeiboSuperSpider`

[20]Some users choose to report geographic origins on their profile pages.

[21]Population data from National Bureau of Statistics (China), National Statistics (Taiwan), Census and Statistics Department (Hong Kong), and Statistics and Census Service (Macau).

levels (e.g., Beijing and Shanghai) also had more discussion per capita than under-developed regions such as Guizhou and Guangxi (Figure 4.2).

We next examined whether those identifying as male or female participated in the discussion equally in our sample dataset. According to Weibo Data Centre (2020), Weibo had 9.2% more female users than male users in 2020. However, the statistic does not tell the story of active users. Referencing the work of Yuan et al. (2018), we computed the normalized M:F ratio $(M:F)_N$ by dividing the male-to-female ratios of our sample Weibo data $(M:F)_W$ by the ratios of the 2020 census $(M:F)_C$. The average $(M:F)_N$ was 0.623, indicating that women were more active in expressing their opinions on this topic. This trend was consistent across Chinese regions except for Hong Kong and Taiwan, where the $(M:F)_N$ of the former was 1.311 and the latter was 0.981. Figure 4.3 demonstrates the gender difference cartographically. The result was similar to Yuan et al. (2018), which discovered that female users were more likely to share their locations on Weibo. It is therefore not a surprise that women were more engaged in this discussion as females also disclose their locations on the platform more frequently (Yuan et al., 2018).

In terms of the temporal trend, Figure 4.4 displays the count of collected Weibo posts and comments over time. Five peaks can be observed from the graph, namely the initial announcement (March 4), the feature update (March 23), the planned feature expansion to multiple platforms (April 15), the feature release across Chinese social media (April 28), and the popularity of IP proxy services reported by the media (May 6).

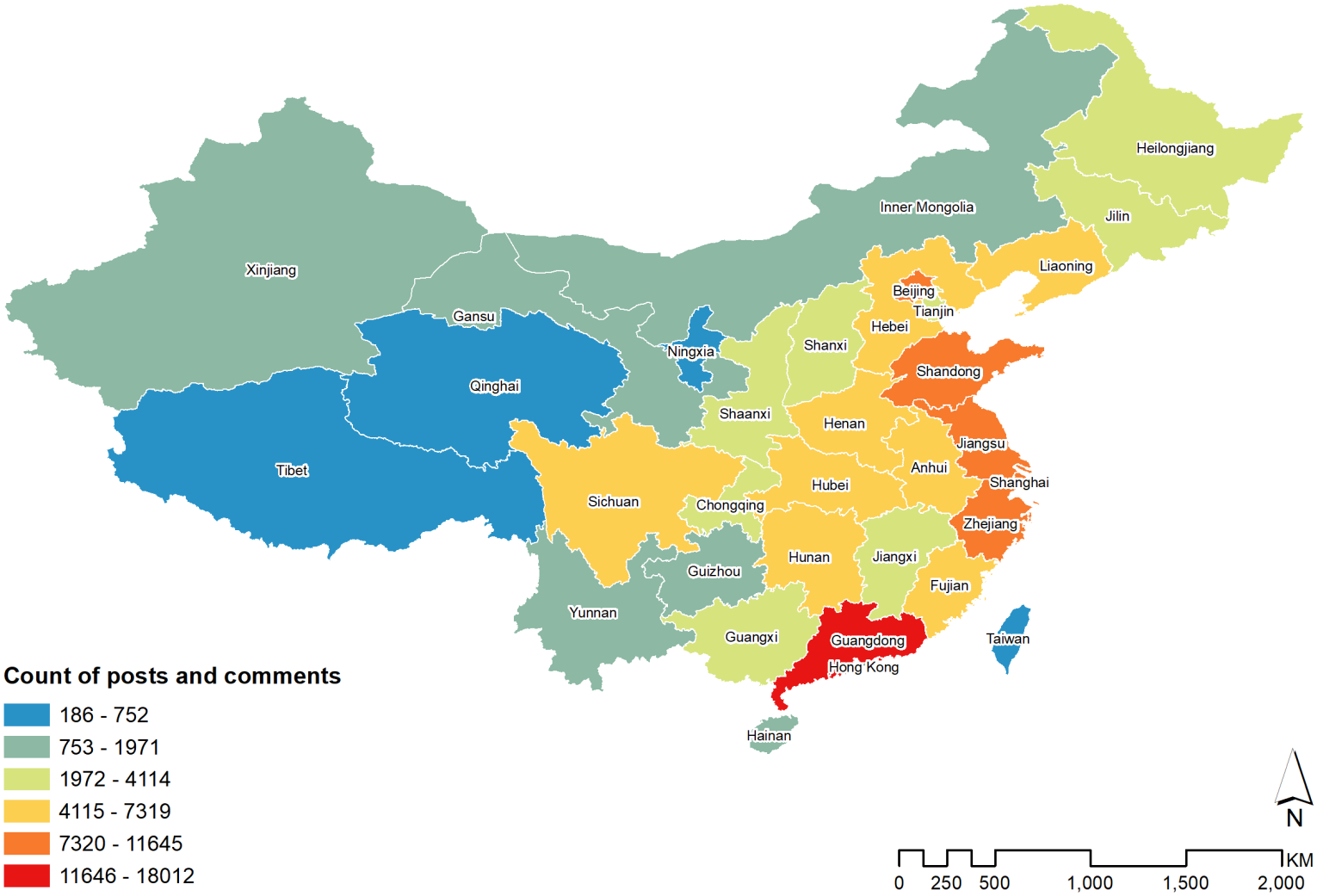

Figure 4.1: Spatial Distribution of Weibo Posts and Comments in the Study Area[22]

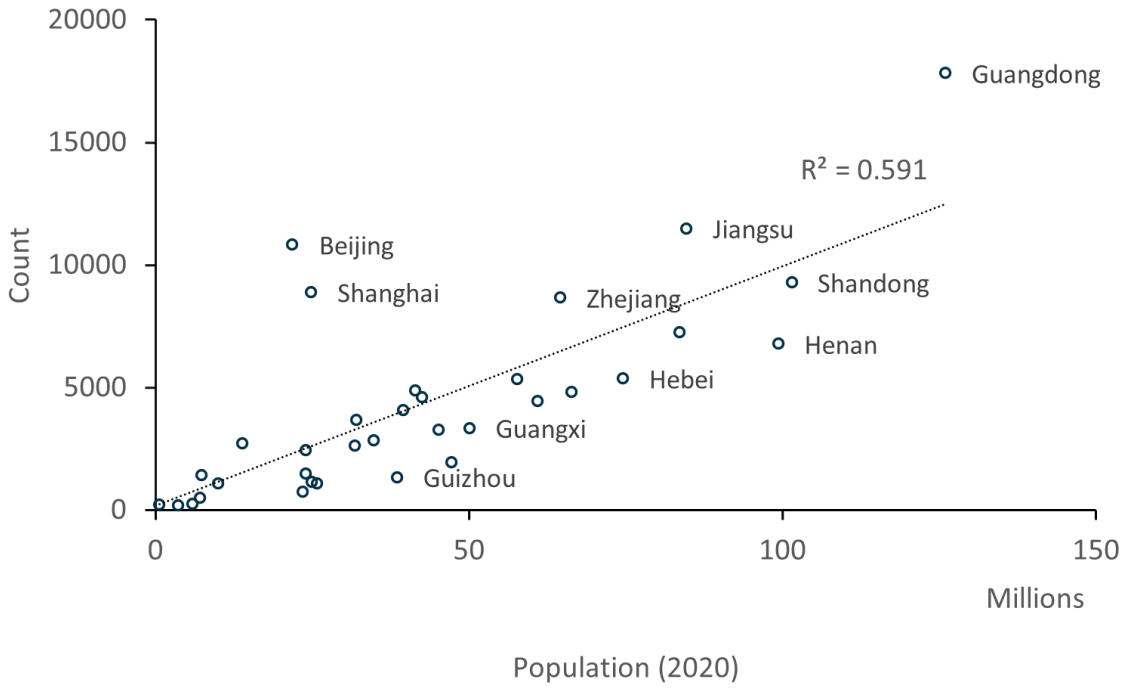

Figure 4.2: Correlation Between Population and Sum of Weibo Posts and Comments

[22]The maps presented in this article serve solely to illustrate the study area. This and the following maps do not depict geopolitical boundaries that are controversial or under dispute.

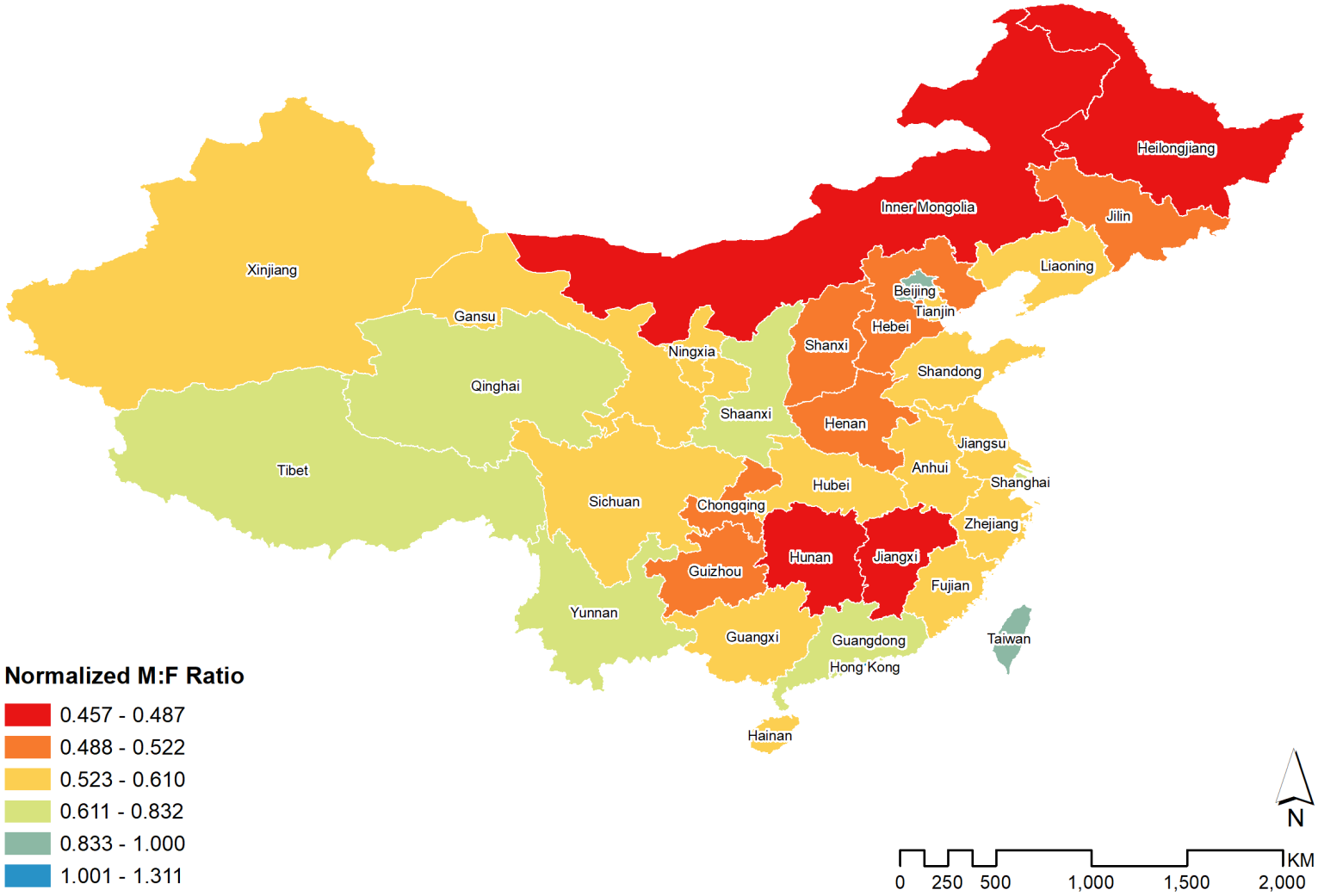

Figure 4.3: Normalized M:F Ratio in the Study Area

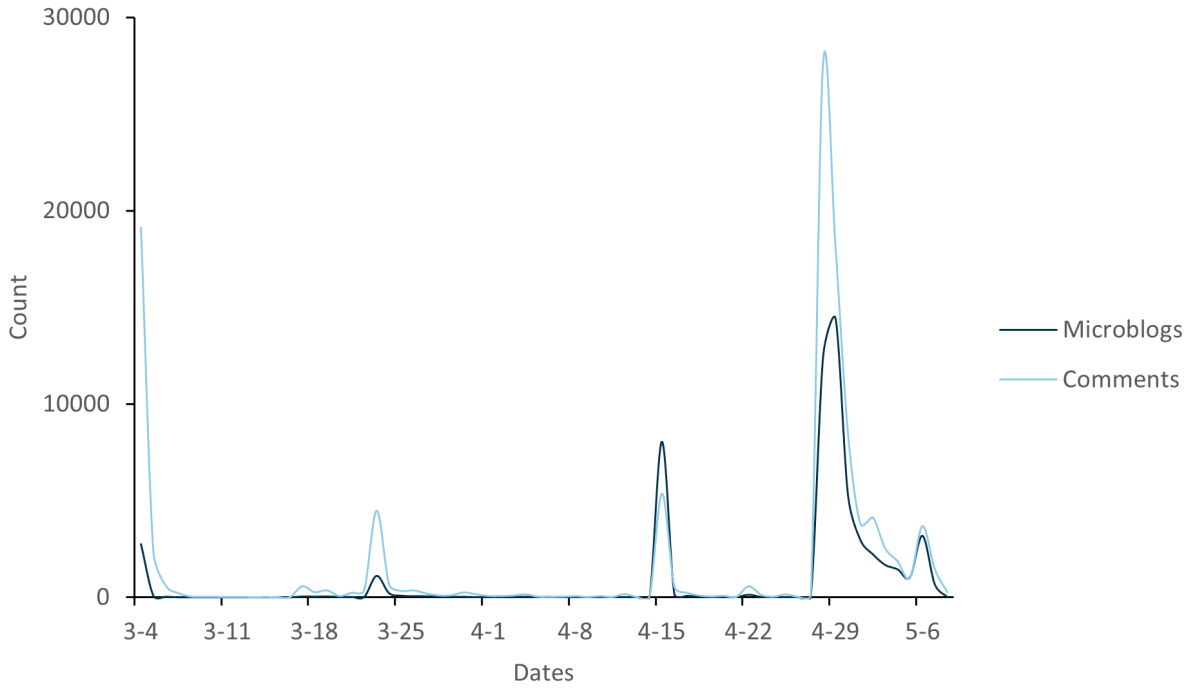

Figure 4.4: Number of Related Weibo Posts and Comments Over Time With Spikes Observed on March 4, 23, April 15, 28, and May 6

4.4 Analysis

Computer-assisted text analysis was administered to analyze public opinions. Specifically, LDA was adopted in the initial probe and clustering, and grounded theory using thematic analysis was used for synthesis and interpretation. LDA is particularly well-suited for this analysis because it can identify implicit topics from textual data. Additionally, LDA's unsupervised nature allows for the model to be used in this study where similar discourses on the same topic are unavailable as training data. The model examines the co-occurrence of words to extract thematic clusters. These clusters of terms contributing to common themes form the basis of further investigation. The qualitative step fits the objective of this study because public opinions are "grounded" in the social media discussion of IP location. We followed

Guest et al. (2011)'s guidelines of thematic analysis with a tweak using prior knowledge. Specifically, possible themes were identified using the outputs of the LDA model, and the structure of the themes was checked iteratively through deep reading of microblog posts and comments.

Topic modelling algorithms[23] were first applied to explore the insights on specific opinions. After cleaning the data, the Chinese text segmentation tool, Jieba[24] was used to extract features. A self-defined `weibo_dict` dictionary was written to help with the segmentation task. Stop words were removed by searching through `baidu_stopwords` and `cn_stopwords`, and only nouns, verbs, and adjectives that are longer than one Chinese character were kept. Next, the hyperparameters were tuned using a randomly sampled subset through grid search. The best coherence score was found when the number of topics (n) was three after testing the model with the number of topics from two to thirty. We then built our LDA models using microblog posts and comments from local Chinese users. The `u_mass` coherence score[25] was -3.065.

Table 4.1 shows the three topics and their top 30 keywords derived from the LDA model, and Figure 4.5 visualizes the top 10 keywords in each topic using word clouds. We computed the probabilities for each topic in every document (i.e., Weibo posts and comments) and determined the dominant topic for each document based on the highest probability. The "# of docs" column indicates the count of documents where the corresponding topic is the dominant one. Additionally, the average probability for each topic, $\bar{p}$, was calculated. Combined with the areas of the circles[26] generated using the pyLDAvis package in Figure 4.6, the prevalence of topics is ranked in the "T" column. The keywords[27] highlight the

[23]Related dictionaries can be found on `https://anonymous.4open.science/status/weibo_lda-B0F7`

[24]See `https://github.com/fxsjy/jieba`

[25]A `u_mass` value that is closer to zero indicates better topic coherence (Mimno et al., 2011).

[26]The larger the circle, the more prevalent the topic.

[27]The frequency distributions of the keywords are also represented as blue bars in Figure 4.6 (Sievert & Shirley, 2014).

underlying themes within each topic. In the first topic, users conveyed their support and favour for the IP location feature, as well as the real name system. They believed that this implementation brought forth opportunities to connect with new friends on the internet. This topic stood out as the predominant one, boasting the highest count of documents and average probability. Privacy concerns were raised in the second topic. Users expressed worries about the exposure of personal information and the potential risks of privacy violations. Moreover, the emergence of the paid IP proxy service garnered attention as it allowed users to change their IP addresses. This countermeasure, described as the underground industry in response to privacy concerns, was ranked second most discussed. The final topic primarily centred around keywords describing the IP location feature and its impact on various social media platforms. The inclusion of "irrelevant" indicated that some users felt minimal impact from the IP location feature and expressed a lack of concern. Therefore, it appeared that three distinct topics emerged from this corpus. We examined the intertopic distance map (Figure 4.6) and confirmed the absence of overlap between these three topics, indicating the relative independence of each topic.

Subsequently, we established a framework comprising of three main categories: *support* (theme 1), *opposition* (theme 2), and *indifference* (theme 3), ranked from the most popular to the least. These findings aligned with the overall impressions of journalists, such as Shen (2022), who noted a mixture of frustration and relief on the platform. Correspondingly, a public poll[28] conducted by *Economic View* yielded a similar outcome. The poll, conducted on April 28, 2022, questioned Weibo users' opinions on the newly introduced IP location feature. Among the 236,000 respondents, approximately 46% responded positively, supporting its implementation along with the "Real-name system." Meanwhile, 35% voiced disapproval, and 19% indicated a lack of concern. This poll further substantiated the credibility of the established framework, attesting to its authenticity rather than mere randomness.

[28] `https://weibo.com/5993531560/Lqwx2zPl2`

Table 4.1: Topics Extracted from the LDA Model

T	Top 30 keywords in each topic	# of docs	$\bar{p}$
1	display, Weibo, IP location, location, comment, address, IP address, Douyin, discover, attribution, function, net friend, open, account, support, province, real name, Zhihu, video, blogger, positioning, Xiaohongshu, homepage, platform, seem, like, keyword, surf the net, suggestion, social	94,996	0.476
2	network, privacy, *IP proxy*, platform, region, *seller*, data, exposure, *paid*, feel, information, infringement, *business*, minimum, video, personal information, *change*, *price*, means, internet, netizen, country, server, industry, system, *modify*, place, hot, *alleged*, risk	32,768	0.340
3	IP location, user, function, display, online, platform, Weibo, WeChat, speech, video, irrelevant, quality, network, open, Douyin, account, information, publish, rumour-mongering, related, content, provide, area, close, public, situation, start, longitude and latitude, full, personal homepage	9,332	0.183

We then started deep reading by filtering microblog posts and comments that contain the keywords in Table 4.1. Possible subtopics were identified and manually coded by quoting the original text, and subtopics were added or adjusted as the reading continued. The established topics became stable near the end of the process. The following sections anatomize the themes of the debate on Weibo grouped by users' standpoints.

4.4.1 Theme 1: Support

Supporters believed the IP location feature is suitable for "online environment purification". They accused the challengers of the policy of being *rumour-mongers* and defended the platforms' decision to quickly implement the feature for anti-disinformation. Supporters also called for more robust regulatory measures to increase transparency on social media platforms. Comments under this theme, as discerned from their tone and reasoning, exemplify the influence of cyber-nationalism in China.

Figure 4.5: Word Clouds of Top 10 Keywords in Each Topic

Concerned users are rumour-mongers. IP location advocates criticized the opponents of the IP location feature. The idea is that if you abide by the law and do not post inappropriate remarks, you need not worry about the publicity of your IP locations. The logic suggests that those who are panicking about the new feature are "foreign forces" spreading rumours on the internet and do not want their real locations to be exposed. Some users even said that "people of integrity do not need privacy", and absolute privacy is long gone when users choose to surf online. Other users believed that privacy invasion is non-existent at the provincial or country level. They did not understand the need to change their IP locations within China but expressed heightened concern if their exposed locations were more precise, such as their home addresses. *Jimu News* also interviewed the "experts" who claimed that the IP location feature "does not involve users' privacy rights" because users could not be identified by their provinces or countries (Zhan, 2022).

Publishing IP locations is helpful for anti-disinformation. One of the major arguments from supporters was that displaying users' IP locations would be helpful for reducing the impact of the "internet water army", who regularly post gossip and disinformation on social media. Although IP proxy services can be purchased for modifying IP locations, *Modern*

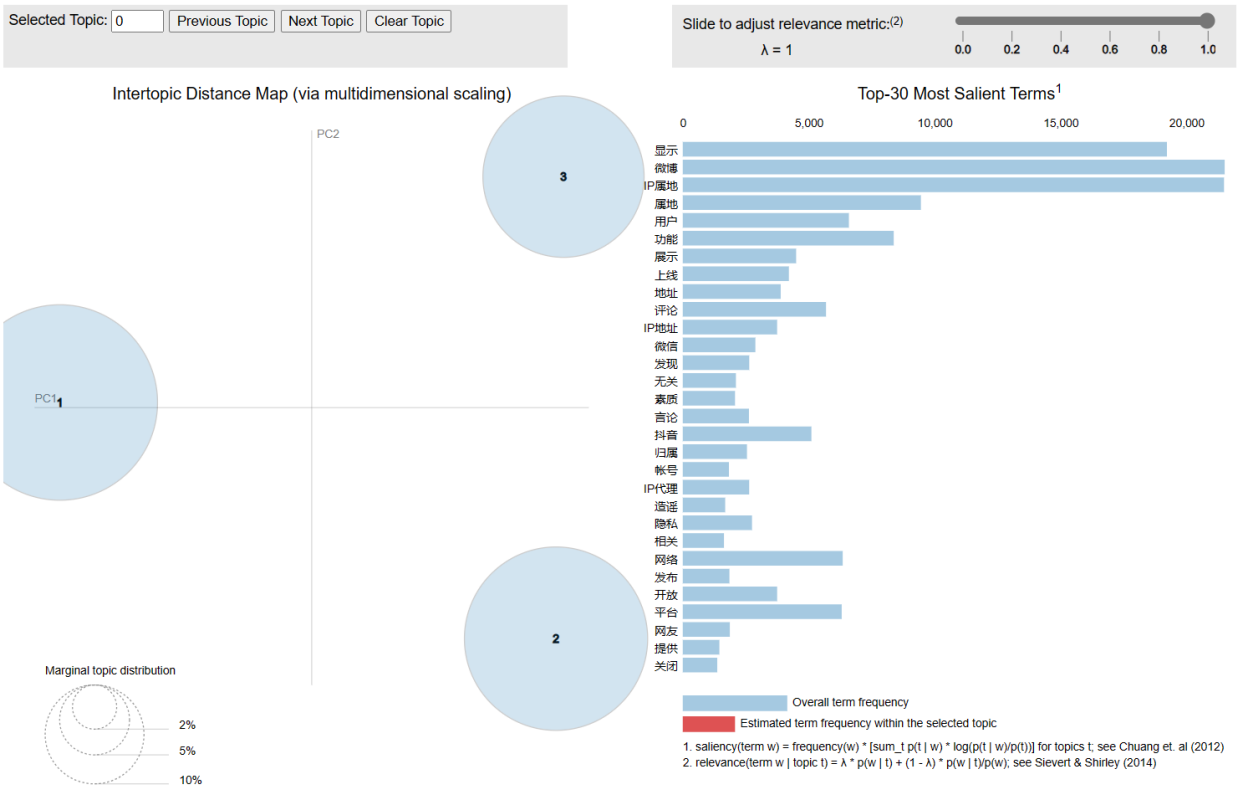

Figure 4.6: Intertopic Distance Map Generated Using pyLDAvis

Express reported that the IP addresses from the sellers were short-term and had few choices of locations (Ji, 2022). Other users also mentioned that the cost of changing IP locations would be insurmountable for the "internet water army" who controls thousands of accounts, which scales down the number of discordant comments on the internet. Regarding ordinary users, publishing their IP locations would also cause fear and discomfort. Thus, "the majority" of the users, according to the supporters, are expected to adjust their social interaction behaviours to promote "positive" voices online.

More actions are needed in blocking IP proxies. The prevalence of IP proxies has caught the media's attention. Supporters believed that IP proxies should be banned so that the display of real IP locations is not limited to well-behaved users. Some worried that the

boom of IP proxy services would lead to the prosperity of the underground economy and the associated value-added industries that are detrimental to the online environment. After media reports went public, many IP proxy services were blocked on popular e-commerce platforms. *China News* also warned users that personal information could be exposed when using IP proxy services. The state media concluded that changing IP addresses does not protect user privacy due to the involvement of third-party servers (Zuo, 2022).

Real-name identification is the solution. Some supporters recalled that platforms such as Coral QQ, Baidu Tieba, and other forums used to display partial or complete IP addresses of users, and the calls for privacy protection were not as strong as the concerns voiced after the launch of the IP location feature. If users did not care historically, they should not care now. In light of the limitations of IP location, some users favoured the real-name system and suggested various policies, including logging in with face IDs, displaying national IDs, and one account per platform. Some supporters also told the opponents that they should stop using Weibo and other social media platforms if they dislike their IP locations being displayed.

4.4.2 Theme 2: Opposition

The plethora of supporters did not deter opponents from expressing their views. Under certain hashtags, protesters dominated the comment section, possibly because "comment control" did not cover the whole spectrum of related keywords. Privacy invasion was repeatedly mentioned, and users shared their opinions of IP location being used as a tool for collective censorship. Negative consequences and political concerns were also brought up under this theme.

Displaying IP locations invades user privacy. Concerned users were upset about privacy loss from displaying IP locations. As the feature was rolled out across all major Chinese social media platforms, some realized the role of government behind the scenes and indicated that the announcement violated the principle of user privacy in the name of "for your good". Although mainstream media claimed that IP location in its current form does not involve user privacy issues, some netizens pointed out the simpleness of user trajectory analysis using IP locations. Combining Weibo posts and users' metadata, personal information could be easily exposed with the help of additional location information. Users are also worried about the collection and misuse of personal geographic data by third-party organizations. As a result, disappointed individuals used "streaking"[29] to describe social media activities in China.

Policymakers were aware of the privacy impacts of publishing IP locations. A controversy of *equality* emerged between rich and poor, public and private, and official and personal accounts. According to Weibo, verified users including orange (personal) and blue (organization) accounts have the option (through settings) to hide their IP locations (Youxia News, 2022). Critics therefore called for "equal treatment" if "defending the good order of the internet" was the original intention of the feature. Verified users were not the only privileged group. While people know that IP locations could be changed, not everyone has the technical knowledge of counter-surveillance, and some may not be able to afford the cost of IP proxy services. As many pointed out, the policy only regulates law-abiding individuals and takes privacy away from people in certain disadvantaged groups.

Since the implementation of the PIPL in 2021, enterprises such as e-commerce platforms have been required to provide users with the option to turn off personalized recommendations. In the case of IP location disclosure, the lack of *consent* also spurred questions about the limits of personal choice. Users were cognizant of the absence of privacy in China but

[29]Users felt that displaying personal locations online is similar to running naked in the public.

claimed that there was still a difference between governmental and public access to personal location information. Privacy was less of a concern to some if the information was only made available to law enforcement units. Others would like the right to turn off the feature and view voluntary and passive location disclosure as distinct actions. When users had no choice but to accept, some opted to change their IP locations using technical measures. Although some users mentioned that IP location was nothing new but a psychological strategy, opponents were against the mandatory display, especially those who travel frequently between provinces. Some indicated that their locations should not be made public if they had location permission settings at the operating system or application levels turned off on their mobile devices. To some, IP location disclosure was reminiscent of COVID-19 containment measures such as the *Big Data Itinerary Card*.

Collective censorship does not work as intended. Some opponents articulated the limited usefulness of publishing IP locations. The availability of IP proxy services means that the feature regulates good netizens but not villains, not to mention its adverse impacts on regional stereotypes. Some were also against banning IP proxy as they use the service for other purposes (e.g., web crawling and gaming). Users denoted that social platforms should be responsible for online speech censorship and should not ask every user to become the internet police. Using public opinions to suppress "improper" speech also raised the controversy of "moral blackmail", which means using moral standards to force people to keep silent. The potential use cases of the new metadata, such as celebrity tracking or data mining, are far removed from the stated purpose of anti-disinformation.

The *accuracy* of displayed IP locations was also a factor that impacted its usefulness. After the launch, many users were curious about the precision of their IP locations but soon found out that the displayed regions were not always accurate within China. Sometimes, the incorrect provinces were adjacent to the real ones, but in other situations, the two ad-

ministrative units were far away. In addition to the flawed mapping system, two different sources contribute to the fake locations. First, using IP proxy could increase the credibility of deceptive information, as mentioned previously. Second, not only fraudsters were incentivized to modify their IP locations – some users reported that their IP locations were changed when they posted microblogs about Covid-19 related protests[30]. The supposed tool of anti-disinformation, as a result, became a tool for concealing the truth.

Showing IP locations does more harm than good. Complaints were centred around the *mental pressure* of making every user's IP location public. Words and phrases such as "quitting the internet", "despairing", and "suffocating" were used to describe people's feelings. Users shared their fears and worried that few others would be willing to speak up about unfair treatment in the future. Since its debut in 2009, Weibo has become a social and political platform providing news and stimulating social movements in China (Chang, 2013). Many saw the mandatory disclosure of IP locations as yet another approach to control freedom of speech[31], and users were afraid of losing this vital venue of appealing for help. Second, concerned users expressed that showing IP locations would increase the degree of *regional discrimination*. On the one hand, xenophobia and hostility were amplified toward foreign users, especially those from Hong Kong and Taiwan. On the other hand, regional stereotypes (Young, 1988) became more evident among domestic users, and viewers might lean towards "rejecting a word because of the speaker." Some indicated that their current locations were not their hometowns and were tired of explaining this to their followers. Thus, IP location plays a role in intensifying conflicts in both situations. Third, (mainly female) users were anxious about *harassment* moving from online to offline. Women complained that they had already received disturbing private messages on Weibo, and IP locations made it

[30] `https://twitter.com/whyyoutouzhele/status/1587512921885736961`

[31] Weibo already has the functionality of "featured comments" that allows official accounts and Weibo VIP members to only display self-interested comments, and has a moderation team that constantly blocks accounts from posting improper contents.

easier for users in the same region to discover each other with the potential of stalking or doxing. Some privacy-conscious users, therefore, took precautionary measures and removed all location-indicative content (when possible) from their Weibo accounts.

The lack of public consultation is disappointing. While the government and media justified the new feature, some opponents derided the reasoning from the officials and suggested that the discussion should have happened before the wide implementation across platforms. The current exchange on Weibo, in the view of the opponents, was to persuade users who disagreed with authority, and any objection was immediately invalid. The outcry of democracy and human rights in this case was clear. Critics were centred around *obedience* vs. *resistance*: Participants were aware of the conflict between personal and communal interests but were unwilling to sacrifice privacy rights in exchange for so-called "national security." *Surveillance* was also a sub-theme of the discussion. Although the pervasiveness of big data has created a digital panopticon (H. Zhang & McKenzie, 2023), some were still hopeful as they believed that IP locations could only be used to track physical movements but not control people's minds. Apprehensions regarding the chilling effect were observed among users who expressed disapproval of the feature. The geographical disclosure at the provincial level might be acceptable. However, what if the granularity is increased (e.g., at the home address level)? The publication of personal locations, therefore, may inhibit or discourage freedom of speech. To some users, IP location in its current form might be a test of people's limits. If defiance is not present, citizens would have fewer rights in the long run. The analogy of the "boiling frog" was frequently invoked to depict the supporters as citizens gradually becoming accustomed to unfavourable changes.

4.4.3 Theme 3: Indifference

A group of users did not care about the debate as they thought displaying one's location had minimal impact on their daily lives. A small number of users in this group had mixed feelings. Their ambivalence toward this feature was platform-dependent and changed over time. The following paragraph summarizes notable opinions on this theme.

First, some felt that there was no privacy before the launch of the IP location feature, so a discussion on whether privacy had been compromised was unnecessary. Acknowledgement of a loss of privacy came from several directions. Some recognized that IP addresses had long been collected by the platforms, some complained delivery services had leaked their personal information, and some acknowledged people's level of acceptance from Covid-19 epidemiological surveys. Second, a few reiterating the idea that the Chinese do not have privacy stated that opponents should immigrate to a foreign country if they want privacy rights. Critics pushed back against this idea and considered that privacy perceptions should have been strengthened over time in China. The policy, in turn, was viewed as a setback. Finally, users' concerns varied as events unfolded. Some were highly concerned at the beginning, but their concern decreased as time went on. Some had no opinion when viewing others' IP locations, but as soon as they saw their own locations, they felt exposed.

4.5 Discussion

The preceding section explains the article's mixed-method approach, along with the outcomes of the thematic analysis. In this section, we put forth corresponding theories based on the findings and relevant literature.

Our initial theory revolves around users' motives for social media usage. As detailed in Section 4.2.2 and 4.2.3, individuals engage with social media platforms for purposes of enjoyment, relaxation, and personal expression (Whiting & Williams, 2013). The cloak of

anonymity in the virtual realm enables users to exhibit their true selves and evade judgment, a departure from the scrutiny often encountered within familiar circles. The introduction of the IP location feature, albeit at the provincial level, triggers privacy concerns as noted in Section 4.4.2. These diverse concerns include regional discrimination, trajectory exposure, and unwelcome harassment, particularly affecting female users. Consequently, users with such reservations aimed to adjust their posting and commenting behaviour by utilizing IP proxy services or altering/deleting the content they opt to share. Weibo has since witnessed the emergence of more controlled and carefully curated self-presentations.

> **Theory 1** Displaying IP location affects users' desire to share their spatial selves on social media.

It is noteworthy to highlight that from a statistical standpoint, proponents of the IP location feature surpassed those in opposition, as evidenced in Table 4.1. This phenomenon is attributed to the following two reasons, with the first pertaining to the understanding of privacy within Chinese culture (see Section 4.2.1). Even in contemporary China, certain members of society perceive privacy as containing concealed and potentially shameful secrets. This perspective may have led supporters to mistakenly believe that individuals attempting to mask their IP locations harbour harmful or illicit intentions when, in reality, these users might seek to protect their personal data. The other factor is the surge of cyber-nationalism within Chinese social media. Supportive voices were observed to be notably prevalent under specific hashtags, with nationalists striving to control comment sections to prevent any backlash against the implementation of IP location, which might negatively impact the government's image. These nationalists were predisposed to dismiss opposing viewpoints, even those grounded in logic. Their strong trust in the government led them to wholeheartedly endorse public policies without considering the ethical implications on data privacy.

> **Theory 2** A substantial Chinese demographic remains indifferent to their data

privacy.

Another explanation for the prevailing indifference among many Weibo users can be attributed to the limited impact of IP location at the provincial level. Specific scenarios, detailed in Section 4.4.2, illustrate instances where geoprivacy might be compromised even at the provincial scale. However, the psychological pressure resulting from such concerns appears to be confined to specific groups of vigilant users. As the chilling effect gains traction, it has a dampening influence on the overall level of interaction and information exchange across social media platforms, including the propagation of disinformation. To a certain extent, the uniform implementation of IP location serves as a calculated measure to counter disinformation stemming from individual accounts, though accompanied by various negative consequences. Conversely, opponents of the feature highlight the potential of altering IP locations, rendering it ineffective as an autonomous strategy for countering disinformation propagated by organized collectives.

Theory 3 Implementing IP location at the provincial level strikes a compromise between countering disinformation and preserving geoprivacy.

Figure 4.4 illustrates that the interest in discussing the IP location feature fluctuates as the event unfolded. While the discussions peaked during the feature's official implementation phase, they subsequently dwindled rapidly as other trending topics came to the forefront. This transient nature of interest has also been observed in Section 4.4.3. In contrast, certain users initially exhibited a lack of sensitivity, observing others' IP locations without much reaction. However, their perspective changed once they began posting and became aware of their own IP locations. These differing responses indicate the variance in individuals' geoprivacy attitudes based on specific circumstances.

Theory 4 Data privacy concerns are subject to short-term fluctuations and can evolve over time.

IP location, if we recall, is not the first instance of self-regulation invented by the Communist Party. As introduced in Section 4.2.4, the social credit system serves as a comprehensive data-driven surveillance mechanism operating on a larger scale, involving both incentives and penalties. Given that an increasing number of citizens are now exposed to information from diverse sources alongside state media, it was not unexpected to witness users expressing their disapproval and dissatisfaction on Weibo. Within this context, opponents raised concerns regarding the unequal treatment of average users compared to official accounts, the inaccurate display of some of their IP locations, and the absence of informed consent and choice in the implementation process. The self-discipline strategy does not consistently yield positive outcomes in this scenario and is likely to encounter more resistance as a growing number of Chinese individuals establish connections with the global community.

> **Theory 5** Forms of self-regulation do not invariably result in conformity and can lead to resistance.

As noted by Chang (2013), Weibo's ecosystem encompasses an array of public opinions that possess the potential to spark social movements. The diverse public views on the platform might explain why Weibo was chosen as the initial testing ground for the IP location feature. The display of users' IP locations serves a dual role: it encourages collective censorship, enabling others to identify evident disinformation, and it promotes self-censorship, as users become more hesitant to post contentious remarks due to privacy concerns. The passion of cyber-nationalists in overseeing the social media platform, combined with the proactive self-protective behaviour of concerned individuals, culminates in a scenario where the initiation of social movements becomes less probable on Weibo.

> **Theory 6** IP location as a censorship tool curtails Weibo's potential as a platform for social movements.

This study has limitations. The temporal change of opinions was difficult to capture. As with many other online discussions involving Chinese social media, users' attitudes shifted over time as new hot topics arose. Furthermore, our analysis only examined the reactions from one platform, Weibo. Social media applications such as Douban and Douyin may capture alternative voices as each user base is distinct. Finally, the use of LDA limits the scope of the deep reading to the topics (and associated terms) that were identified. Marginal suggestions, as a result, may not be captured in the discussion.

4.6 Conclusions

The addition of the IP location feature garnered significant attention upon its release in March and April 2022. These locations were automatically appended to posts and comments without users' consent on Chinese social media. The reception to this feature implementation was swift, generating a multitude of strong user opinions. Employing a mixed-methods approach, we analyzed these opinions and categorized the arguments in favour of and against the IP location feature. Our analysis revealed that densely populated regions along the east coast of China exhibited relatively higher user engagement in the discussion. Except for Hong Kong and Taiwan, the conversation predominantly featured female users. Broadly speaking, opposing viewpoints were discerned, with some expressing support and others registering disapproval. Our analyses demonstrated the diversity of public opinions, with certain perspectives evolving over time. Heated statements and confrontations often stemmed from proponents of the feature targeting privacy advocates with differing viewpoints. This phenomenon can be linked to the traditional Chinese association of privacy with "shameful secrets," coupled with users' tendency to exhibit zero tolerance for opposing opinions on the internet. Through our deep reading methodology, we unearthed an uneven distribution of contrasting views under various hashtags, signalling that dissenting voices might have been

overshadowed by the supporters, an approach previously employed to counter disinformation. This innovative attempt demonstrates the Chinese state's concern about disinformation and the deficient effect of conventional strategies such as information correction and content removal, which compelled authorities to impose intrusive measures at the expense of user privacy. Meanwhile, opponents of the feature remain skeptical about its efficacy in countering disinformation, given the accessibility of IP proxy services. In the future, the central regime should reevaluate the foundational principles of data privacy protection within the Civil Code and the PIPL, rectifying disparities that enabled the collection and involuntary disclosure of users' IP locations. While public authorities possess the capability to establish legal exemptions, the overuse of "national security" and "public interest" for privacy violations is likely to breed further distrust in the government.

4.7 References

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

Alemanno, A. (2018). How to counter fake news? A taxonomy of anti-fake news approaches. *European Journal of Risk Regulation*, *9*(1), 1–5.

An, L., Yu, C., Lin, X., Du, T., Zhou, L., & Li, G. (2018). Topical evolution patterns and temporal trends of microblogs on public health emergencies: An exploratory study of Ebola on Twitter and Weibo. *Online Information Review*, *42*(6), 821–846.

Anstead, N., & O'Loughlin, B. (2015). Social media analysis and public opinion: The 2010 UK general election. *Journal of Computer-Mediated Communication*, *20*(2), 204–220.

Bamman, D., O'Connor, B., & Smith, N. (2012). Censorship and deletion practices in Chinese social media. *First Monday*, *17*(3).

Bentham, J. (1791). *Panopticon; or, the inception-house.* Thomas Byrne.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *Journal of Machine Learning Research*, *3*, 993–1022.

Cao, J. (2005). Protecting the right to privacy in China. *Victoria University of Wellington Law Review*, *36*, 645–664.

Chang, X. (2013). China's Weibo: Political and social implications? *Education About Asia*, *18*(2), 16–20.

Chapman, A., Hadfield, M., & Chapman, C. (2015). Qualitative research in healthcare: An introduction to grounded theory using thematic analysis. *Journal of the Royal College of Physicians of Edinburgh*, *45*(3), 201–205.

Chen, B., Wang, X., Zhang, W., Chen, T., Sun, C., Wang, Z., & Wang, F.-Y. (2022). Public opinion dynamics in cyberspace on Russia-Ukraine war: A case analysis with chinese weibo. *IEEE Transactions on Computational Social Systems*, *9*(3), 948–958.

Cosgrove, E. (2019). *One billion surveillance cameras will be watching around the world in 2021, a new study says.* CNBC. Retrieved from `https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html` (Accessed: 2023-03-06)

Cui, S., & Qi, P. (2021). The legal construction of personal information protection and privacy under the Chinese civil code. *Computer Law & Security Review*, *41*, 105560.

Dong, X., & Lian, Y. (2021). A review of social media-based public opinion analyses: Challenges and recommendations. *Technology in Society*, *67*, 101724.

Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda. *Annals of the International Communication Association*, *43*(2), 97–116.

Ekenga, C. C., McElwain, C.-A., & Sprague, N. (2018). Examining public perceptions about lead in school drinking water: A mixed-methods analysis of Twitter response to an environmental health hazard. *International Journal of Environmental Research and Public Health*, *15*(1), 162.

Europol & Eurojust. (2018). *Common challenges in combating cybercrime.* Europol and Eurojust Public Information. Retrieved from `https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf` (Accessed: 2023-03-15)

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied thematic analysis.* Sage.

Han, X., Wang, J., Zhang, M., & Wang, X. (2020). Using social media to mine and analyze public opinion related to COVID-19 in China. *International Journal of Environmental Research and Public Health*, *17*(8).

Heilmann, S. (2016). Leninism upgraded: Xi jinping's authoritarian innovations. *China Economic Quarterly*, *20*(4), 15–22.

Helm, R. K., & Nasu, H. (2021). Regulatory responses to 'fake news' and freedom of expression: normative and empirical evaluation. *Human Rights Law Review*, *21*(2), 302–328.

Humphreys, L. (2012). Connecting, coordinating, cataloguing: Communicative practices on mobile social networks. *Journal of Broadcasting & Electronic Media*, *56*(4), 494–510.

Jaidka, K., Zhou, A., Lelkes, Y., Egelhofer, J., & Lecheler, S. (2022). Beyond anonymity: Network affordances, under deindividuation, improve social media discussion quality. *Journal of Computer-Mediated Communication*, *27*(1).

Jansen, S. C., & Martin, B. (2015). The streisand effect and censorship backfire. *International Journal of Communication*, *9*, 656–671.

Ji, Y. (2022). *They panicked after the "public display of IP location", and IP proxy went viral.* Xiandaikuaibao. Retrieved from `https://new.qq.com/rain/a/20220505A09ZF600` (Accessed: 2023-02-15)

Kaye, D. (2018). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.* United Nations. Retrieved from `https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement` (Accessed: 2023-03-15)

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593.

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... others (2018). The science of fake news. *Science*, *359*(6380), 1094–1096.

Lee, K.-F. (2018). *AI superpowers: China, silicon valley, and the new world order*. Houghton Mifflin.

Li, P., Cho, H., Qin, Y., & Chen, A. (2021). #MeToo as a connective movement: Examining the frames adopted in the anti-sexual harassment movement in China. *Social Science Computer Review*, *39*(5), 1030–1049.

Liu, J., & Zhao, H. (2021). Privacy lost: Appropriating surveillance technology in China's fight against COVID-19. *Business Horizons*, *64*(6), 743–756.

MacKinnon, R. (2011). Liberation technology: China's "networked authoritarianism". *Journal of Democracy*, *22*(2), 32–46.

Mendelson, A. L., & Papacharissi, Z. (2010). Look at us: Collective narcissism in college student Facebook photo galleries. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 259–281). Routledge.

Mimno, D., Wallach, H., Talley, E., Leenders, M., & McCallum, A. (2011). Optimizing semantic coherence in topic models. In *Proceedings of the 2011 conference on empirical methods in natural language processing* (pp. 262–272).

Mollema, L., Harmsen, I. A., Broekhuizen, E., Clijnk, R., De Melker, H., Paulussen, T., ... others (2015). Disease detection or public opinion reflection? Content analysis of tweets, other social media, and online newspapers during the measles outbreak in the netherlands in 2013. *Journal of Medical Internet Research*, *17*(5), e3863.

Nelson, L. K. (2020). Computational grounded theory: A methodological framework. *Sociological Methods & Research*, *49*(1), 3–42.

Nelson, L. K., Burk, D., Knudsen, M., & McCall, L. (2021). The future of coding: A comparison of hand-coding and three types of computer-assisted text analysis methods. *Sociological Methods & Research*, *50*(1), 202–237.

Papacharissi, Z. (2011). A networked self. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 304–318). Routledge.

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the us and the eu? *Penn State Journal of Law & International Affairs*, *8*(1), 49–117.

Pu, X., Jiang, Q., & Fan, B. (2022). Chinese public opinion on Japan's nuclear wastewater discharge: A case study of Weibo comments based on a thematic model. *Ocean & Coastal Management*, *225*, 106188.

Pye, L. W. (1991). The state and the individual: An overview interpretation. *The China Quarterly*, *127*, 443–466.

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. *Computer Law & Security Review*, *34*(6), 1342–1354.

Schwartz, R., & Halegoua, G. R. (2015). The spatial self: Location-based identity performance on social media. *New Media & Society*, *17*(10), 1643–1660.

Shen, X. (2022, May 2). *Weibo's new user location display appears to show that western tech gurus are based in China.* South China Morning Post. Retrieved from `http://www.scmp.com/tech/big-tech/article/3176272/weibos-new-policy-display-user-locations-prompts-some-humour-among` (Accessed: 2022-08-06)

Sievert, C., & Shirley, K. (2014). LDAvis: A method for visualizing and interpreting topics. In *Proceedings of the workshop on interactive language learning, visualization, and interfaces* (pp. 63–70).

State Council. (2014). *Planning outline for the construction of a social credit system (2014-2020).* China Copyright and Media. Retrieved from `https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/` (Accessed: 2023-03-06)

State Council. (2017). *Notice of the state council on issuing the plan for market regulation during the 13th five-year plan period.* China Law Info. Retrieved from `http://lawinfochina.com/Display.aspx?lib=law&Cgid=289420` (Accessed: 2023-03-06)

Stock, K. (2018). Mining location from social media: A systematic review. *Computers, Environment and Urban Systems*, *71*, 209–240.

Wang, Z., & You, Y. (2016). The arrival of critical citizens: Decline of political trust and shifting public priorities in China. *International Review of Sociology*, *26*(1), 105–124.

Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of big data: The survey and countermeasures. *Computer Law & Security Review*, *31*(6), 782–792.

Weibo Data Centre. (2020). *Weibo 2020 user development report.* Weibo. Retrieved from `https://data.weibo.com/report/file/view?download_name=4a774760-40fe-5714-498e-865d87a738fe&file-type=.pdf` (Accessed: 2023-04-12)

Westin, A. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research*, *16*(4), 362–369.

Xie, R., Chu, S. K. W., Chiu, D. K. W., & Wang, Y. (2021). Exploring public response to COVID-19 on Weibo with LDA topic modeling and sentiment analysis. *Data and Information Management*, *5*(1), 86–99.

Yan, J., & Wang, L. (1996). Legal protection and compensation for damage of the citizens' right to privacy. *Modern Law Science*, *1996*(2), 86–92.

Young, L.-C. (1988). Regional stereotypes in China. *Chinese Studies in History*, *21*(4), 32–57.

Youxia News. (2022). *Do not want to display your IP location on Weibo? Customer support gives a way to hide.* Youxia. Retrieved from `https://www.ali213.net/news/html/2022-4/672333.html` (Accessed: 2023-04-12)

Yuan, Y., Wei, G., & Lu, Y. (2018). Evaluating gender representativeness of location-based social media: A case study of Weibo. *Annals of GIS*, *24*(3), 163–176.

Zhan, X. (2022). *Full implementation of IP location, experts: No invasion of privacy.* `https://www.sohu.com/a/542710749_121284943`. Jimuxinwen. (Accessed: 2023-02-15)

Zhang, H., & McKenzie, G. (2023). Rehumanize geoprivacy: From disclosure control to human perception. *GeoJournal*, *88*(1), 189–208.

Zhang, K., & Kizilcec, R. (2014). Anonymity in social media: Effects of content controversiality and social endorsement on sharing behavior. In *Proceedings of the international AAAI conference on web and social media* (Vol. 8, pp. 643–646).

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283–289.

Zuo, Y. (2022). *Who is still wearing the "emperor's new clothes" after showing IP location?* China News. Retrieved from `https://www.chinanews.com.cn/cj/2022/05-07/9748106.shtml` (Accessed: 2023-02-15)

Preamble to Chapter 5

While Weibo serves as a rich source of public opinion, its distinctive user base must be acknowledged. Therefore, in this chapter, I expand my investigation beyond text analysis to include an online survey targeting broader Chinese internet users. The primary objective of this survey is to investigate the factors influencing geoprivacy behaviours. These factors include privacy knowledge, attitudes, and demographic variables such as age, gender, and geographic origin. Hypotheses were formulated based on the knowledge-attitude-behaviour model, and ordinal regression was employed to substantiate these hypotheses. Additionally, I explore underlying behavioural changes prompted by the IP location feature among Chinese users. The results of this survey offer compelling evidence that supports the continuum of geoprivacy knowledge, attitude, and behaviour, featuring the presence of privacy-conscious individuals, or "privacy actives," within the Confucius country. Collectively, the findings of this chapter, in conjunction with the discoveries from Chapter 4, enrich our comprehension of the dynamics of geoprivacy in the Chinese context.

Chapter 5

The Geoprivacy Knowledge-Attitude-Behaviour Triad

Abstract

Location privacy is unique as it often involves location-based services and geosocial media. China has an internet penetration rate of over 70% and a massive user base of social media. However, the topic of privacy attitudes among Chinese individuals remains understudied. We analyzed location privacy concerns in China through an online survey and regression analysis. Our findings suggest a positive relation among privacy knowledge, attitude, and behaviour, consistent with related literature. Declarative knowledge (e.g., privacy rights), on the other hand, was found to have a negative relation with privacy concerns, which has not been reported previously. In terms of demographic moderators, females had less privacy knowledge but more privacy protection behaviours, while the impact of age on privacy concerns was inconclusive. A notable discovery was the regional difference in privacy concerns within China, suggesting the potential geopolitical influence on individuals' values and beliefs. Combined with the uncovering of behavioural change in response to involuntary location disclosure, the results of this article challenge the conventional notion that Chinese individuals are indifferent to their online privacy, thus re-introducing an under-explored perspective from the global south into location privacy studies.

5.1 Introduction

Pervasive digital technologies have led to data privacy concerns for consumers and citizens. According to Zhou & Li (2014), data privacy concerns are related to individuals' understanding of privacy risks and potential negative consequences of information exposure. Data privacy concerns are distinct from physical privacy concerns, with the former targeting control of personal data and the latter focusing on boundaries and distance in the real world. The development of the World Wide Web and ubiquitous computing fosters an online environment that encourages information sharing, which, according to the cues-filtered-out theory (Sproull & Kiesler, 1986), is because social and contextual cues are absent in computer-mediated settings. At the same time, users' perceptions of online privacy risks persist substantially. In an analysis of app store reviews, for example, users' top complaints were centred around data privacy violations (Khalid et al., 2014). It is therefore important to achieve a balance between privacy protection and social benefits through application design and policy development. Measuring people's level of privacy concerns is one pathway toward privacy-aware design.

In this article, we investigate data privacy concerns related to geosocial media – in other words, location privacy concerns. Our society needs to be cautious about prevalent location data collection in essential online services and interactions. China, as an authoritarian state, was able to implement a widely applicable rule of compulsory location disclosure. By the end of April 2022, the internet-protocol-based location (or IP location) feature has been universally adopted on all major Chinese social media, including versatile platforms such as WeChat that can be difficult to break away from. Displayed at the provincial level for Chinese and country level for overseas IPs, the feature is less intrusive than publishing street-level locations, but the majority is prohibited from turning off the feature. As a result, IP location fundamentally alters the effectiveness of conventional practices for controlling information

flow, such as limiting post access. The public access to personal regional information has forced users to cope with the new norm.

Previous research on location privacy concerns primarily concentrates on contextual factors that could influence users' preferences regarding location sharing rather than studying users' cognitive processes behind location disclosure decisions. For example, Benisch et al. (2011) tracked 27 users' location sharing preferences and analyzed the impact of temporal and interpersonal factors on users' decision-making process. The availability of complex privacy settings increased the frequency of location sharing. The spatial factor (e.g., place types) was not adequately addressed. To fill in the research gap of the previous study, Lin et al. (2013) performed a similar analysis, adding work locations vs. homes in their survey and compared results between American and Chinese university students. Research in this field has also inquired about different types of privacy concerns. For instance, Li (2020) interviewed 47 Chinese university students and divided people's considerations into social privacy concerns (e.g., malicious personal attacks, sexual harassment, and targeted advertising) and constitutional privacy concerns (e.g., information leaks, location tracking, and surveillance). However, not all concerns are consistently negative, and users sometimes risk exposing their personal information in exchange for digital services. This phenomenon was also discovered in location-based mobile commerce, where not all users outweigh the value of privacy over personalization. For those who value their personal data, their privacy perceptions could also be ambivalent (Lee & Rha, 2016). This privacy paradox suggests the importance of understanding individuals' privacy attitudes, as a one-size-fits-all approach would likely fail to achieve its intended outcomes.

To the best of the authors' knowledge, this is the first study to explore the regional differences in location privacy concerns within China. There is a scarcity of studies that have specifically addressed location privacy concerns of Chinese individuals, even on a national scale (Li, 2020). Huang et al. (2021) compared people's level of privacy concerns regarding

location tracking for COVID-19 containment in the United States, Hong Kong, and South Korea. However, the study did not survey citizens in mainland China. Lin et al. (2013) identified some location-sharing patterns of Chinese students, but the participants were all from one university in Beijing. Considering the recent progressions in IP location policy and drawing upon the knowledge-attitude-behaviour model, this article aims to fill the research gap by conducting a survey involving participants from diverse occupations and regions throughout mainland China. The primary objective is to address the following research questions:

RQ1. What factors moderate individuals' privacy knowledge and attitudes? Here, we explore the impact of demographic variables such as gender, age, and region on privacy literacy and expectations.

RQ2. Do privacy knowledge and attitudes influence privacy-related behaviours? This inquiry investigates the potential interplay between knowledge and attitudes, knowledge and behaviours, and attitudes and behaviours.

RQ3. Does the introduction of the IP location feature change individuals' privacy behaviours? Are there substantial privacy concerns that could prompt users to stop posting on affected social media platforms? Or is there a privacy paradox where individuals continue using the applications despite acknowledging the privacy risks?

The remainder of this article is structured as follows: Section 5.2 reviews the theories and applications of the knowledge-attitude-behaviour model and develops the hypotheses and research model for the study. Section 5.3 outlines the survey and data analysis methodology employed. Section 5.4 presents the results of the statistical analysis. Section 5.5 discusses the policy implications and lists potential areas for future research. Finally, Section 5.6 concludes the article by summarizing the main findings.

5.2 The Knowledge-Attitude-Behaviour Model

5.2.1 Theoretical Background

The knowledge-attitude-behaviour (KAB) model, which uses the accumulation of knowledge to explain shifts in attitudes and subsequently behaviours, has been investigated in the context of modelling perceived privacy in location-based services (LBS) (Poikela, 2020; Seidl et al., 2020). Although there is a wealth of research on privacy concerns, existing theories on information disclosure offer diverse explanations for users' cognitive processes and online behaviours, lacking a consensus (Barth & De Jong, 2017). This section aims to review the pertinent theories and applications in the field.

Knowledge and Behaviour

The privacy calculus theory (Culnan & Armstrong, 1999) offers one explanation for the knowledge and behaviour relationship, stating that users engage in a rational risk-benefit assessment when deciding whether to disclose personal information. Users intend to disclose personal data when perceived benefits are greater than risks. Privacy knowledge (or literacy) is required in this mental process to assess the value of social rewards and make logical decisions about information disclosure. Generally, privacy knowledge can be divided into declarative knowledge (i.e., privacy rights and risks) and procedural knowledge (i.e., steps of privacy protection) (Debatin et al., 2009; Park, 2013). Both types of privacy literacy enhance an individual's ability to active privacy management (Baruh et al., 2017), which means that additional knowledge may lead to more conservative information disclosure behaviours. Contrarily, other studies have reported an opposite effect, indicating that increased knowledge may result in more permissive behaviours. One explanation is that heightened awareness of privacy risks and improved efficacy in privacy management diminish individuals' "fear of disclosure" (Turow & Hennessy, 2007). Alternatively, users may value more about applica-

tion functionality, design, and costs and care less about potential privacy risks even with adequate technical knowledge and financial resources (Barth et al., 2019). In other words, risk perception is not persuasive in applying privacy protection strategies (Oomen & Leenes, 2008).

While the precise connection between knowledge and behaviour may vary, additional theories provide support for the existence of this relationship. In game theory, for example, one party is unaware of all the utilities and rules of the other. The individual's privacy decision may thus be impacted by the missing information or knowledge of the counterpart, and the justification is named the theory of incomplete information (Harsanyi, 1967). The information-motivation-behaviour skills model (Fisher et al., 1994) also reinforces the presence of the relationship and is primarily used in examining health-related behaviours.

Attitude and Behaviour

The ambivalent relationship is more evident between privacy attitude and behaviour. Previous studies have found that while some users recognize privacy risks from using mobile LBS, they do not take appropriate actions to protect their location information. This disparity between one's attitude towards privacy and their actual privacy-related actions is known as the *privacy paradox* (Cottrill & Thakuriah, 2015; Li, 2020; Taddei & Contena, 2013). One widely cited explanation is the privacy calculus theory mentioned previously: people are willing to trade their private information for personal or social benefits through a rational risk-benefit calculation (Cottrill & Thakuriah, 2015; Huang et al., 2021; Jiang et al., 2013; Barth et al., 2019; Ricker et al., 2015). The benefits can range from retail values to personalized services (Acquisti & Grossklags, 2005). Privacy concerns can also be superseded by the app's appeal, promised gratifications, or users' time constraints (Barth & De Jong, 2017). Prior experience and privacy knowledge can mediate the risk-benefit calculation. When users lack experience with privacy breaches and their adverse consequences, they might underes-

timate the extent of privacy risks involved and engage in risky actions (Dienlin & Trepte, 2015), which indirectly demonstrates the validity of the theory of incomplete information.

The privacy calculus theory is reasonable and persuasive, yet unlike computers, humans have emotions and do not always make logical decisions. Other theories can, therefore, be categorized into affection-based explanations of the privacy paradox. Users could rely on their instincts without evaluating the potential risks of sharing information online (Barth & De Jong, 2017). Situational factors can bias these affect-based heuristics (e.g., subconscious valuation) and lead to decisions in contradictory to people's generic privacy attitudes (Kehr et al., 2015; Culnan & Armstrong, 1999). Online environment is a situational factor that promotes information sharing. The fuzzy boundaries make privacy violations less tangible and sensible in cyberspace compared to the real world (Acquisti et al., 2015). Consequently, individuals disregard cybersecurity and privacy incidents and persist in sharing their personal information in exchange for perceived advantages. In addition, information sharing can be an indispensable part of our daily life. As symbolic interactionism (Blumer, 1986) suggests, social interaction is the basis for society. People arrive at a consensus regarding events by engaging in communication and gradually exchanging information over time. Thus, the importance of maintaining social structures outweighs potential privacy risks, which offers another explanation of ambivalent privacy behaviours.

Although the privacy paradox exists, Baruh et al. (2017) reviewed 166 studies from 34 countries and concluded that privacy concerns usually lead to less frequent information disclosure and more frequent privacy protection. Moderating factors such as gender, culture, and regulations do not alter the generalized conclusion. In this sense, the positive correlation between privacy attitude and behaviour is observed more frequently. The theory of reasoned action (Ajzen & Fishbein, 1980) strongly supports this relationship by suggesting that people's behavioural intention is based on their attitude towards a specific behaviour and subjective norms. The intention, in turn, positively influences people's possibility of

taking certain actions. Parallel conclusions have likewise been attained in other studies. As an illustration, Ketelaar & Van Balen (2018) uncovered that an increased level of privacy concerns was correlated with a more negative attitude towards phone-embedded tracking. Moreover, this negative attitude was linked to more restrained location-sharing behaviours. Wu et al. (2012) also found that online privacy concerns had a significant negative correlation with willingness to disclose. Both findings substantiate the conclusion reached by Baruh et al. (2017).

5.2.2 Relevant Applications

Although this article is about online location privacy, the subject in question, *location*, is still associated with a region or a pair of coordinates in the physical environment. Hence, empirical studies in environmental psychology may share similar veins with research on privacy attitudes. Table 5.1 summarizes the findings from representative studies, in which the first part is related to environmental behaviour. The knowledge-attitude-behaviour model has been frequently applied in environmental psychology, but the relationship between the three remains undetermined. Levine & Strube (2012) studied college students' pro-environmental behaviours and found that their behaviours were significantly influenced by their knowledge about environmental issues. The students' explicit attitudes about the environment could also predict their behaviours through the mediation of pro-environment intentions. Polonsky et al. (2012) looked into carbon-related environmental issues and discovered a positive relation between knowledge and attitude, as well as attitude and behaviour. The hypotheses of the two pairs were tested by both general and domain-specific (i.e., carbon offset) questions presented in an online survey. Paço & Lavrador (2017) applied the model in energy consumption among Portuguese students but did not find solid supportive evidence of a correlation between the three subjects. Liu et al. (2020) extracted data from a large-scale

survey in China and confirmed the positive relation between knowledge vs. attitude and attitude vs. behaviour. Though a direct link between knowledge and behaviour could not be confirmed, attitude and intention mediated the relationship between the two.

Privacy-related studies and their findings are listed in the second part of Table 5.1. For example, Crossler & Bélanger (2019) examined users' location-protective behaviours and concluded that privacy knowledge determined users' location permissions on their smartphones. Furini et al. (2020) conducted two rounds of surveys, before and after educating the participants about common data abuse practices, and found that people's privacy concerns increased after learning about data collected by the installed applications. Finally, Seidl et al. (2020) surveyed people's geomasking behaviours (i.e., manipulation of personal locations for public sharing) and concluded that people's privacy behaviours were influenced by their privacy knowledge and attitude. Therefore, previous studies suggested various relationships between knowledge, attitude, and behaviour, and the results depend on the application domain, geographic region, and demographic group. The one consensus is that only positive relationships, if any, were detected. The positive correlations align with the conclusion by Baruh et al. (2017) in section 5.2.1. In other words, the privacy paradox is not a dominant phenomenon despite its widespread recognition. Therefore, we propose:

H1. Privacy knowledge is positively associated with privacy concerns.

H2. Privacy knowledge is positively associated with privacy protection behaviours.

H3. Privacy concerns are positively associated with privacy protection behaviours.

5.2.3 Moderating Factors

The conflicting interpretations between knowledge, attitude, and behaviour, as described in the prior sections, indicate the need for moderators in mediating the relations of the

Table 5.1: Empirical Studies on the Knowledge (K), Attitude (A), and Behaviour (B) Relationship

Reference	K vs. A	K vs. B	A vs. B	Country
Levine & Strube (2012)	x	+	+	United States
Polonsky et al. (2012)	+	N/A	+	United States
Paço & Lavrador (2017)	x	x	N/A	Portugal
Liu et al. (2020)	+	x	+	China
Crossler & Bélanger (2019)	N/A	+	N/A	United States
Furini et al. (2020)	+	N/A	N/A	Italy
Seidl et al. (2020)	N/A	+	+	United States

Notes: x: not significant; +: positive relationship; N/A: not available.

three (Ajzen & Fishbein, 2005; Baruh et al., 2017). Gender, age, and culture are three factors that can cause substantial variations. In terms of gender, females were found to have higher privacy concerns (Huang et al., 2021; Ketelaar & Van Balen, 2018), were less knowledgeable about technical countermeasures of privacy threats (Park, 2015), but more likely to act as privacy-conscious decision-makers (Hoy & Milne, 2010). Inconsistent findings were observed for privacy concerns between different age groups (Miltgen & Peyrat-Guillard, 2014; Hoofnagle et al., 2010). In certain instances, young people had higher privacy concerns (Huang et al., 2021) and adjusted their information-sharing behaviours more frequently (Ketelaar & Van Balen, 2018). In alternative scenarios, young people were more confident in their ability of personal data protection and showed less concern on privacy-related issues (Miltgen & Peyrat-Guillard, 2014). For example, in H.-S. Kim (2016), young users worried less about privacy risks when sharing locations on Facebook. The contradictory outcomes can be explained by the theories of privacy knowledge and behaviour outlined in section 5.2.1. Culture (e.g., collectivism vs. individualism) also influences people's location privacy attitude and behaviour as seen in the studies among European countries (Miltgen & Peyrat-Guillard, 2014), between the United States and China (Lin et al., 2013), and between the U.S. and East Asia (Huang et al., 2021). While a probe into privacy concerns within a single country and their geographical variances was not identified, it is worth noting that geographic

regions influence people's privacy attitudes to some extent based on national comparisons. The reason behind the absence of literature from this perspective can be explained by Tobler's first law of geography (Tobler, 1970): nearby things are more correlated than distant objects, so do individual minds, beliefs, and social norms within a national boundary. A notable variation in privacy concerns is less likely to be observed in a region with a similar cultural background. Therefore, we propose:

H4. Females possess lower levels of privacy knowledge but exhibit higher levels of privacy concerns and privacy protection behaviours.

H5. Young individuals possess higher levels of privacy knowledge but exhibit lower levels of privacy concerns and privacy protection behaviours.

H6. Privacy knowledge, attitude, and behaviour do not exhibit a significant difference among users from a single culture, even when considering their provincial origins.

A research model is developed based on the literature review and the six hypotheses (Figure 5.1).

5.3 Methodology

5.3.1 Measurement

We designed our online survey comprising 22 questions (refer to Appendix A), drawing from existing scales of online privacy and relevant studies in location privacy. A consent form (refer to Appendix B) is presented at the commencement of the survey and requires agreement before proceeding. The first section asked about respondents' internet experience (Q2–4), which determines their level of engagement on the social media platforms of interest and their prior encounter with privacy breaches. As indicated by Zafeiropoulou et al. (2013),

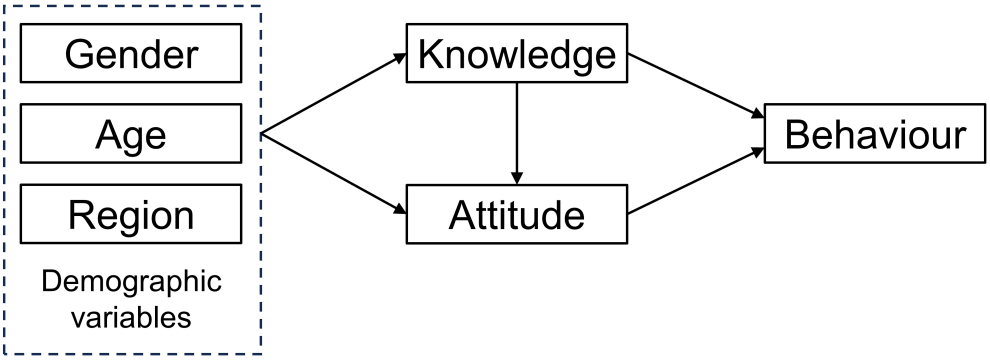

Figure 5.1: Research Model. On the left side, we hypothesize that females and older adults would demonstrate more pronounced privacy-protective behaviours, while the regions of origin would not have a statistically significant impact. On the right side, we expect a positive relationship between privacy knowledge, attitude, and behaviour.

users' privacy concerns were dependent on the online platforms they interact with. Next, we surveyed participants' location privacy knowledge based on the online privacy literacy scale in Trepte et al. (2015) and the online privacy questions in Hoofnagle et al. (2010), with the former targeting Europeans and the latter fitting Americans. Both declarative (Q5 & 7) and procedural (Q6) knowledge were covered. Specific questions about IP location were asked, with the remainder tailored to the Chinese context. Following privacy knowledge, a significant portion of the survey questions (Q8–9, 11–13) focused on location privacy attitudes. Questions (Q8 & 11) in this section employed a five-point Likert scale, which were inspired by the Internet Users' Information Privacy Concerns (IUIPC) (Malhotra et al., 2004) and the privacy concerns related questions in Hoofnagle et al. (2010) and Zafeiropoulou et al. (2013). Map scale was explored (Q12) as it impacts people's perceived location disclosure risk (J. Kim et al., 2021). Then, location privacy behaviours were inquired (Q14–15) by adapting questions from Hoofnagle et al. (2010) and Seidl et al. (2020). Again, the Likert scale was used to assess participants' personal beliefs. Privacy protection practices such as misrepresentation (Jiang et al., 2013) were considered. Regarding location privacy, people

may choose to enter inaccurate locations when prompted (Q14.4). The last section (Q16–22) covered demographic variables such as respondents' gender, age, and geographic origins. Skill-testing questions (e.g., Q1 & 10) were included throughout the survey, and two Likert scale questions (Q8.3 & 8.4) were repeated in Q11 using slightly different phrases to ascertain respondents' attentiveness to the questions and the consistency of their responses.

5.3.2 Data Collection and Cleaning

We chose to host the survey on Credamo[32], a professional research and survey platform that has more than 3 million users. Only adults (people who were over 18 years old) were invited to participate in the study. China was selected as the study area because of its large population base and cohesive cultural composition. The majority of individuals from China (73%), according to World Bank (2021), have access to the internet. Among those internet users, over 97% interact with at least one social media platform (Kemp, 2023). The survey was randomly distributed by Credamo in 31 provincial-level administrative regions of China (excluding Hong Kong, Macao, and Taiwan) from December 2022 to January 2023. Each participant was offered a cash incentive of three Chinese yuan (about 0.44 USD). Fifty responses were collected per iteration, resulting in a total of 1,000 responses obtained. After multiple iterations, we noticed that more females completed the survey, so males were targeted to improve the sample's representativeness. To avoid data scarcity, respondents' self-reported province of origin were grouped into seven regions based on Figure 5.2.

Data cleaning was conducted to ensure the validity of the analysis. Responses that fell outside the acceptable range, either exceeding the 95^{th} percentile in duration of completion or falling below the 5^{th} percentile, were excluded from the analysis. Skill-testing questions (e.g., Q1 & 10) were also used to filter valid responses, and only responses who answered the questions correctly were kept. The answers of Q8.3 & 8.4 were compared with the repeated

[32] `https://www.credamo.world/`

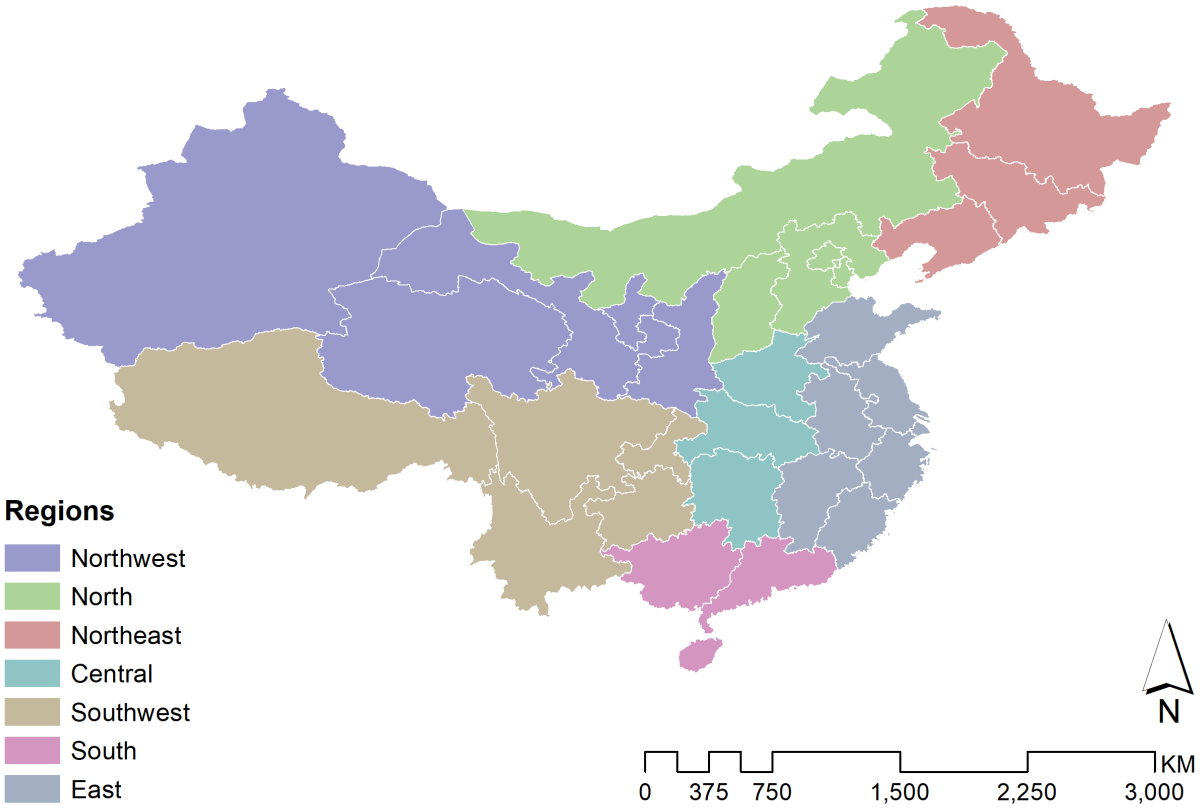

Figure 5.2: Regions of Mainland China Explored in the Study[33]

counterparts (the answers of Q11.4 & 11.3), and only responses that were less than or equal to one Likert point away were accepted. If "Not sure" was selected in Q8.3 or 8.4, the counterpart had to be the same to remain in the analysis. Finally, to ensure the moderating factors could be properly assessed, participants who reported "Prefer not to answer" in their demographic statistics were removed as the final step. This process yielded a total of 491 responses available for subsequent data analysis.

5.3.3 Data Analysis

Ordinal regression was frequently used in analyses of privacy preferences (e.g., Stutzman et al., 2011; Cho et al., 2019; Poikela, 2020; Seidl et al., 2020). In this analysis, we employed ordinal logistic regression using backward elimination based on the ordered categorical variables extracted from the survey (see Table 5.2). Different Likert scales were transformed into a common five-point scale. Measures in reverse order were recoded so that higher scores consistently indicate greater levels of privacy knowledge, increased privacy concerns, and enhanced privacy protection behaviours. Males and females were coded as 1 and 0 respectively. Spearman's correlation matrix (Spearman, 1904) was implemented to spot significant predictors of the response variables. An ordinal regression model was built for each knowledge, attitude, and behaviour variable in Table 5.2. Only statistically significant explanatory variables ($p<0.05$) were included in the models, except for the categorical variable of respondents' geographic origin. Results of the most relevant regression models, categorized by knowledge (models 1 to 2), attitude (models 3 to 13), and behaviour (models 14 to 20), are presented in Table 5.4 and Table 5.5. Additional models can be found in Appendix C.

[33]This map of the study area does not depict geopolitical boundaries that are controversial or under dispute.

Table 5.2: Variable Definitions

Groups	**Var.**	**Descriptions**	**References to Survey Questions**
Experience	E1	Weibo usage frequency	Average of Q2_Weibo and Q3_Weibo
	E2	Douyin usage frequency	Average of Q2_Douyin and Q3_Douyin
	E3	WeChat usage frequency	Average of Q2_WeChat and Q3_WeChat
	E4	Prior experience of privacy breach	Q4
Knowledge	K1	Location data collection practices	Sum of correct options selected in Q5
	K2	Privacy law	Q6
	K3	Location privacy protection techniques	Sum of correct options selected in Q7
Attitude	A1	Concerns of location disclosure	Q8.1
	A2	Concerns of location data collection	Q8.2
	A3	Temporal change of location privacy concerns	Average of Q8.3 and Q11.4
	A4	Views of others' location privacy concerns	Recoded average of Q8.4 and Q11.3
	A5	Misuse of displayed location information	Q11.1
	A6	Misuse of collected location information	Q11.2
	A7	Scope of the IP location feature	Q11.5
	A8	IP location vs. GPS location	Q11.6
	A9	The missing function of hiding IP location	Q11.7
	A10	Cares towards the IP locating process	Q11.8
	A11	Lack of confidence in IP location accuracy	Recoded Q11.9
	A12	Geographic scale of IP location	Recoded Q12
Behaviour	B1	Turn off mobile location services	Recoded Q14.1
	B2	Not share locations on social media	Recoded Q14.2
	B3	Not allow location access when prompted	Recoded Q14.3
	B4	Enter inaccurate location data	Q14.4
	B5	Use IP location to follow celebrities	Q14.5
	B6	Test IP location accuracy	Q14.6
	B7	Quit social media after April 2022	Q15
Demographic	D1	Gender	Q16
	D2	Age	Q17
	D3	Regions of origin	Aggregated Q18 based on Figure 5.2

5.4 Results

5.4.1 Sample Characteristics

Table 5.3 showcases the demographic distribution of the 491 participants who remained in the study. The majority of the participants were between the age of 20 to 39, with the median in the range of 30 to 34. The respondents were highly educated: more than 90% of the respondents hold a bachelor's degree or above. However, income inequality is observed despite a skewed distribution of education backgrounds. One explanation of the widespread distribution of monthly income could be the various economic development levels across the country. Most participants originated from East China, followed by North China and South China. The region with the lowest representation was Northwest China, which reflects the unequal population distribution on the vast land.

5.4.2 General Location Privacy Concerns

We first illustrate the general trends in participants' internet experience and their knowledge, attitudes, and behaviours related to location privacy. According to the violin plots (Figure 5.3), Douyin (E2) emerged as the most widely used social media platform, surpassing the popular microblogging site Weibo (E1) and instant messaging app WeChat (E3). Only a small proportion of respondents reported no prior experience of privacy breaches in the past five years (E4), with the majority encountering such breaches once or twice. In Figure 5.4, while participants demonstrated a general awareness of the potential methods of location data collection on social media (K1), their knowledge regarding countermeasures for location surveillance (K3) was comparatively limited. In fact, their declarative knowledge (K2), especially regarding the recently implemented Personal Information Protection Law (PIPL), was notably low, with a majority of respondents expressing uncertainty about its specifics.

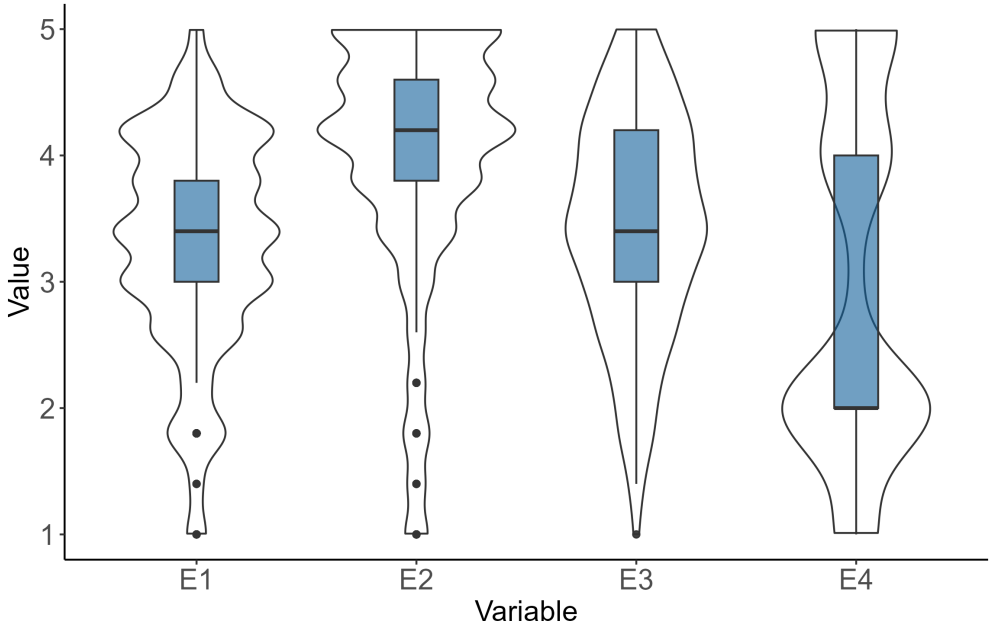

Figure 5.3: Violin Plots of Experience: Weibo (E1), Douyin (E2), and WeChat (E3) usage frequency, as well as prior experience of privacy breach (E4).

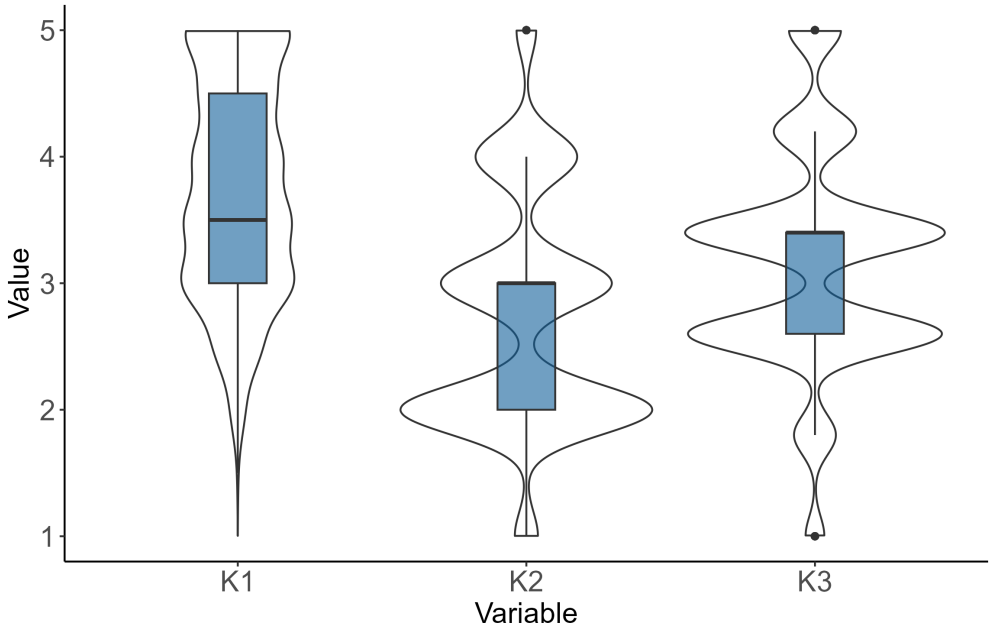

Figure 5.4: Violin Plots of Knowledge: location data collection practices (K1), privacy law (K2), and location privacy protection techniques (K3).

Table 5.3: Demographic Statistics

Variables	**Levels**	**Frequency**	**Percentage (%)**
Gender	Male	240	48.9
	Female	251	51.1
Age	≤19	2	0.4
	20-24	86	17.5
	25-29	147	29.9
	30-34	145	29.5
	35-39	53	10.8
	40-44	14	2.9
	45-49	24	4.9
	≥50	20	4.1
Region of origin	Northwest	16	3.3
	North	86	17.5
	Northeast	31	6.3
	Central	49	10.0
	Southwest	32	6.5
	South	77	15.7
	East	200	40.7
Education	High school or below	5	1.0
	Associate	41	8.4
	Bachelor's	358	72.9
	Master's or above	87	17.7
Monthly income (¥)	≤1,500	30	6.1
	1,501-3,000	36	7.3
	3,001-5,000	63	12.8
	5,001-8,000	128	26.1
	8,001-10,000	89	18.1
	10,001-15,000	67	13.6
	15,001-20,000	40	8.1
	≥20,001	38	7.7

Regarding location privacy attitude (Figure 5.5), the majority of participants agreed that they were not always willing to share their locations on social media (A1), and their concerns regarding pervasive location data collection remained high (A2). In fact, the respondents' location privacy concerns were more pronounced compared to five years ago (A3). Interestingly, while some respondents felt that others were overly concerned about privacy, a larger number of individuals indicated otherwise (A4). When comparing privacy concerns related

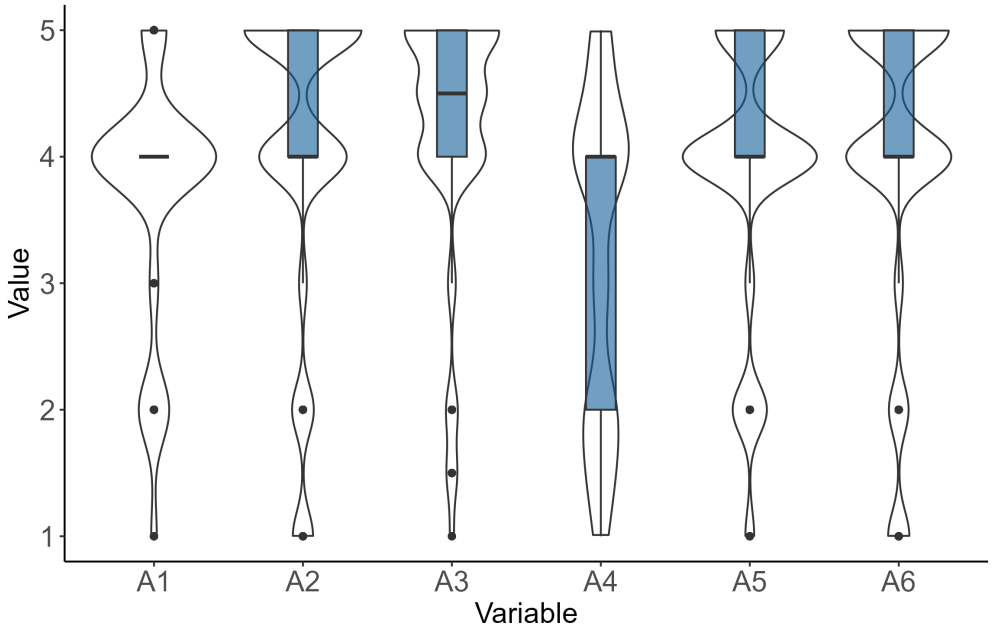

Figure 5.5: Violin Plots of General Attitudes: the concerns of location disclosure (A1) and location data collection (A2), temporal change of location privacy concerns (A3), views of others' location privacy concerns (A4), and attitudes towards the misuse of displayed (A5) and collected (A6) location information.

to publicly displayed personal locations (A5) and locations collected in the background (A6), more concerns were observed in the latter case.

In terms of location privacy behaviour (Figure 5.6), the privacy paradox was evident: despite the high level of privacy concerns expressed, people demonstrated a willingness to share their locations and did not adopt more restrictive behaviours. Most individuals kept their location services enabled (B1) and consented to location access when prompted (B3). Although respondents displayed some selectivity in sharing their locations on social media (B2), the majority did not intentionally provide inaccurate location information (B4).

Correlations Between Knowledge, Attitude, and Behaviour

The correlation matrix is calculated to understand the relationship between knowledge, attitude, and behaviour. Only significant correlation coefficients ($p \leq 0.05$) are presented in

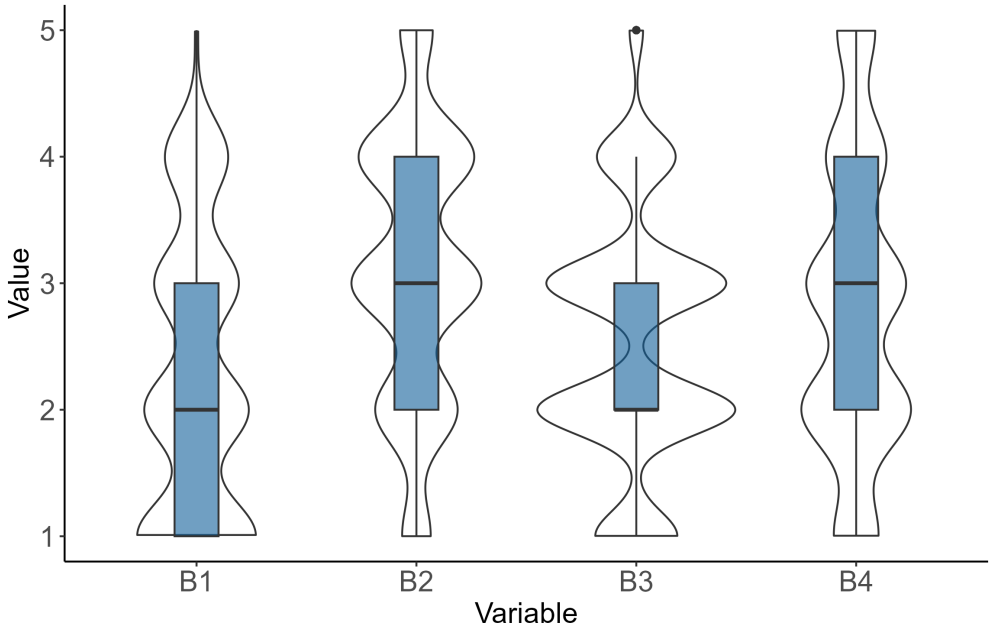

Figure 5.6: Violin Plots of General Behaviours: turning off mobile location services (B1), not sharing locations on social media (B2), not allowing location access when prompted (B3), and entering inaccurate location data (B4).

Figure 5.7. Regarding internet experience, higher engagement on one social media platform was associated with increased participation on others (0.32 to 0.41). However, social media usage negatively correlated with prior experiences of privacy breaches (-0.09 to -0.13). Generally, greater social media usage and previous negative experiences were linked to a higher level of privacy knowledge (0.10 to 0.32). One exception was that respondents with more privacy violation experiences exhibited lower levels of declarative privacy knowledge (-0.13). In terms of attitude, individuals who used social media more frequently expressed lower privacy concerns (-0.10 to -0.24), while those who had experienced privacy breaches held opposite views (0.18 to 0.31). A similar relationship could be noted between internet experience and privacy behaviour (-0.09 to -0.25 for E1 to E3 vs. B1 to B4, and 0.14 to 0.29 for E4 vs. B1 to B4).

Overall, knowledge, attitude, and behaviour variables positively correlated with them-

selves. While not all correlations were statistically significant, increased procedural knowledge (K1 & K3) tended to be associated with higher privacy concerns (0.09 to 0.14), while greater declarative knowledge (K2) was linked to reduced concerns (-0.12 to -0.26). The relationship between knowledge (K1 to K3) and behaviour (B1 to B4) was not clear, with both positive and negative correlations present, and few significant results were found. Regarding attitude (A1 to A6) and behaviour (B1 to B4), privacy concerns were generally positively associated with privacy behaviours (0.15 to 0.47).

In terms of demographic variables, males demonstrated higher privacy knowledge (0.13) and lower privacy protection behaviours (-0.09 to -0.11), while older respondents displayed more declarative knowledge (0.21) and fewer privacy concerns (-0.06 to -0.07). The relationships between gender and attitude, as well as age and behaviour, were not established.

Ordinal Regression Results

Ordinal regression results are presented in Table 5.4 and 5.5, where the former lists the model coefficients, and the latter provides the fit-measure statistics of the regression models. First, about knowledge and demographic variables (Model 1), it was observed that older respondents possessed higher levels of declarative privacy knowledge. In terms of countermeasures for location surveillance (Model 2), male respondents exhibited greater knowledge. Southwest had the highest level of procedural knowledge in location spoofing, followed by Northwest, while Northeast had the lowest level.

Next, we summarize the findings with privacy attitude as the response variable (Models 3 to 8). Regarding experience, an increase in Weibo usage was associated with a lower belief that other people were overconcerned about location privacy. In contrast, an increase in WeChat usage showed the opposite effect (Model 6). Additional engagement in Douyin, similar to WeChat users, resulted in fewer concerns about location sharing on social media (Model 3). Consistently, prior privacy breach experiences increased respondents' level of loca-

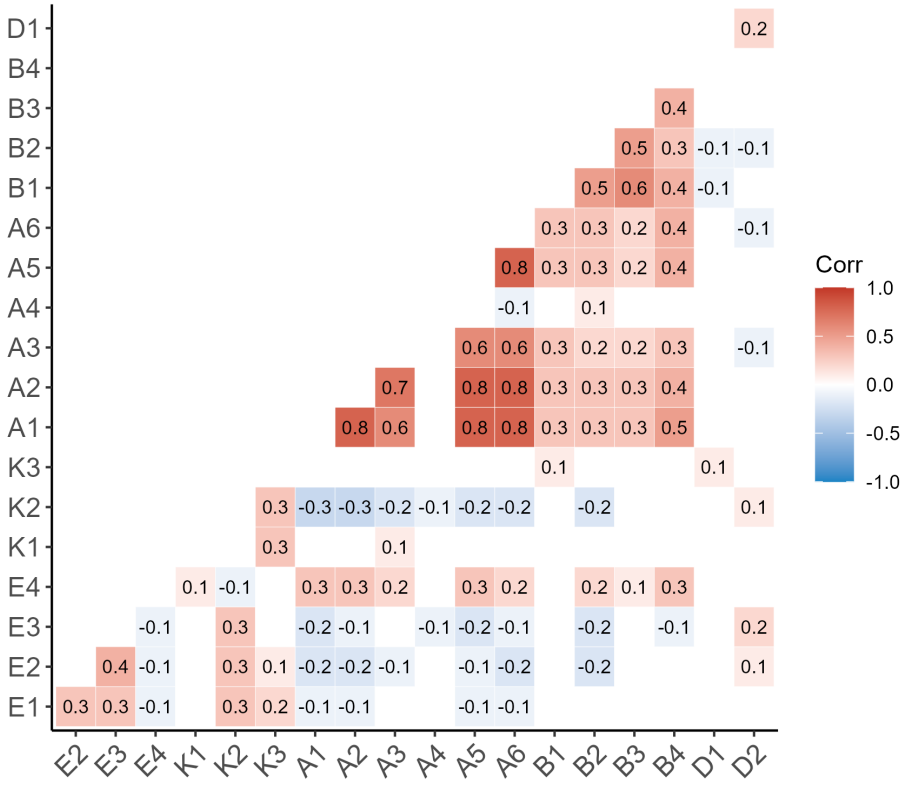

Figure 5.7: Correlation Matrix. Displayed values are statistically significant correlation coefficients (significance level = 0.05).

tion privacy concerns across the board (except for Model 6, where E4 was insignificant). For knowledge and attitude, declarative knowledge consistently decreased respondents' privacy concerns (Models 5, 7, and 8), while procedural knowledge had the opposite effect (Models 3 to 8). Regarding demographic variables, age and gender were not significant moderating factors of attitude. Compared to Northeast China, other regions exhibited a higher level of privacy concerns (Models 3, 6, and 7). Northwest experienced the greatest increase in concerns about location sharing on social media (Model 3) and the potential misuse of public location data (Model 7). On the other hand, East China had the lowest degree of agreement on the statement regarding overconcerned media and netizens about privacy (Model 6).

We then built our models with privacy behaviour as the dependent variable (Models 14 to 17). In terms of experience, frequent users of each platform displayed their own characteristics. Frequent Weibo users were less likely to allow location access when prompted (Model 16), frequent Douyin users shared their location on social media more frequently (Model 15), and frequent WeChat users enabled location services on their phones less frequently (Model 14). Prior experiences of privacy incidents led to an increase in inaccurate address submissions online (Model 17) and a decrease in location disclosure on social media (Model 15). Regarding knowledge and behaviour, we observed that greater knowledge about location spoofing resulted in less frequent enabling of location services (Model 14). In the relationship between attitude and behaviour, a higher degree of privacy concerns corresponded to a higher degree of privacy protection behaviours. This relationship was consistent across all four behavioural variables (Model 14 to 17). Regarding demographic variables, males more frequently enabled location services on their phones and shared locations on social media (Model 14 & 15). Compared to Northeast China, Southwest exhibited the largest increase in privacy protection behaviours (Model 14 & 16), making it the most conservative region when it comes to enabling location services and granting location access on phones. Participants from Northwest China exhibited a surprising openness to location disclosure, which

contradicted their high level of privacy concerns (Model 14 to 16). However, the decrease in privacy protection behaviours in the Northwest region was not statistically significant (p ranges from 0.28 to 0.99).

Table 5.4: Regression Results

Model	Response Variable	Predictor	Estimate	SE	Z	p
1	K2	D2	0.161	0.056	2.890	0.004
2	K3	D1	0.465	0.168	2.760	0.006
		D3: East – Northeast	0.456	0.348	1.310	0.190
		Central – Northeast	0.581	0.420	1.380	0.167
		North – Northeast	0.649	0.380	1.710	0.088
		South – Northeast	0.783	0.385	2.030	0.042
		Northwest – Northeast	1.066	0.553	1.930	0.054
		Southwest – Northeast	1.153	0.479	2.410	0.016
3	A1	E2	-0.312	0.102	-3.060	0.002
		E4	0.445	0.072	6.180	<.001
		K2	-0.484	0.108	-4.480	<.001
		D3: East – Northeast	1.083	0.404	2.680	0.007
		Central – Northeast	1.526	0.488	3.120	0.002
		North – Northeast	1.379	0.439	3.140	0.002
		South – Northeast	0.912	0.442	2.060	0.039
		Northwest – Northeast	2.226	0.646	3.440	<.001
		Southwest – Northeast	0.984	0.529	1.860	0.063
4	A2	E4	0.315	0.063	4.980	<.001
		K2	-0.551	0.103	-5.350	<.001
		K3	0.348	0.107	3.260	0.001
5	A3	E4	0.286	0.061	4.720	<.001
		K1	0.198	0.095	2.090	0.037
		K2	-0.227	0.092	-2.470	0.014
6	A4	E1	0.266	0.103	2.588	0.010
		E3	-0.268	0.100	-2.677	0.007
		K2	-0.243	0.099	-2.452	0.014
		D3: East – Northeast	1.097	0.329	3.337	<.001
		Central – Northeast	0.216	0.391	0.553	0.580
		North – Northeast	0.197	0.351	0.562	0.574
		South – Northeast	0.778	0.363	2.143	0.032
		Northwest – Northeast	0.434	0.556	0.781	0.435
		Southwest – Northeast	0.322	0.432	0.746	0.456
7	A5	E4	0.395	0.065	6.040	<.001

Continued on next page

Table 5.4 – continued from previous page

Model	Response Variable	Predictor	Estimate	SE	Z	*p*
		K2	-0.365	0.105	-3.470	<.001
		K3	0.192	0.107	1.790	0.073
		D3: East – Northeast	0.762	0.371	2.050	0.040
		Central – Northeast	0.932	0.442	2.110	0.035
		North – Northeast	0.939	0.403	2.330	0.020
		South – Northeast	0.979	0.412	2.370	0.018
		Northwest – Northeast	1.677	0.588	2.850	0.004
		Southwest – Northeast	0.660	0.495	1.330	0.183
8	A6	E4	0.212	0.061	3.460	<.001
		K2	-0.332	0.097	-3.410	<.001
		K3	0.253	0.105	2.420	0.016
13	A12	E2	-0.174	0.088	-1.982	0.047
		E3	0.203	0.100	2.022	0.043
		K1	0.323	0.097	3.345	<.001
		D1	-0.432	0.168	-2.576	0.010
		D3: East – Northeast	0.843	0.378	2.231	0.026
		Central – Northeast	0.410	0.436	0.940	0.347
		North – Northeast	0.431	0.405	1.065	0.287
		South – Northeast	0.327	0.406	0.804	0.422
		Northwest – Northeast	0.471	0.575	0.819	0.413
		Southwest – Northeast	0.633	0.470	1.345	0.179
14	B1	E3	0.243	0.100	2.433	0.015
		K3	0.270	0.096	2.816	0.005
		A1	0.540	0.117	4.603	<.001
		A3	0.236	0.115	2.048	0.041
		D1	-0.373	0.171	-2.185	0.029
		D3: East – Northeast	0.505	0.379	1.332	0.183
		Central – Northeast	-0.026	0.455	-0.057	0.954
		North – Northeast	0.677	0.410	1.652	0.098
		South – Northeast	0.708	0.416	1.702	0.089
		Northwest – Northeast	-0.651	0.600	-1.085	0.278
		Southwest – Northeast	1.420	0.480	2.961	0.003
15	B2	E2	-0.270	0.087	-3.094	0.002
		E4	0.147	0.062	2.375	0.018
		A1	0.515	0.091	5.633	<.001
		A4	0.153	0.068	2.256	0.024
		D1	-0.439	0.171	-2.572	0.010
		D3: East – Northeast	0.742	0.358	2.075	0.038
		Central – Northeast	0.986	0.424	2.325	0.020

Continued on next page

Table 5.4 – continued from previous page

Model	Response Variable	Predictor	Estimate	SE	Z	*p*
		North – Northeast	0.578	0.386	1.495	0.135
		South – Northeast	0.831	0.390	2.128	0.033
		Northwest – Northeast	-0.004	0.575	-0.007	0.994
		Southwest – Northeast	0.742	0.448	1.655	0.098
16	B3	E1	0.239	0.100	2.386	0.017
		A1	0.692	0.091	7.640	<.001
		D3: East – Northeast	0.622	0.357	1.739	0.082
		Central – Northeast	0.740	0.424	1.746	0.081
		North – Northeast	0.718	0.392	1.832	0.067
		South – Northeast	0.980	0.394	2.487	0.013
		Northwest – Northeast	-0.517	0.561	-0.922	0.356
		Southwest – Northeast	1.654	0.454	3.647	<.001
17	B4	E4	0.235	0.062	3.780	<.001
		K2	0.177	0.094	1.890	0.059
		A1	0.646	0.139	4.650	<.001
		A5	0.443	0.125	3.550	<.001
20	B7	E1	0.269	0.105	2.570	0.010
		A1	0.535	0.153	3.500	<.001
		A3	0.452	0.124	3.640	<.001
		A4	-0.213	0.072	-2.950	0.003
		A5	0.458	0.143	3.200	0.001

5.4.3 Specific Concerns Regarding IP Location

This section reports IP-location-related privacy attitudes and behaviours of the survey participants. Starting at attitudes (Figure 5.8), the distributions to answers of A7, A8, and A9 were similar. The majority of respondents agreed that limiting the scope of the IP location feature will reduce their privacy concerns (A7), and users' privacy is violated when the feature cannot be turned off (A9). Still, the preponderance also agreed that the IP location feature is less intrusive than GPS location (A8), and the accuracy of their IP locations can be trusted (A11). The satisfaction of location accuracy was followed by a strong desire to know the location determination process (A10), signalling the importance of transparency. In terms of the most appropriate geographic scale (A12), nearly 40% of respondents preferred

Table 5.5: Regression Model Summary

Model	Response Variable	Deviance	AIC
1	K2	1245	1255
2	K3	1397	1421
3	A1	958	984
4	A2	1158	1172
5	A3	1435	1453
6	A4	1719	1749
7	A5	1108	1134
8	A6	1199	1213
13	A12	1514	1544
14	B1	1277	1307
15	B2	1333	1363
16	B3	1273	1297
17	B4	1336	1352
20	B7	1032	1050

Note: AIC = Akaike information criterion.

IP location to be displayed at the provincial level (if necessary), followed by country and regional levels. Less than 15% of respondents believed that a finer scale would balance between privacy protection and anti-disinformation, and none selected street level in the responses. In Model 13 (Table 5.4), we discovered that Douyin users (-0.17) and male respondents (-0.43) preferred a finer scale. In comparison, WeChat users (0.20) and respondents with more location data collection knowledge (0.32) voted for a coarser scale. Compared to Northeast China, respondents from all other regions preferred a coarser scale, with participants from East China expressing the strongest preference for the coarsest scale (0.84).

Regarding behaviours (Figure 5.9), most respondents did not use IP location to follow the latest activities of celebrities (B5). Although many participants seemed to care about their IP location accuracy, only a portion of participants tested their assumption that their IP locations were accurately displayed (B6). In terms of the behavioural change after the introduction of the IP location feature (B7), the answers were divided: nearly 60% of respondents agreed or strongly agreed that they stopped using specific social media platforms

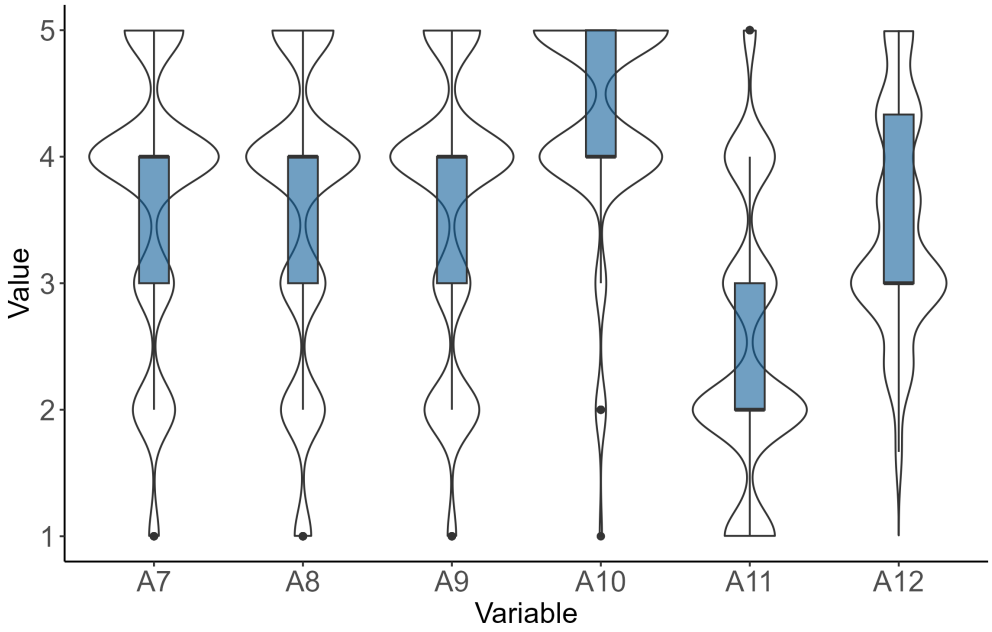

Figure 5.8: Violin Plots of Attitudes Specific to IP Location: scope of the IP location feature (A7), IP location vs. GPS location (A8), the missing function of hiding IP location (A9), cares towards the IP locating process (A10), lack of confidence in IP location accuracy (A11), and geographic scale of IP location (A12).

since April 2022, while the rest disagreed, including a small percent of unsure participants. In Model 20 (Table 5.4), we found that the level of Weibo usage (0.27) and participants' privacy concerns had a positive correlation (0.45 to 0.54 for A1, A3, and A5) with their choice of quitting social media.

5.5 Discussion

The majority of the survey respondents' level of privacy concerns has increased compared to five years ago due to the common experience of privacy breaches and increased awareness of privacy risks. Therefore, there is no better time to discuss location privacy concerns in China. Two themes arise from the survey results, namely *transparency* and *control*. Participants worried about the misuse of personal location information passively collected by social media

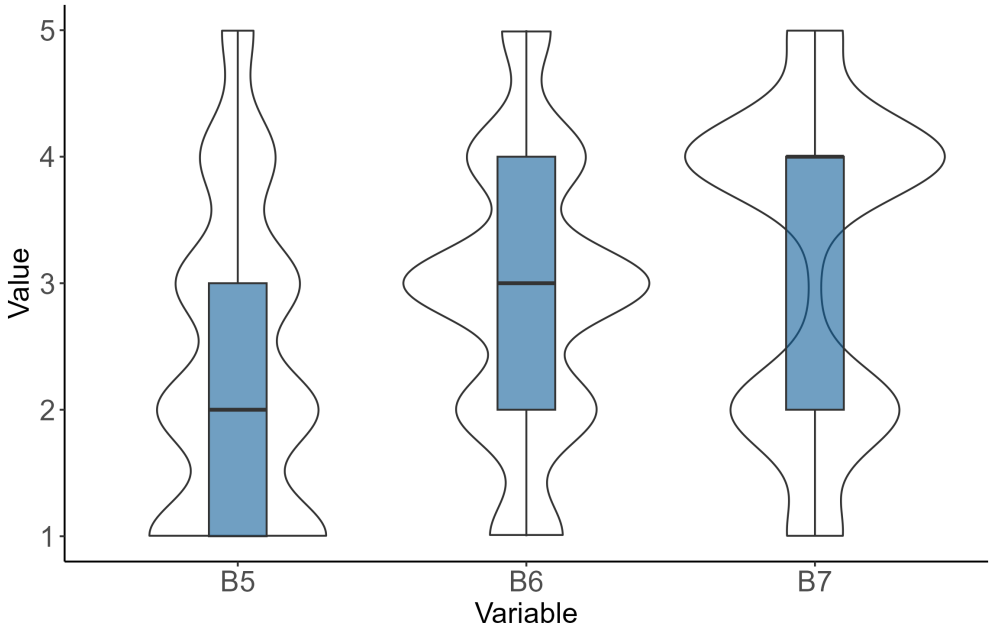

Figure 5.9: Violin Plots of Behaviours Specific to IP Location: using IP location to follow celebrities (B5), testing IP location accuracy (B6), and quitting social media after April 2022 (B7).

platforms and were interested in learning how their IP locations were determined. These results indicate that respondents desire a more transparent process of location data collection and transfer. Additionally, to reduce participants' level of privacy concerns, the authority could limit the scope of when and where IP location is applied or allow social media platforms to offer an option to toggle the feature. These responses suggest that individuals prefer to have more control over how and when their IP locations are shared.

The correlation and regression outputs determine whether the hypotheses are true. Generally, location privacy knowledge positively influences location privacy attitude (H1) and behaviour (H2), with one exception that declarative knowledge was negatively associated with location privacy concerns. This exception may be explained by the increased trust from learning more about PIPL, which in turn lessens the respondents' sensitive nerves about location privacy. Thus, H1 holds if its subject is specified as "procedural privacy knowledge"

(i.e., technical steps of privacy protection). For H2, only one supporting evidence between K3 and B1 was observed (Model 14), so H2 holds, but more evidence is needed to make a stronger argument. A robust positive relationship was observed between privacy attitude and behaviour, with consistent results across all variables. Therefore, H3 is also supported.

The effect of the moderating factors are summarized below. H4 (gender vs. knowledge/attitude/behaviour, or KAB) partially holds as we only found statistically significant evidence to support that males possess higher levels of privacy knowledge and exhibit lower levels of privacy protection behaviours. Both age and gender did not significantly moderate privacy attitudes, suggesting the presence of potential alternative moderators. Although H5 (age vs. KAB) does not hold due to the lack of statistically significant coefficients, we discovered that senior respondents were more knowledgeable about PIPL. H6 (regions of origin vs. KAB) was found to be false, although it is usually assumed that individuals from one country share similar concerns and behaviours due to coherent social norms and cultural identity. Specifically, Northeast China consistently exhibited the lowest level of privacy knowledge and concerns as well as a relatively low level of privacy protection behaviours. This phenomenon is likely related to the geopolitical context of Northeast China, where the three provinces were among the pioneering industrialized regions (Zhang, 2008). Although the era of collectively planned heavy manufacturing has come to an end, people in Northeastern China, especially the older generation, still miss the old days and prefer stable careers supported by the government, partly because there are few better jobs than civil servants in the post-industrial era (Attrill, 2020). This reliance on the central regime may explain their attitude and behaviour towards location privacy. On the contrary, respondents from East China expressed the least agreement with the statement regarding the overconcern of others. They preferred the coarsest geographic scale of IP location, suggesting that this group of respondents believed that people's privacy concerns need to be recognized, shared, and discussed. This liberal mindset of East China is probably linked to its high

level of economic development and openness to Western ideologies. Interestingly, responses from Southwest China had the highest level of location protection knowledge and behaviour, and responses from Northwest China shared the highest level of location privacy concerns. This phenomenon is likely associated with the agglomeration of visible minorities and the politically charged atmosphere in West China.

Privacy paradox was also observed in our analysis. Collectively, although respondents had relatively strong location privacy concerns, they did not exhibit a high level of privacy protection behaviours and still shared their locations frequently. A specific case was Northwest China, where the participants had a relatively high acceptance level of location disclosure compared to their comparatively elevated level of privacy concerns. Even so, a substantial number of respondents chose to discontinue using specific social media platforms, citing privacy concerns and specifically mentioning Weibo. Consequently, online discussions became less vibrant on Chinese social media.

People's privacy concerns were also platform-dependent. Douyin users, for example, demonstrated fewer privacy concerns and more frequent location sharing, while Weibo users chose to act contrarily. WeChat users also expressed extra desire for personal location protection and acted accordingly. The difference between Douyin and WeChat can be explained by their different use cases. While Douyin is primarily a short video platform, WeChat is predominantly a messaging app for maintaining social ties with friends and families (Elegant, 2019). The contrasting level of closeness between contacts, therefore, led to the results above. Weibo is a distinct case among the three. Since the IP location feature was tested and debuted on Weibo, the debate between proponents and opponents was intense and even made the discussion to the top of the trending topic list. Thus, it is understandable that Weibo users also demonstrated additional privacy concerns and protection behaviours.

5.5.1 Limitations

This study is not without limitations. First, backward elimination has been criticized because the stepwise approach may exclude real explanatory variables that are not statistically significant (Smith, 2018). However, this issue is mitigated in our analysis as each category has more than one response variable, so the chance of missing true explanatory variables is reduced. It would also be unpersuasive to reject the null hypotheses if insignificant independent covariates were included in our models. Second, respondents' regions of origin were not equally distributed, with the majority from East China, so the generalizability of our findings was limited to some extent. However, in observational data, achieving an equal geographic distribution is often unfeasible. In cases of rare events where significant concerns may arise, the threshold for defining rare events was set at 1% or less of the sample size (King & Zeng, 2001). In our analysis, the category with the smallest number of respondents (Northwest) accounted for more than 3% of the total sample, suggesting that the issue may be mild. Finally, sampling bias is unavoidable when using any data collection platform. Since our survey was distributed on Credamo, users who did not sign up for Credamo were out of reach.

5.5.2 Future Works

Knowledge and attitude are two factors that can influence people's privacy behaviour. Additional factors could be explored in future studies. For example, intention, which is situated between privacy attitudes and behaviour, was not investigated in this study. A positive relation was usually found between privacy intention and behaviour (e.g., Baruh et al. 2017). The variance in behaviour explained by intentions can be limited (Sheeran, 2002), however, and actual disclosure frequently surpasses intention by a significant margin (Norberg et al., 2007). Future studies can also investigate the effectiveness of raising users' awareness as a

means of influencing their privacy behaviours. In Momen & Piekarska (2017), for instance, the authors designed a mobile application that can display and notify users about the data access permissions and data collection actions of installed applications to verify the efficacy of privacy nudges (Acquisti, 2009). Moreover, experiments can be carried out as surveys can only capture respondents' self-assessments of their behaviours. In the case of this survey, experiments can be difficult and time-consuming to conduct as we are interested in people's behavioural change in the relatively long term.

5.6 Conclusions

The norm of privacy has not been adequately addressed in Chinese society historically, but the development of PIPL served as a wake-up call of better privacy protection. The implementation of the IP location feature countered the latest regulation, which led to heated debate on social media, making this study a timely topic in the field of society and space. Through analyzing the responses of an online survey, this article fills the research gap of location privacy concerns in China. Using ordinal logistic regression, we discovered that privacy knowledge and attitudes positively influenced privacy protection behaviours. Privacy knowledge and attitudes shared the same positive relation except declarative knowledge, which had an opposite effect on privacy concerns. In terms of the moderating factors, male respondents exhibited extra procedural knowledge and less protection behaviours, while senior respondents were more knowledgeable about their privacy rights. The regional difference in location privacy concerns was also notable, with participants from the Northeast at the bottom, while those from the Northwest, Southwest, and East ranked among the top. Although privacy paradox was observed, more than half of the respondents reported decreased social media usage since the introduction of the IP location feature, suggesting the potential influence of behavioural changes resulting from unintended location disclosure. From

our analysis, Chinese citizens care about their location privacy and act following their privacy attitudes. The policymakers should therefore consider the impact of internet policy on individual behaviours.

5.7 References

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, *7*(6), 82–85.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-hall.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B. Johnson, & M. Zanna (Eds.), *The handbook of attitudes* (pp. 173–221). Lawrence Erlbaum Associates Publishers.

Attrill, N. (2020). Northeast China's rust belt politics: A new governing challenge for the party-state in a post-industrial era? *Available at SSRN 3667616*.

Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

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

Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, *15*, 679–694.

Blumer, H. (1986). *Symbolic interactionism: Perspective and method*. University of California Press.

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior*, *101*, 1–13.

Cottrill, C. D., & Thakuriah, P. V. (2015). Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies*, *56*, 132–148.

Crossler, R. E., & Bélanger, F. (2019). Why would i use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research*, *30*(3), 995–1006.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-mediated Communication*, *15*(1), 83–108.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297.

Elegant, N. X. (2019). *For China's social media giants, it's a battle for the ages.* Fortune. Retrieved from `https://fortune.com/2019/10/25/wechat-douyin-tiktok-china/` (Accessed: 2023-08-29)

Fisher, J. D., Fisher, W. A., Williams, S. S., & Malloy, T. E. (1994). Empirical tests of an information-motivation-behavioral skills model of aids-preventive behavior with gay men and heterosexual university students. *Health Psychology*, *13*(3), 238–250.

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, *25*, 1055–1061.

Harsanyi, J. C. (1967). Games with incomplete information played by "bayesian" players, part I. The basic model. *Management Science*, *14*(3), 159–182.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45.

Huang, J., Kwan, M.-P., & Kim, J. (2021). How culture and sociopolitical tensions might influence people's acceptance of COVID-19 control measures that use individual-level geo-referenced data. *ISPRS International Journal of Geo-Information*, *10*(7), 490.

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*(3), 579–595.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.

Kemp, S. (2023). *Digital 2023: China.* Data Reportal. Retrieved from `https://datareportal.com/reports/digital-2023-china` (Accessed: 2023-06-28)

Ketelaar, P. E., & Van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182.

Khalid, H., Shihab, E., Nagappan, M., & Hassan, A. E. (2014). What do mobile app users complain about? *IEEE Software*, *32*(3), 70–77.

Kim, H.-S. (2016). What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior*, *54*, 397–406.

Kim, J., Kwan, M.-P., Levenstein, M. C., & Richardson, D. B. (2021). How do people perceive the disclosure risk of maps? Examining the perceived disclosure risk of maps and its implications for geoprivacy protection. *Cartography and Geographic Information Science*, *48*(1), 2–20.

King, G., & Zeng, L. (2001). Logistic regression in rare events data. *Political Analysis*, *9*(2), 137–163.

Lee, J.-M., & Rha, J.-Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, *63*, 453–462.

Levine, D. S., & Strube, M. J. (2012). Environmental attitudes, knowledge, intentions and behaviors among college students. *The Journal of Social Psychology*, *152*(3), 308–326.

Li, H. (2020). Negotiating privacy and mobile socializing: Chinese university students' concerns and strategies for using geosocial networking applications. *Social Media + Society*, *6*(1), 2056305120913887.

Lin, J., Benisch, M., Sadeh, N., Niu, J., Hong, J., Lu, B., & Guo, S. (2013). A comparative study of location-sharing privacy preferences in the United States and China. *Personal and Ubiquitous Computing*, *17*(4), 697–711.

Liu, P., Teng, M., & Han, C. (2020). How does environmental knowledge translate into pro-environmental behaviors? The mediating role of environmental attitudes and behavioral intentions. *Science of the total environment*, *728*, 138126.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125.

Momen, N., & Piekarska, M. (2017). Towards improving privacy awareness regarding apps' permissions. In *Proceedings of the international conference on digital society (ICDS)* (Vol. 11, pp. 18–23).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management* (Vol. 1, pp. 121–138).

Paço, A., & Lavrador, T. (2017). Environmental knowledge and attitudes and behaviours towards energy consumption. *Journal of Environmental Management*, *197*, 384–392.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236.

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the internet. *Computers in Human Behavior*, *50*, 252–258.

Poikela, M. E. (2020). *Perceived privacy in location-based mobile system*. Springer.

Polonsky, M. J., Vocino, A., Grau, S. L., Garma, R., & Ferdous, A. S. (2012). The impact of general and carbon-related environmental knowledge on attitudes and behaviour of US consumers. *Journal of Marketing Management*, *28*(3-4), 238–263.

Ricker, B., Schuurman, N., & Kessler, F. (2015). Implications of smartphone usage on privacy and spatial cognition: Academic literature and public perceptions. *GeoJournal*, *80*, 637–652.

Seidl, D. E., Jankowski, P., Clarke, K. C., & Nara, A. (2020). Please enter your home location: Geoprivacy attitudes and personal location masking strategies of internet users. *Annals of the American Association of Geographers*, *110*(3), 586–605.

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1–36.

Smith, G. (2018). Step away from stepwise. *Journal of Big Data*, *5*(1), 1–12.

Spearman, C. (1904). The proof and measurement of association between two things. *The American Journal of Psychology*, *15*(1), 72–101.

Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science*, *32*(11), 1492–1512.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*(1), 590–598.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826.

Tobler, W. (1970). A computer movie simulating urban growth in the Detroit region. *Economic geography*, *46*(sup1), 234–240.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. Hert (Eds.), *Reforming european data protection law* (pp. 333–365). Springer.

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society*, *9*(2), 300–318.

World Bank. (2021). *Individuals using the internet (% of population) - China.* The World Bank Group. Retrieved from `https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CN` (Accessed: 2023-06-28)

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? In *Proceedings of the 5th annual ACM web science conference* (pp. 463–472).

Zhang, P. (2008). Revitalizing old industrial base of northeast China: Process, policy and challenge. *Chinese Geographical Science*, *18*, 109–118.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283–289.

Chapter 6

Discussion

Chapter 4 and 5 have examined privacy concerns among Chinese individuals using two datasets, namely social media data and survey results. In this chapter, I endeavour to expand on the discussion points presented in the manuscripts. I first illustrate the evolving landscape of privacy regulations within China. Subsequently, the appropriateness of the IP location feature as an anti-disinformation tool is critically analyzed, particularly when considering privacy implications. Moving forward, I explore potential areas for future research in behavioural geoprivacy. The chapter concludes with a proposal for embracing place-based privacy, drawing a compelling connection to the discussion presented in previous chapters. I contemplate the importance of integrating geographical context into privacy frameworks, recognizing the impact of platial information on individual privacy concerns. By referring to user-tailored privacy and group privacy, I aspire to contribute to a more nuanced and contextually relevant approach toward information privacy protection. Together, the discussion of privacy rights in China and the forward-looking idea of place-based privacy further support the culturally relativistic view toward geoprivacy.

6.1 Privacy Rights within the Chinese Legal Framework

The preceding chapters have emphasized the cultural impacts on individuals' privacy attitudes and behaviours. A country's regulations reflect its culture to some degree. By analyzing the understanding of privacy within the Chinese legal framework, I aim to pro-

vide a refreshed perspective on recent developments in privacy protection within the region, contrasting with the traditional East Asian view towards privacy. I then assess whether the IP location feature adheres to the country's own legal guidelines, which serves as a reminder for lawmakers to consider privacy-related principles in future social media policies.

6.1.1 Privacy as a Personality Right: A Case Study of the Civil Code of the People's Republic of China

While the English literature on Chinese information privacy has focused on the Cyber Security Law and the Personal Information Protection Law (see Chapter 4), the Civil Code of the People's Republic of China (PRC), hereinafter referred to as the Civil Code, has received comparatively less attention from Western scholars. Implemented in January 2021, the Civil Code is essential to help understand public opinions as it is a foundational legal reference. Compared to its predecessor, the General Principles of the Civil Law of the PRC, the Civil Code features a newly dedicated book of personality rights that necessitates thorough discussion.

We list some of the country's unique privacy protection philosophies by drawing interpretations from simplified Chinese literature. Instead of classifying information privacy as a subcategory of privacy, the Civil Code (National People's Congress, 2020) covers the right to privacy and the protection of personal information together in the book of Personality Rights. Since the implementation of the PIPL, the interest in personal information is often compared with the right to privacy because of the overlap between the two, but the interpretations are often split into various directions. For example, Wang (2021) stated that according to the Civil Code, the right to privacy takes precedence over the interest in personal information when both are applicable. However, Cheng (2022) disagreed and claimed that he was unable to conclude that the strength of legal protection of the right to privacy is

greater than the interest in personal information. Zhou (2021) suggested that the two rights should be treated in parallel and different rules should be applied in different contexts. Peng (2023) also acknowledged the difference and implied that the interest in personal information covers further protection of information autonomy and personality interests. In summary, Chinese scholars have yet to have a consensus about the priority of the two. The experts do agree on the following. First, in China, only natural persons[34] have the right to privacy because the core of personality rights is based on personal freedom and dignity (Li, 2022). The privacy of legal persons is called trade secrets instead (Yan & Wang, 1996). Second, the subjective expectation of privacy is limited by its irrelevance to public interest (Peng, 2023). Whether private information is worth receiving legal protection is determined by whether public interest outweighs the right to privacy (Wang, 2022). The desire for public interest is often linked to the tradition of collectiveness (Lü, 2005), which quietly impacts public opinions on government policies.

The debate surrounding personality rights in the Civil Code signifies a notable disagreement even among scholars. In this situation, one might wonder how ordinary citizens can develop a clear comprehension of their privacy rights. In our examination of public opinions regarding the IP location feature on Weibo (see Chapter 4), we observe instances of irrational attacks from some of the proponents of the feature towards the concerned users. This phenomenon prompts a consideration of privacy awareness among these supporters, which remains in question. Consequently, it becomes imperative to make concerted efforts towards disseminating knowledge about privacy laws to a broader Chinese population. Perhaps anonymity is not the sole catalyst, as ignorance also contributes to online disorder.

[34]Real and living human beings

6.1.2 Normative Considerations of the IP Location Feature: Assessing Its Role in Combating Disinformation

Setting aside the coverage of privacy rights in regulatory texts, it is also worth deliberating whether the IP location feature aligns with the legal principles of combating disinformation. Helm & Nasu (2021) published three requirements for regulatory responses to fake news: the principles of *legality*, *necessity*, and *proportionality*. Since the original intention of the IP location feature was anti-disinformation, we use the normative considerations above to guide our discussion.

Indeed, privacy concerns have prompted the Chinese public to question the legality of the IP location feature. A lawsuit was filed after the initial release when the feature only applied to Russia-Ukraine-related content (Legal Search, 2022). The suit claimed that the platform violated the "legitimacy, rightfulness, and necessity" principle of personal information processing because users did not consent to the access and collection of personal location information. The case was officially filed with the Beijing Internet Court in April 2022, and the news article reporting this case was removed from WeChat shortly thereafter. Given this and the Weibo discourse presented in Chapter 4, we identify the Chinese population who value their personal information. In this case, the Civil Code and the PIPL failed to protect users' location information. With the Cyberspace Administration of China (CAC) regulation[35] that came into effect in August 2022, mandating service providers to disclose users' IP locations, the rule has effectively eliminated any potential for legal debate of "consent and choice". Even without the CAC mandate, some scholars argued that "public interest" can be an exception of personal information handling without consent (Sun et al., 2022).

Supporters and regulators of the feature frequently mentioned the need for anti-disinformation services. The effectiveness of the measure remains to be assessed, however. The novelty of

[35]See Cyberspace Administration of China (2022).

this regulatory response also makes the evaluation of effectiveness more complex, as comparable examples in other countries are not available. As mentioned by opponents, locations can be modified by IP proxy services, so the mandatory disclosure only addresses a minority of disinformation issues. While initially, some supporters observed a more civil online environment with less disinformation, the effectiveness of the chilling effect would decrease as a greater number of users become familiar with the technical countermeasures. In addition, the participation rate in online discussions could diminish because not all users are inclined to alter their IP addresses at every occasion. Considering that anonymity may not contribute to incivility and low quality of online discussion (Jaidka et al., 2022), IP location may be a superfluous feature that purely impacts user experience. Given that the draft CAC regulation was published in October 2021 and the initial testing on Weibo occurred five months later (Sun et al., 2022), it is also reasonable to speculate that the feature was never intended to solely apply to Russia-Ukraine-related content in the first place. The initially limited scope of the regulation (e.g., applicable to sensitive topics only) allowed for the expansion of this feature from a public interest perspective. In its current form, the all-inclusive nature of the regulation acts as a barrier to disinformation circulation that can be easily bypassed and reduces the overall vibrancy of discussion on Chinese social media.

Proportionality often requires "national authorities to choose the least intrusive measure of interference" (Helm & Nasu, 2021). The granularity of the exposed locations and scope of the regulations thus became the centre of the controversy. Opponents suggested that a simple differentiation between mainland China and overseas users could ease the concern of "foreign forces", while the CAC rule implies that rumour mongers within China are also of concern. The problem with reporting locations at the provincial level is that although individual identification using provinces remains challenging, the additional information increases the risk of privacy violation and regional stereotyping. Furthermore, whether users' current provinces count as private information should be determined by the users themselves.

As people's location privacy concerns are cognate-based and context-dependent (Zhang & McKenzie, 2023), the involuntary disclosure undoubtedly impacts many users' continued engagement on social media. A digital divide between local and foreign users may be a more proportional approach for anti-disinformation as it would have minimal impact on the majority of users. Nevertheless, it may result in other significant issues (e.g., xenophobia). If we consider the cost-benefit analysis above, the measure raises too many barriers while having limited influence on real news dissemination. Anonymity is arguably the foundation of social media communication, and the boundary between our virtual and physical environments must be respected. Users log in to online platforms to experience and express things they feel uncomfortable sharing in the physical world. This tighter integration with the real world brings issues of social class to online environments that were previously free from such constraints. The additional location information does little for user retention but clogs an already crowded user interface. As one Weibo user pointed out, they have no interest in seeing others' private information that was forcefully displayed on their screen.

6.2 Limitations and Implications of Research

The studies of privacy attitudes in this dissertation has its limitations. The focus of the studies is on Chinese social media users, which means there is an issue of the digital divide where certain regions or demographics have unequal access to modern information technology. Critics may argue that the group of Chinese who do not or seldomly use the internet has been ignored in the attitude analysis. However, the motivation of this research is based on ubiquitous computing and new forms of location sharing in the information age. This shift from physical to digital privacy is driven by the new formats of location data on social media, which make geographers contemplate new threats and risks towards geoprivacy in the online environment. Thus, given the aim and scope of the dissertation, the targeted research

population remains representative.

More specific limitations are chapter-dependent. For instance, Chapter 4 only collects user opinions from one platform, Weibo, which has its own user base. Although privacy-related expressions on other social media platforms need to be further explored, Weibo is still the epicentre of the discussion given its microblog format and its history of original testing of the IP location feature. In Chapter 5, the research model does not consider socioeconomic classes as one of the moderating factors of privacy attitudes and behaviours. Since not everyone has the technical knowledge to use or financial stability to afford IP proxy services, it is valid to assume the potential impact on user opinions from hierarchical social categories. Whether a higher class has higher or lower privacy concerns remains a question because of limited existing research.

The implications of the research can be summarized in multiple aspects. The studies recognize the group of Chinese users who are indifferent to location data disclosure. However, the uniform policy ignores the concerns from privacy actives. Given that social media has seamlessly integrated into individuals' everyday life, the IP location feature coerces behavioural changes in a selected number of users and forces them to adopt new digital routines. The impact on users' free expression of their spatial selves may have a deep influence on society – the recent "run movement," in which people are looking to flee China, is an illustration (Ni, 2022).

Another notable discovery is that respondents who were more knowledgeable about national privacy regulations indicated fewer privacy concerns, suggesting that Chinese citizens believe in a law-based society. However, does the law protect its people, especially vulnerable groups such as females who voiced their concerns about potential harassment caused by unwanted location disclosure? Based on the legal analysis in Section 6.1, it seems that the detailed rules contradict the higher law. If this is the case, what legal actions could citizens take to protect their right to privacy? According to legal expert Ping Jiang, the current

legislation on the protection of civil and political rights is far from perfect in China. One instance is that the concept of the rule of law in China has always emphasized the predominance of public power, with private rights often marginalized (Jiang, 2013). While public power plays a crucial role in building a law-based society, the imbalanced power dynamics make the road to justice long and difficult. From the Weibo discourse, we learned that the public wants consultation before implementing the IP location feature so that its effectiveness in combating disinformation and its associated negative consequences can be closely scrutinized. The different treatment of official and VIP accounts also makes users question whether average citizens' right to privacy is protected appropriately. There is no doubt that more users would support its implementation if the IP location feature is not universally applied but only to social media posts of specific events (e.g., the Russian-Ukraine crisis). Other adjustments, such as a toggle or a more coarse geographic scale, can also be made to ensure the feature more proportional to its original goal.

6.3 Advancing the Field of Behavioural Geoprivacy: A Forward Perspective[36]

6.3.1 Opportunities in Modern Privacy Research

The extent of information that social media platforms possess about us can be pretty overwhelming based on our previous discussion. Given the inevitable convergence of the physical and virtual worlds, how can we effectively safeguard our privacy? While the privacy risks are ubiquitous, there have been significant enhancements in privacy-preserving technologies in recent years. One issue is that general security and privacy-preservation techniques such

[36]A version of this section appears in Zhang, H., & McKenzie, G. (2022). Towards place-based privacy: Challenges and opportunities in the "smart" world. In *Proceedings of the 2022 IEEE International Symposium on Technology and Society (ISTAS)*.

as encryption (e.g., HTTPS), access control (e.g., two-factor authentication), and relay (e.g., Tor network) (Seamons, 2022) may not all be applicable in the "smart" world that is omni-connected and constantly computed. Other technical solutions to privacy also have their limitations (Knijnenburg et al., 2022). In this section, we introduce two emerging areas in privacy research, namely user-tailored privacy and group privacy.

User-tailored privacy (UTP) is a forward-looking research area that aims to customize information privacy settings based on users' preferences and simplify the decision-making process of information disclosure using machine learning algorithms. Kobsa (2001) first introduced the concept of UTP. The idea is different from personalized privacy (Xiao & Tao, 2006), in which the model adjusts the degree of anonymity. Knijnenburg et al. (2022) further researched this topic and proposed the "measure, model, adapt" framework for UTP: first measuring the user by contextual and personal variables, then modelling privacy to determine the targets of privacy preservation, and finally adapting the system to achieve privacy-aware personalization. Essentially, UTP acts as a recommender system for privacy protection. It is a design philosophy that can not only recommend privacy settings but also websites, applications, and information disclosure options in social networks. Starting from a simple profile, UTP increases the number of automated recommendations, especially on frequently used features, as the collection of user preferences progresses. The process balances the trade-off between privacy and other design goals through an automated approach, which reduces users' decision burden and can take advantage of the data deluge in our smart world.

The smart world and its ubiquitous data collection also pose privacy threats to groups and collectives, in addition to individuals (Suh & Metzger, 2022). Whether it is group profiling (e.g., racial profiling), COVID-19 contact tracing (e.g., regional discrimination based on people's travel history), or fitness tracking (e.g., disclosure of secret military operations based on aggregated Strava data (Hern, 2018)), more and more examples highlight the need for protecting privacy at a collective level. Groups, in this case, can be self-constituted

or algorithmically determined (Suh & Metzger, 2022). In the latter category, individuals are unaware of their belonging to specific groups. Privacy in this definition is also twofold, including "their" privacy (i.e., the "privacies" of individual group members) and "its" privacy (i.e., the privacy of the entire group) (Suh & Metzger, 2022). Multiple challenges remain to be addressed to preserve group privacy better. First, collaborative group privacy strategies face hindrances during the execution process because of the communication cost in multi-stakeholder decision-making environments (Jia & Xu, 2016). Second, conflicts can happen when individual and group privacy rights contradict and coordination fails within groups. Finally, it is still being determined how to properly manage the privacy of individuals who are unconscious of their group membership (Loi & Christen, 2020). This challenge will be a significant concern as the number of algorithmically determined groups boom on the internet.

In the context of the IP location feature, both design principles could potentially contribute to mitigating concerns related to *proportionality*. Take UTP as an example, which could be implemented to suggest the appropriate geographical granularity for disclosing IP locations on social media. This recommendation could be inferred from factors such as users' privacy preferences, the content of their posts, and the spatial-temporal metadata associated with those posts. Instead of requiring users to make decisions on a case-by-case basis, users could adjust global settings as necessary, allowing the algorithm to make optimal choices to uphold privacy goals. Moreover, group privacy could be conceptualized as a risk detection system. In instances where platforms identify hate speech targeted at users from specific regions, the system could automatically conceal these users' IP locations to prevent further harm. IP locations would only be visible when the privacy risks for these groups are minimal. By combining these two design philosophies, a balance between the objectives of privacy protection and anti-disinformation can be achieved to a considerable extent.

6.3.2 Towards Place-Based Privacy

Both UTP and group privacy are valuable approaches in modern privacy research. In this section, we propose the umbrella term *place-based privacy* to combine the key notions of the two solutions from a platial perspective. Traditionally, computationally-focused researchers have recognized the field of location privacy (Beresford & Stajano, 2003), and through the continued practice of "Geo$X$" (geo-labeling of scientific subjects), the field of geoprivacy emerged (Weiser & Scheider, 2014). While the concept is well understood, location privacy appears to be data-centric, and geoprivacy is not widely referenced by scholars outside of geography and spatial data science. Place-based privacy interprets this topic from another angle. Compared to geographic coordinates, the concept of place has built-in ambiguity and emotional attachments (Gao et al., 2013). Place and privacy can, therefore, be linked together when thinking from a cognate-based viewpoint (Zhang & McKenzie, 2023) (i.e., in terms of privacy, "it is the belief that I am being watched that's my grievance" (Wacks, 2015)). McKenzie et al. (2016) acknowledged the idea of place-based privacy in their semantic analysis of geosocial check-ins and recognized the importance of platial information in geoprivacy research.

Here, we extend the discussion by treating platial information as contextual factors, which expands the term to include a broader scope than masking locations alone. Building on previous work (Zhang & McKenzie, 2023), place-based privacy concerns are *culturally situated*, *location-dependent*, *time-variant*, and *people-centred* (Figure 6.1). Its key characteristics differentiate the concept from contextual privacy (Nissenbaum, 2011), in which the context can go beyond the specified constraints and be more difficult to model. We propose place-based groups, either as physical places or as cyberplaces (Wellman, 2001), in addition to self-constituted and algorithmically determined groups (see Section 6.3.1). When places are broader regions or online communities, privacy concerns differ substantially based on

cultural backgrounds (Petronio, 2002) such as religions, histories, and sense of belonging. When places suggest points, privacy concerns are also location-dependent (McKenzie et al., 2016). A higher degree of concern may arise at hospitals or intimate sections in online marketplaces. Depending on the time of the day, individuals or groups perform a range of activities from one place to another as physical persons or avatars. Information disclosure decisions are therefore time-variant: for social networking services, different sharing preferences have been observed between working hours, mealtime, and personal time (Lin et al., 2013). Finally, place-based privacy is people-centred. Places do not exist without human activities or imaginations (Zhang & McKenzie, 2023), and privacy is not a concern without human perceptions. Collectively, the human-centric notion becomes people-centred, which makes personalized privacy protection essential in both the physical and the virtual space.

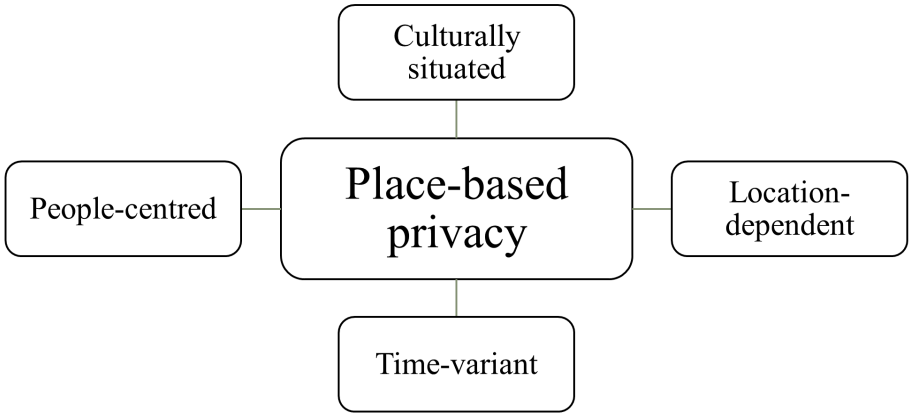

Figure 6.1: Key Characteristics of Place-Based Privacy

In conclusion, place-based privacy, as a subfield of humanistic geography (Tuan, 1976), contributes to human behavioural modelling from perceptual analysis. Additional critics and reflections on the people-place relationship are essential to better predict people's privacy behaviours (Zhang, 2023).

Chapter 7

Conclusions

Returning to the inception, this dissertation has demonstrated the multifaceted nature of privacy. This is precisely why, in Chapter 3, I began with a philosophical exploration of this concept. While computational endeavours in privacy preservation hold significance, grasping users' desires for anonymity and data control is pivotal in refining computer systems that handle the collection, possession, processing, and sharing of personal information. Recognizing the inherent human dimension in these inquiries, I acknowledge that numbers alone do not provide a full picture of privacy expectations. Hence, in Chapter 4, I employed mixed methods to comprehend public attitudes, harnessing the strengths of both quantitative and qualitative research approaches. While social media is a rich data source, I understand the necessity of primary data in privacy modelling, leading me to conduct an online survey in Chapter 5. The examination of the interplay between knowledge, attitude, and behaviour revealed fresh insights from the global south and reaffirmed the existence of the relationship among the triad. To sum up, each chapter in this dissertation is motivated by the outcomes of the preceding study. As a whole, these chapters weave a cohesive narrative, providing a diverse interpretation of this critical intersection of privacy and geography.

As expounded in this dissertation, geoprivacy represents a unique case of privacy perception, incorporating spatial-temporal factors that render this contextual information particularly challenging to model. A pivotal revelation from our studies is the existence of spatial variations in geoprivacy attitudes. While Chapter 3 underscored the impact of culture, Chapter 5 discovered geographical disparities, even within the same cultural context, which

effectively dismantles the information cocoon. When we critique privacy infringements occurring on the other side of the world, we must be cognizant that the threshold for accepting personal information usage can significantly differ within and between the region(s) of the event. As a result, it is important to respect individual differences in privacy concerns.

For future research, as previously highlighted in Chapter 6, platial information holds immense potential for modelling user-tailored privacy recommendations. Geoprivacy, therefore, should not be limited to the privacy of geodata; spatial-temporal information serves as the foundational infrastructure that addresses the broader challenges in digital privacy. The discourse on geoprivacy extends beyond the discipline of geography and applies to a wider spectrum of social science literature. Furthermore, as Chapter 4 and 5 demonstrate, female users exhibited comparatively lower privacy knowledge and a greater level of privacy concerns because of their higher frequency of location sharing on social media and worries about potential physical harassment. Consequently, researchers should continue promoting feminist geoprivacy (Linabary & Corple, 2019), enhancing privacy literacy among females, and effectively addressing their evident privacy concerns.

In conclusion, this dissertation regards geoprivacy as a social form and advocates for a culturally relativistic view on this subject. Understanding geoprivacy facilitates responsible location data sharing and contributes collective social values to the community. This approach explains the resistance encountered after the implementation of the IP location feature in China, as the involuntary disclosure of personal locations, even at a provincial level, disrupts the established norms of social media interaction and diminishes online vitality as a consequence (Foucault, 1977). There is a need to rehumanize geoprivacy and supply due consideration to public opinions. Embracing alternative interpretations of geoprivacy not only renders culturally marginalized groups visible within the discourse of digital justice but also deciphers the ostensibly irrational privacy paradox, where desires in computer-mediated environments supersede pragmatism (Arora, 2019).

Epilogue

Five years ago, I could never have imagined composing a doctoral dissertation centred on geoprivacy attitudes and behaviours. When I applied for doctoral programs, I was certain I wanted to continue my work in geographic information science. My prior research focused on the assessment of data quality in OpenStreetMap, which is an area that is more readily associated with geography than privacy. Even within the community of spatial data scientists specializing in geoprivacy, my work leans less toward the computational aspects prevalent in studies of anonymity, cryptography, and differential privacy. However, the ubiquitous datafication of our society often leads us astray, causing us to lose sight of our original motivations. When the primary objective is to develop state-of-the-art algorithms aimed at refining accuracy scores to the n^{th} decimal place, we must question the actual value of these contributions to the scientific community. Given that improved results can be achieved through hyperparameter optimization in machine learning, this concern assumes particular significance. When one contemplates famine, conflict, climate crisis, infectious diseases, and income instability afflicting populations on the opposite side of the globe, these issues undoubtedly take precedence, demanding immediate attention. Privacy, in this regard, could be seen as a concern distressing the privileged, first-world population. Therefore, we must take a step back, critically reflecting on the reasons behind our intentions to work on geoprivacy preservation techniques. This dissertation serves as a reminder of why we want to protect our geoprivacy and prompts us to question whose geoprivacy we are preserving. Throughout its completion, I often grappled with self-doubt, acutely aware that the focal points of my

inquiry diverged substantially from the quantitative literature. I consider myself fortunate to have encountered Yi-Fu Tuan's work, in which his human-centred approach fortifies my resolve to persist in this direction. Furthermore, I am indebted to my conversation with Dan Montello at the American Association of Geographers Annual Meeting in Denver, who affirmed that the mixed-method approach I employed was well-suited for behavioural research, an assurance particularly encouraging in light of the predominantly unidimensional studies I surveyed. I would also like to express my gratitude to my supervisor, Grant McKenzie, for recognizing my contributions to social theory development. This inspired me to integrate the chapters into a cohesive dissertation in its current form. Finally, I would like to applaud the inclusiveness of geography, which afforded me the latitude to draw on works beyond the confines of my field, including media studies, sociology, legal studies, philosophy, computer science, and environmental psychology. Acquiring the interdisciplinary knowledge presented in this dissertation is similar to taking a self-directed course in liberal arts that was absent from my technical undergraduate education. All in all, thank you, geography, for allowing me to become who I wanted to be.

Consolidated References

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, *7*(6), 82–85.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274.

Adams, A., & Sasse, M. A. (1999). Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie? In *Interact* (pp. 214–221).

Adams, B., & Janowicz, K. (2012). On the geo-indicativeness of non-georeferenced text. In *Proceedings of the international AAAI conference on web and social media* (Vol. 6).

Agnew, J. A. (2014). *Place and politics: The geographical mediation of state and society*. Routledge.

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

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-hall.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B. Johnson, & M. Zanna (Eds.), *The handbook of attitudes* (pp. 173–221). Lawrence Erlbaum Associates Publishers.

Alemanno, A. (2018). How to counter fake news? A taxonomy of anti-fake news approaches. *European Journal of Risk Regulation*, *9*(1), 1–5.

Alrayes, F., & Abdelmoty, A. (2014). No place to hide: A study of privacy concerns due to location sharing on geo-social networks. *International Journal on Advances in Security*, *7*(3/4), 62–75.

Alrayes, F., Abdelmoty, A., El-Geresy, W., & Theodorakopoulos, G. (2020). Modelling perceived risks to personal privacy from location disclosure on online social networks. *International Journal of Geographical Information Science*, *34*(1), 150–176.

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

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Amini, S., Lindqvist, J., Hong, J., Lin, J., Toch, E., & Sadeh, N. (2011). Caché: caching location-enhanced content to improve user privacy. In *Proceedings of the 9th international conference on mobile systems, applications, and services* (pp. 197–210).

An, L., Yu, C., Lin, X., Du, T., Zhou, L., & Li, G. (2018). Topical evolution patterns and temporal trends of microblogs on public health emergencies: An exploratory study of Ebola on Twitter and Weibo. *Online Information Review*, *42*(6), 821–846.

Anderson, B. (2008). For space (2005): Doreen massey. *Key texts in human geography*, 227–235.

Anstead, N., & O'Loughlin, B. (2015). Social media analysis and public opinion: The 2010 UK general election. *Journal of Computer-Mediated Communication*, *20*(2), 204–220.

Aristotle. (1999). *Politics* (B. Jowett, Trans.). Batoche Books. `https://historyofeconomicthought.mcmaster.ca/aristotle/Politics.pdf`.

Arora, P. (2019a). Decolonizing privacy studies. *Television & New Media*, *20*(4), 366–378.

Arora, P. (2019b). *The next billion users: Digital life beyond the west*. Harvard University Press.

Arora, P., & Scheiber, L. (2017). Slumdog romance: Facebook love and digital privacy at the margins. *Media, Culture & Society*, *39*(3), 408–422.

Asai, A., & Barnlund, D. C. (1998). Boundaries of the unconscious, private, and public self in Japanese and Americans: A cross-cultural comparison. *International Journal of Intercultural Relations*, *22*(4), 431–452.

Attrill, N. (2020). Northeast China's rust belt politics: A new governing challenge for the party-state in a post-industrial era? *Available at SSRN 3667616*.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Pew Research Center. Retrieved from `https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf` (Accessed: 2023-07-08)

Bamman, D., O'Connor, B., & Smith, N. (2012). Censorship and deletion practices in Chinese social media. *First Monday*, *17*(3).

Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. In *Proceedings of the international conference on information systems (ICIS 2008).*

Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

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

Bellatti, J., Brunner, A., Lewis, J., Annadata, P., Eltarjaman, W., Dewri, R., & Thurimella, R. (2017). Driving habits data: Location privacy implications and solutions. *IEEE Security & Privacy*, *15*(1), 12–20.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, *15*, 679–694.

Bentham, J. (1791). *Panopticon; or, the inception-house*. Thomas Byrne.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, *2*(1), 46–55.

Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., Gazaki, M., & Hubaux, J.-P. (2016). A machine-learning based approach to privacy-aware information-sharing in mobile social networks. *Pervasive and Mobile Computing*, *25*, 125–142.

Blaschke, T., Merschdorf, H., Cabrera-Barona, P., Gao, S., Papadakis, E., & Kovacs-Györi, A. (2018). Place versus space: from points, lines and polygons in gis to place-based representations reflecting language and culture. *ISPRS International Journal of Geo-Information*, *7*(11), 452.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *Journal of Machine Learning Research*, *3*, 993–1022.

Blumer, H. (1986). *Symbolic interactionism: Perspective and method*. University of California Press.

Bochner, S., & Hesketh, B. (1994). Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. *Journal of Cross-Cultural Psychology*, *25*(2), 233–257.

Bowyer, K. W. (2004). Face recognition technology: Security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. *Pew Internet & American Life Project*, *4*, 1–19.

Bracy, J. (2021). *China adopts national privacy law.* IAPP. Retrieved from `https://iapp.org/news/a/china-adopts-national-privacy-law/`

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest*. MIT Press.

Canares, M. (2018). *Online privacy: will they care? Teenagers use of social media and their understanding of privacy issues in developing countries.* World Wide Web Foundation. Retrieved from `http://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf`

Cao, J. (2005). Protecting the right to privacy in China. *Victoria University of Wellington Law Review*, *36*, 645–664.

Capurro, R. (2005). Privacy. An intercultural perspective. *Ethics and Information Technology*, *7*(1), 37–47.

Casey, E. S. (1993). *Getting back into place: Toward a renewed understanding of the place-world*. Indiana University Press.

Castree, N. (2003). Place: connections and boundaries in an interdependent world. In N. Clifford, S. Holloway, S. Rice, & G. Valentine (Eds.), *Key concepts in geography* (pp. 165–186). Sage London.

Caverlee, J., & Webb, S. (2008). A large-scale study of myspace: observations and implications for online social networks. In *Proceedings of the international AAAI conference on web and social media* (Vol. 2, pp. 36–44).

Chakravartty, P., Kuo, R., Grubbs, V., & McIlwain, C. (2018). #CommunicationSoWhite. *Journal of Communication*, *68*(2), 254–266.

Chang, C.-W., & Chen, G. M. (2014). College students' disclosure of location-related information on Facebook. *Computers in Human Behavior*, *35*, 33–38.

Chang, X. (2013). China's Weibo: Political and social implications? *Education About Asia*, *18*(2), 16–20.

Chapman, A., Hadfield, M., & Chapman, C. (2015). Qualitative research in healthcare: An introduction to grounded theory using thematic analysis. *Journal of the Royal College of Physicians of Edinburgh*, *45*(3), 201–205.

Chen, B. (2011). *Why and how apple is collecting your iphone location data.* Wired. Retrieved from `https://www.wired.com/2011/04/apple-iphone-tracking/`

Chen, B., Wang, X., Zhang, W., Chen, T., Sun, C., Wang, Z., & Wang, F.-Y. (2022). Public opinion dynamics in cyberspace on Russia-Ukraine war: A case analysis with chinese weibo. *IEEE Transactions on Computational Social Systems*, *9*(3), 948–958.

Chen, G.-M. (1995). Differences in self-disclosure patterns among Americans versus Chinese: A comparative study. *Journal of Cross-Cultural Psychology*, *26*(1), 84–91.

Cheng, X. (2022). On the relationship between personal information rights and privacy rights. *Contemporary Law Review*, *2022*(4), 59–71.

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

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior*, *101*, 1–13.

Chor, B., Goldreich, O., Kushilevitz, E., & Sudan, M. (1995). Private information retrieval. In *Proceedings of IEEE 36th annual foundations of computer science* (pp. 41–50).

Chow, C.-Y., Mokbel, M. F., & Liu, X. (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica*, *15*(2), 351–380.

Cisco. (2022). *Cisco 2022 consumer privacy survey.* Cisco. Retrieved from `https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf` (Accessed: 2023-07-08)

Citron, D. K., & Henry, L. M. (2010). Visionary pragmatism and the value of privacy in the twenty-first century. *Michigan Law Review*, *108*(6), 1107–1126.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Clarke, R. (1994). Dataveillance by governments: The technique of computer matching. *Information Technology & People*, *7*(2), 46–85.

Clarke, R., & Wigan, M. (2011). You are where you've been: The privacy implications of location and tracking technologies. *Journal of Location Based Services*, *5*(3-4), 138–155.

Cloke, P., Crang, P., & Goodwin, M. (2013). *Introducing human geographies*. Routledge.

Cohen, J. E. (1999). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, *52*(5), 1373–1438.

Cohen, J. E. (2012). What privacy is for. *Harvard Law Review*, *126*(7), 1904–1933.

Coke, E. (1979). *The first part of the institutes of the laws of england. 1628*. Reprint.

Coke, S. E. (1604). *Selected writings of Sir Edward Coke, vol. I.* Liberty Fund. `https://oll.libertyfund.org/title/shepherd-selected-writings-of-sir-edward-coke-vol-i`.

Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): A review of the use, definition and measurement of IPA. In *Proceedings of the 50th Hawaii international conference on system sciences* (pp. 4021–4030).

Cosgrove, E. (2019). *One billion surveillance cameras will be watching around the world in 2021, a new study says.* CNBC. Retrieved from `https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html` (Accessed: 2023-03-06)

Cottrill, C. D., & Thakuriah, P. V. (2015). Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies*, *56*, 132–148.

Cramer, R., Damgård, I. B., et al. (2015). *Secure multiparty computation and secret sharing*. Cambridge University Press.

Crampton, J. W. (2003). Cartographic rationality and the politics of geosurveillance and security. *Cartography and Geographic Information Science*, *30*(2), 135–148.

Crampton, J. W. (2015). Collect it all: National security, big data and governance. *GeoJournal*, *80*(4), 519–531.

Crawford, K. (2014). *The anxieties of big data.* The New Inquiry. Retrieved from `https://thenewinquiry.com/the-anxieties-of-big-data/`

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, *55*(93).

Creemers, R., Shi, M., Dudley, L., & Graham, W. (2020). *China's draft 'personal information protection law' (full translation).* New America. Retrieved from `https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/` (Accessed: 2023-07-22)

Cresswell, T. (2009). Place. *International encyclopedia of human geography*, *8*, 169–177.

Crossler, R. E., & Bélanger, F. (2019). Why would i use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research*, *30*(3), 995–1006.

Cui, S., & Qi, P. (2021). The legal construction of personal information protection and privacy under the Chinese civil code. *Computer Law & Security Review*, *41*, 105560.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342.

Cvrcek, D., Kumpost, M., Matyas, V., & Danezis, G. (2006). A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on privacy in electronic society* (pp. 109–118).

Cyberspace Administration of China. (2022). *Internet user account information management regulations.* China Cyber Information. Retrieved from `http://www.cac.gov.cn/2022-06/26/c_1657868775042841.htm` (Accessed: 2023-04-12)

Dalkir, K. (2017). *Knowledge management in theory and practice.* MIT Press.

Danezis, G., Lewis, S., & Anderson, R. J. (2005). How much is location privacy worth? In *Workshop on the economics of information security (WEIS)* (Vol. 5).

Davies, S. G. (1997). Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity. In P. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 143–166). MIT Press.

Dearman, D., Hawkey, K., & Inkpen, K. M. (2005). Rendezvousing with location-aware devices: Enhancing social coordination. *Interacting with Computers*, *17*(5), 542–566.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-mediated Communication*, *15*(1), 83–108.

DeCew, J. W. (1997). Privacy and information technology. *Center for the Study of Ethics in Society*, *10*(2), 1–50. `https://scholarworks.wmich.edu/ethics_papers/40/`.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management*, *14*(4), 57–93.

Dobson, J. E., & Fisher, P. F. (2003). Geoslavery. *IEEE Technology and Society Magazine*, *22*(1), 47–52.

Dobson, J. E., & Fisher, P. F. (2007). The panopticon's changing geography. *Geographical Review*, *97*(3), 307–323.

Dong, X., & Lian, Y. (2021). A review of social media-based public opinion analyses: Challenges and recommendations. *Technology in Society*, *67*, 101724.

Dourish, P., & Mainwaring, S. D. (2012). Ubicomp's colonial impulse. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 133–142).

Downs, R. M. (1981). Maps and metaphors. *The Professional Geographer*, *33*(3), 287–293.

Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. In R. Billen, E. Joao, & D. Forrest (Eds.), *Dynamic & mobile GIS: Investigating change in space and time* (pp. 35–52). CRC Press.

Durkheim, E. (1893). The division of labour in society (G. Simpson, Trans.). In F. Dobbin (Ed.), *The new economic sociology: A reader.* Princeton University Press.

Dwork, C. (2011). Differential privacy. *Encyclopedia of Cryptography and Security*, 338–340.

Egan, M. (2022). Privacy boundaries in digital space: An exercise in responsibilisation. *Information & Communications Technology Law*, *31*(3), 301–318.

Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda. *Annals of the International Communication Association*, *43*(2), 97–116.

Ekenga, C. C., McElwain, C.-A., & Sprague, N. (2018). Examining public perceptions about lead in school drinking water: A mixed-methods analysis of Twitter response to an environmental health hazard. *International Journal of Environmental Research and Public Health*, *15*(1), 162.

Elegant, N. X. (2019). *For China's social media giants, it's a battle for the ages.* Fortune. Retrieved from `https://fortune.com/2019/10/25/wechat-douyin-tiktok-china/` (Accessed: 2023-08-29)

El Emam, K., Buckeridge, D., Tamblyn, R., Neisa, A., Jonker, E., & Verma, A. (2011). The re-identification risk of Canadians from longitudinal demographics. *BMC Medical Informatics and Decision Making*, *11*(1), 1–12.

Elwood, S., & Leszczynski, A. (2011). Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum*, *42*(1), 6–15.

European Commission. (2023). *The digital services act package.* Shaping Europe's Digital Future. Retrieved from `https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package` (Accessed: 2023-07-22)

Europol & Eurojust. (2018). *Common challenges in combating cybercrime.* Europol and Eurojust Public Information. Retrieved from `https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf` (Accessed: 2023-03-15)

Evans, L. (2011). Location-based services: Transformation of the experience of space. *Journal of Location Based Services*, *5*(3-4), 242–260.

Fabrigar, L. R., Petty, R. E., Smith, S. M., & Crites Jr, S. L. (2006). Understanding knowledge effects on attitude-behavior consistency: The role of relevance, complexity, and amount of knowledge. *Journal of Personality and Social Psychology*, *90*(4), 556–577.

Fisher, J. D., Fisher, W. A., Williams, S. S., & Malloy, T. E. (1994). Empirical tests of an information-motivation-behavioral skills model of aids-preventive behavior with gay men and heterosexual university students. *Health Psychology*, *13*(3), 238–250.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage.

Fraser, A. (2019). Land grab/data grab: Precision agriculture and its new horizons. *The Journal of Peasant Studies*, *46*(5), 893–912.

Friedman, B., Lin, P., & Miller, J. K. (2005). Informed consent by design. *Security and Usability*, 503–530.

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, *25*, 1055–1061.

Gao, H., Tang, J., & Liu, H. (2012). gSCorr: Modeling geo-social correlations for new check-ins on location-based social networks. In *Proceedings of the 21st ACM international conference on information and knowledge management* (pp. 1582–1586).

Gao, S., Janowicz, K., McKenzie, G., & Li, L. (2013). Towards platial joins and buffers in place-based GIS. In *ACM SIGSPATIAL COMP'13.*

Gavison, R. (1992). Feminism and the public/private distinction. *Stanford Law Review*, *45*(1), 1–46.

Georgiou, M. (2006). *Architectural privacy: A topological approach to relational design problems* (Unpublished doctoral dissertation). University College London.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy.* University of Chicago Press.

Gold, J. R. (1980). *An introduction to behavioural geography.* Oxford University Press.

Golledge, R. G., & Stimson, R. J. (1997). *Spatial behavior: A geographic perspective.* Guilford Press.

Goodchild, M. F. (2011). Formalizing place in geographic information systems. In L. Burton, S. Matthews, M. Leung, S. Kemp, & D. Takeuchi (Eds.), *Communities, neighborhoods, and health* (pp. 21–33). Springer.

Grossklags, J., & Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *Workshop on the economics of information security (WEIS).*

Gu, Y., Yao, Y., Liu, W., & Song, J. (2016). We know where you are: Home location identification in location-based social networks. In *2016 25th international conference on computer communication and networks (ICCCN)* (pp. 1–9).

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied thematic analysis.* Sage.

Gupta, S., Xu, H., & Zhang, X. (2011). Balancing privacy concerns in the adoption of location-based services: an empirical analysis. *International Journal of Electronic Business*, *9*(1-2), 118–137.

Haerpfer, C., et al. (Eds.). (2022). *World values survey: Round seven - country-pooled datafile version 5.0.* JD Systems Institute & WVSA Secretariat. Retrieved from `https://doi.org/10.14281/18241.20` (Accessed: 2023-07-08)

Hamzei, E., Winter, S., & Tomko, M. (2020). Place facets: A systematic literature review. *Spatial Cognition & Computation*, *20*(1), 33–81.

Han, X., Wang, J., Zhang, M., & Wang, X. (2020). Using social media to mine and analyze public opinion related to COVID-19 in China. *International Journal of Environmental Research and Public Health*, *17*(8).

Handel, A. (2018). Distance matters: Mobilities and the politics of distance. *Mobilities*, *13*(4), 473–487.

Harrison, S., & Dourish, P. (1996). Re-place-ing space: The roles of place and space in collaborative systems. In *Proceedings of the 1996 ACM conference on computer supported cooperative work* (pp. 67–76).

Harsanyi, J. C. (1967). Games with incomplete information played by "bayesian" players, part I. The basic model. *Management Science*, *14*(3), 159–182.

Hartshorne, R. (1939). The nature of geography: A critical survey of current thought in the light of the past. *Annals of the Association of American geographers*, *29*(3), 173–412.

Harvey, D. (2005). *The new imperialism*. Oxford University Press.

Harvey, D. (2018). *The limits to capital*. Verso books.

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463–471.

Heidegger, M. (2008). *Being and time*. SUNY Press.

Heiligenstein, M. X. (2023). *Facebook data breaches: Full timeline through 2023.* Firewall Times. Retrieved from `https://firewalltimes.com/{Facebook}-data-breach-timeline/` (Accessed: 2023-07-20)

Heilmann, S. (2016). Leninism upgraded: Xi jinping's authoritarian innovations. *China Economic Quarterly*, *20*(4), 15–22.

Helm, R. K., & Nasu, H. (2021). Regulatory responses to 'fake news' and freedom of expression: normative and empirical evaluation. *Human Rights Law Review*, *21*(2), 302–328.

Hern, A. (2018). *Fitness tracking app strava gives away location of secret us army bases.* The Guardian. Retrieved from `https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases`

Herskovits, M. J. (1949). *Man and his works: the science of cultural anthropology*. Alfred A. Knopf.

Hillier, B. (2007). *Space is the machine: A configurational theory of architecture*. Space Syntax.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Sage.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. McGraw Hill.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, *168*, 539–564.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45.

Huang, J., Kwan, M.-P., & Kim, J. (2021). How culture and sociopolitical tensions might influence people's acceptance of COVID-19 control measures that use individual-level geo-referenced data. *ISPRS International Journal of Geo-Information*, *10*(7), 490.

Humphreys, L. (2012). Connecting, coordinating, cataloguing: Communicative practices on mobile social networks. *Journal of Broadcasting & Electronic Media*, *56*(4), 494–510.

Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Lenz, R., Longhurst, J., ... Wolf, P. (2010). *Handbook on statistical disclosure control*. ESSnet on Statistical Disclosure Control. Retrieved from `https://cros-legacy.ec.europa.eu/system/files/SDC_Handbook.pdf`

Ipsos. (2019). *CIGI-Ipsos global survey on internet security and trust 2019 part I & II: Internet security, online privacy & trust.* Centre for International Governance Innovation. Retrieved from `https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf` (Accessed: 2023-07-08)

Ittelson, W. H. (1960). *Visual space perception*. Springer.

Jaidka, K., Zhou, A., Lelkes, Y., Egelhofer, J., & Lecheler, S. (2022). Beyond anonymity: Network affordances, under deindividuation, improve social media discussion quality. *Journal of Computer-Mediated Communication*, *27*(1).

Jansen, S. C., & Martin, B. (2015). The streisand effect and censorship backfire. *International Journal of Communication*, *9*, 656–671.

Jhally, S., & Livant, B. (1986). Watching as working: The valorization of audience consciousness. *Journal of Communication*, *36*(3), 124–143.

Ji, Y. (2022). *They panicked after the "public display of IP location", and IP proxy went viral.* Xiandaikuaibao. Retrieved from `https://new.qq.com/rain/a/20220505A09ZF600` (Accessed: 2023-02-15)

Jia, H., & Xu, H. (2016). Autonomous and interdependent: Collaborative privacy management on social networking sites. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 4286–4297).

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys*, *54*(1), 1–36.

Jiang, P. (2013). *Building constitutional socialism.* Economic Herald. Retrieved from `https://www.aisixiang.com/data/58774.html` (Accessed: 2024-02-20)

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*(3), 579–595.

Johnson, J. L. (1992). A theory of the nature and value of privacy. *Public Affairs Quarterly*, *6*(3), 271–288.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1–24.

Jones, C. B., Purves, R. S., Clough, P. D., & Joho, H. (2008). Modelling vague places with knowledge from the web. *International Journal of Geographical Information Science*, *22*(10), 1045–1065.

Jordan, T., Raubal, M., Gartrell, B., & Egenhofer, M. (1998). An affordance-based model of place in GIS. In *Proceedings of the international symposium on spatial data handling* (Vol. 8, pp. 98–109).

Kaasinen, E. (2003). User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, *7*(1), 70–79.

Kar, B., Crowsey, R. C., & Zale, J. J. (2013). The myth of location privacy in the United States: Surveyed attitude versus current practices. *The Professional Geographer*, *65*(1), 47–64.

Kaye, D. (2018). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.* United Nations. Retrieved from `https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement` (Accessed: 2023-03-15)

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Kelly, M. (2023). *Here's why threads is delayed in Europe.* The Verge. Retrieved from `https://www.theverge.com/23789754/threads-meta-twitter-eu-dma-digital-markets` (Accessed: 2023-07-20)

Kemp, S. (2023). *Digital 2023: China.* Data Reportal. Retrieved from `https://datareportal.com/reports/digital-2023-china` (Accessed: 2023-06-28)

Keßler, C., & McKenzie, G. (2018). A geoprivacy manifesto. *Transactions in GIS*, *22*(1), 3–19.

Ketelaar, P. E., & Van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182.

Khalid, H., Shihab, E., Nagappan, M., & Hassan, A. E. (2014). What do mobile app users complain about? *IEEE Software*, *32*(3), 70–77.

Khoi, N. M., Casteleyn, S., Moradi, M. M., & Pebesma, E. (2018). Do monetary incentives influence users' behavior in participatory sensing? *Sensors*, *18*(5), 1426.

Khoshgozaran, A., & Shahabi, C. (2007). Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *Proceedings of the international symposium on spatial and temporal databases* (Vol. 10, pp. 239–257).

Kido, H., Yanagisawa, Y., & Satoh, T. (2005). Protection of location privacy using dummies for location-based services. In *International conference on data engineering workshops (ICDEW)* (Vol. 21, pp. 1248–1248).

Kim, H.-S. (2016). What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior*, *54*, 397–406.

Kim, J., Kwan, M.-P., Levenstein, M. C., & Richardson, D. B. (2021). How do people perceive the disclosure risk of maps? Examining the perceived disclosure risk of maps and its implications for geoprivacy protection. *Cartography and Geographic Information Science*, *48*(1), 2–20.

King, G., & Zeng, L. (2001). Logistic regression in rare events data. *Political Analysis*, *9*(2), 137–163.

Kitchin, R., & Dodge, M. (2014). *Code/space: Software and everyday life.* MIT Press.

Kitiyadisai, K. (2005). Privacy rights and protection: foreign values in modern Thai context. *Ethics and Information Technology*, *7*(1), 17–26.

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of Social Issues*, *33*(3), 52–65.

Knijnenburg, B., Anaraky, R. G., Wilkinson, D., Namara, M., He, Y., Cherry, D., & Ash, E. (2022). User-tailored privacy. In B. Knijnenburg, X. Page, P. Wisniewski, H. Lipford, N. Proferes, & J. Romano (Eds.), *Modern socio-technical perspectives on privacy* (pp. 367–393). Springer, Cham.

Kobsa, A. (2001). Tailoring privacy to users' needs. In *Proceedings of the international conference on user modeling* (Vol. 8, pp. 301–313).

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593.

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences* (pp. 1–10).

Kummer, T.-F., Leimeister, J. M., & Bick, M. (2012). On the importance of national culture for the design of information systems. *Business & Information Systems Engineering*, *4*(6), 317–330.

Kummer, T.-F., Recker, J., & Bick, M. (2017). Technology-induced anxiety: Manifestations, cultural influences, and its effect on the adoption of sensor-based technology in German and Australian hospitals. *Information & Management*, *54*(1), 73–89.

Kummer, T.-F., Ryschka, S., & Bick, M. (2018). Why do we share where we are? The influence of situational factors on the conditional value of check-in services. *Decision Support Systems*, *115*, 1–12.

Kymäläinen, P., & Lehtinen, A. A. (2010). Chora in current geographical thought: Places of co-design and re-membering. *Geografiska Annaler: Series B, Human Geography*, *92*(3), 251–261.

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on ubiquitous computing (Ubicomp)* (pp. 273–291).

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... others (2018). The science of fake news. *Science*, *359*(6380), 1094–1096.

Lee, J.-M., & Rha, J.-Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, *63*, 453–462.

Lee, J.-S., & Hoh, B. (2010). Sell your experiences: A market mechanism based incentive for participatory sensing. In *2010 IEEE international conference on pervasive computing and communications (PerCom)* (pp. 60–68).

Lee, K.-F. (2018). *AI superpowers: China, silicon valley, and the new world order*. Houghton Mifflin.

Lee, L. T. (2007). Digital media technology and individual privacy. In C. Lin & D. Atkin (Eds.), *Communication technology and social change* (pp. 504–549). Routledge.

Legal Search. (2022). *The first case of user IP location protection: Weibo forced to disclose user IP location and was sued in court.* China Digital Times. Retrieved from `https://chinadigitaltimes.net/chinese/680556.html` (Accessed: 2023-03-18)

Leszczynski, A. (2015). Spatial big data and anxieties of control. *Environment and Planning D: Society and Space*, *33*(6), 965–984.

Levine, D. S., & Strube, M. J. (2012). Environmental attitudes, knowledge, intentions and behaviors among college students. *The Journal of Social Psychology*, *152*(3), 308–326.

Li, H. (2020). Negotiating privacy and mobile socializing: Chinese university students' concerns and strategies for using geosocial networking applications. *Social Media + Society*, *6*(1), 2056305120913887.

Li, P., Cho, H., Qin, Y., & Chen, A. (2021). #MeToo as a connective movement: Examining the frames adopted in the anti-sexual harassment movement in China. *Social Science Computer Review*, *39*(5), 1030–1049.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*, 453–496.

Li, Y. (2022). On the positive concept of personality right in the civil code. *Journal of Comparative Law*, *2022*(1), 71–82.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 501–510).

Lin, J., Benisch, M., Sadeh, N., Niu, J., Hong, J., Lu, B., & Guo, S. (2013). A comparative study of location-sharing privacy preferences in the United States and China. *Personal and Ubiquitous Computing*, *17*(4), 697–711.

Linabary, J. R., & Corple, D. J. (2019). Privacy for whom?: A feminist intervention in online research practice. *Information, Communication & Society*, *22*(10), 1447–1463.

Liu, J., & Zhao, H. (2021). Privacy lost: Appropriating surveillance technology in China's fight against COVID-19. *Business Horizons*, *64*(6), 743–756.

Liu, P., Teng, M., & Han, C. (2020). How does environmental knowledge translate into pro-environmental behaviors? The mediating role of environmental attitudes and behavioral intentions. *Science of the total environment*, *728*, 138126.

Locke, J. (2003). *Second treatise of government*. Gutenberg. `https://www.gutenberg.org/files/7370/7370-h/7370-h.htm`.

Loi, M., & Christen, M. (2020). Two concepts of group privacy. *Philosophy & Technology*, *33*(2), 207–224.

Lü, Y.-H. (2005). Privacy and data privacy issues in contemporary China. *Ethics of Information Technologies*, *7*, 7–15.

MacKinnon, R. (2011). Liberation technology: China's "networked authoritarianism". *Journal of Democracy*, *22*(2), 32–46.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). *Teens, social media, and privacy.* Pew Research Center. Retrieved from `https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/`

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261.

Massey, D. (1997). The spatial construction of youth cultures. In T. Skelton & G. Valentine (Eds.), *Cool places* (pp. 132–140). Routledge.

Massey, D. (2012). *Power-geometry and a progressive sense of place*. Routledge.

McCandless, D., Evans, T., Quick, M., Hollowood, E., Miles, C., Hampson, D., & Geere, D. (2021). *World's biggest data breaches & hacks.* Information is Beautiful. Retrieved from `https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`

McKenzie, G., & Janowicz, K. (2014). Coerced geographic information: The not-so-voluntary side of user-generated geo-content. In *Proceedings of the international conference on geographic information science* (Vol. 8).

McKenzie, G., Janowicz, K., & Seidl, D. (2016). Geo-privacy beyond coordinates. In T. Sarjakoski, M. Y. Santos, & L. T. Sarjakoski (Eds.), *Geospatial data in a changing world* (pp. 157–175). Springer.

Mead, M. (1973). *Coming of age in samoa*. American Museum of Natural History. Retrieved from `http://epcdssocialstudies.pbworks.com/f/Reading+Anthro.docx`

Mendelson, A. L., & Papacharissi, Z. (2010). Look at us: Collective narcissism in college student Facebook photo galleries. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 259–281). Routledge.

Merton, R. K. (1968). *Social theory and social structure*. Simon and Schuster.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4).

Michael, K., & Michael, M. (2011). *The social and behavioural implications of location-based services.* Taylor & Francis.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65–74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57.

Miller, D., Sinanan, J., Wang, X., McDonald, T., Haynes, N., Costa, E., ... Nicolescu, R. (2016). *How the world changed social media*. UCL Press.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125.

Mimno, D., Wallach, H., Talley, E., Leenders, M., & McCallum, A. (2011). Optimizing semantic coherence in topic models. In *Proceedings of the 2011 conference on empirical methods in natural language processing* (pp. 262–272).

Mocnik, F.-B. (2022). Putting geographical information science in place–towards theories of platial information and platial information systems. *Progress in Human Geography*, *46*(3), 798–828.

Mollema, L., Harmsen, I. A., Broekhuizen, E., Clijnk, R., De Melker, H., Paulussen, T., ... others (2015). Disease detection or public opinion reflection? Content analysis of tweets, other social media, and online newspapers during the measles outbreak in the netherlands in 2013. *Journal of Medical Internet Research*, *17*(5), e3863.

Momen, N., & Piekarska, M. (2017). Towards improving privacy awareness regarding apps' permissions. In *Proceedings of the international conference on digital society (ICDS)* (Vol. 11, pp. 18–23).

Nakada, M., & Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology*, *7*(1), 27–36.

Naous, D., Kulkarni, V., Legner, C., & Garbinato, B. (2019). Information disclosure in location-based services: An extended privacy calculus model. In *Proceedings of the international conference on information systems* (Vol. 40).

National People's Congress. (2020). *Civil code of the People's Republic of China.* China National Congress. Retrieved from `http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf` (Accessed: 2023-04-12)

Naveed, M., Ayday, E., Clayton, E. W., Fellay, J., Gunter, C. A., Hubaux, J.-P., ... Wang, X. (2015). Privacy in the genomic era. *ACM Computing Surveys*, *48*(1), 1–44.

Nelson, L. K. (2020). Computational grounded theory: A methodological framework. *Sociological Methods & Research*, *49*(1), 3–42.

Nelson, L. K., Burk, D., Knudsen, M., & McCall, L. (2021). The future of coding: A comparison of hand-coding and three types of computer-assisted text analysis methods. *Sociological Methods & Research*, *50*(1), 202–237.

Ni, V. (2022). *'Run philosophy': the Chinese citizens seeking to leave amid Covid uncertainty.* The Guardian. Retrieved from `https://www.theguardian.com/world/2022/jul/20/run-philosophy-the-chinese-citizens-seeking-to-leave-amid-covid-uncertainty` (Accessed: 2024-02-20)

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Nissenbaum, H. (2020). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2015). Enhancing privacy through caching in location-based services. In *2015 IEEE conference on computer communications (INFOCOM)* (pp. 1017–1025).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Nouwt, S. (2008). Reasonable expectations of geo-privacy. *SCRIPTed*, *5*(2), 375–403.

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management* (Vol. 1, pp. 121–138).

Paço, A., & Lavrador, T. (2017). Environmental knowledge and attitudes and behaviours towards energy consumption. *Journal of Environmental Management*, *197*, 384–392.

Papacharissi, Z. (2011). A networked self. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 304–318). Routledge.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236.

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the internet. *Computers in Human Behavior*, *50*, 252–258.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303.

Pee, L. G. (2011). Attenuating perceived privacy risk of location-based mobile services. In *Proceedings of the European conference on information systems (ECIS)* (Vol. 19).

Peng, C. (2023). Right to privacy and its relationship with personal information in Chinese law. *China Law Review*, *2023*(1), 161–178.

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the us and the eu? *Penn State Journal of Law & International Affairs*, *8*(1), 49–117.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press.

Phoenix SPI. (2023). *2022-23 survey of Canadians on privacy-related issues.* Office of the Privacy Commissioner of Canada. Retrieved from `https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/` (Accessed: 2023-07-08)

Pirie, G. (2009). Distance. In R. Kitchin & N. Thrift (Eds.), *International encyclopedia of human geography* (p. 242–251). Oxford: Elsevier.

Poikela, M. E. (2020). *Perceived privacy in location-based mobile system*. Springer.

Polonsky, M. J., Vocino, A., Grau, S. L., Garma, R., & Ferdous, A. S. (2012). The impact of general and carbon-related environmental knowledge on attitudes and behaviour of US consumers. *Journal of Marketing Management*, *28*(3-4), 238–263.

Pontes, T., Vasconcelos, M., Almeida, J., Kumaraguru, P., & Almeida, V. (2012). We know where you live: Privacy characterization of foursquare behavior. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 898–905).

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*(2), 181–195.

Preoţiuc-Pietro, D., & Cohn, T. (2013). Mining user behaviours: A study of check-in patterns in location based social networks. In *Proceedings of the 5th annual ACM web science conference* (pp. 306–315).

Proshansky, H. M., Ittelson, W. H., & Rivlin, L. G. (1970). *Environmental psychology: Man and his physical setting*. Holt, Rinehart and Winston New York.

Prudham, S. (2009). Commodification. In N. Castree, D. Demeritt, D. Liverman, & B. Rhoads (Eds.), *A companion to environmental geography* (pp. 123–142). Wiley.

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, *29*(4), 1841–1848.

Pu, X., Jiang, Q., & Fan, B. (2022). Chinese public opinion on Japan's nuclear wastewater discharge: A case study of Weibo comments based on a thematic model. *Ocean & Coastal Management*, *225*, 106188.

Purves, R. S., Winter, S., & Kuhn, W. (2019). Places in information science. *Journal of the Association for Information Science and Technology*, *70*(11), 1173–1182.

Pye, L. W. (1991). The state and the individual: An overview interpretation. *The China Quarterly*, *127*, 443–466.

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. *Computer Law & Security Review*, *34*(6), 1342–1354.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333.

Restuccia, F., Das, S. K., & Payton, J. (2016). Incentive mechanisms for participatory sensing: Survey and research challenges. *ACM Transactions on Sensor Networks (TOSN)*, *12*(2), 1–40.

Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review*, *66*, 41.

Ricker, B., Schuurman, N., & Kessler, F. (2015). Implications of smartphone usage on privacy and spatial cognition: Academic literature and public perceptions. *GeoJournal*, *80*, 637–652.

Rose-Redwood, R. S. (2006). Governmentality, geography, and the geo-coded world. *Progress in Human Geography*, *30*(4), 469–486.

Rossi, L., & Musolesi, M. (2014). It's the way you check-in: Identifying users in location-based social networks. In *Proceedings of the second ACM conference on online social networks* (pp. 215–226).

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404.

Rzeszewski, M., & Luczys, P. (2018). Care, indifference and anxiety—attitudes toward location data in everyday life. *ISPRS International Journal of Geo-Information*, *7*(10), 383.

Sadilek, A., Kautz, H., & Bigham, J. P. (2012). Finding your friends and following them to where you are. In *Proceedings of the fifth ACM international conference on web search and data mining* (pp. 723–732).

Scheider, S., & Janowicz, K. (2014). Place reference systems. *Applied Ontology*, *9*(2), 97–127.

Schneier, B. (2015). *Data and goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Schwartz, R., & Halegoua, G. R. (2015). The spatial self: Location-based identity performance on social media. *New Media & Society*, *17*(10), 1643–1660.

Schwarz, N. (1999). Self-reports: How the questions shape the answers. *American psychologist*, *54*(2), 93.

Seamons, K. (2022). Privacy-enhancing technologies. In B. Knijnenburg, X. Page, P. Wisniewski, H. Lipford, N. Proferes, & J. Romano (Eds.), *Modern socio-technical perspectives on privacy* (pp. 149–170). Springer, Cham.

Securiti Research Team. (2023). *Data privacy laws and regulations around the world.* Securiti. Retrieved from `https://securiti.ai/data-privacy-laws/` (Accessed: 2023-07-22)

Segall, M. H., Lonner, W. J., & Berry, J. W. (1998). Cross-cultural psychology as a scholarly discipline: On the flowering of culture in behavioral research. *American Psychologist*, *53*(10), 1101–1110.

Seidl, D. E., Jankowski, P., Clarke, K. C., & Nara, A. (2020). Please enter your home location: Geoprivacy attitudes and personal location masking strategies of internet users. *Annals of the American Association of Geographers*, *110*(3), 586–605.

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1–36.

Shen, X. (2022, May 2). *Weibo's new user location display appears to show that western tech gurus are based in China.* South China Morning Post. Retrieved from http://www.scmp.com/tech/big-tech/article/3176272/weibos-new-policy-display-user-locations-prompts-some-humour-among (Accessed: 2022-08-06)

Sievert, C., & Shirley, K. (2014). LDAvis: A method for visualizing and interpreting topics. In *Proceedings of the workshop on interactive language learning, visualization, and interfaces* (pp. 63–70).

Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of Sociology*, *11*(4), 441–498.

Smith, G. (2018). Step away from stepwise. *Journal of Big Data*, *5*(1), 1–12.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Solove, D. J. (2008). *Understanding privacy.* Harvard University Press.

Spearman, C. (1904). The proof and measurement of association between two things. *The American Journal of Psychology*, *15*(1), 72–101.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*, 161–167.

Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science*, *32*(11), 1492–1512.

State Council. (2014). *Planning outline for the construction of a social credit system (2014-2020).* China Copyright and Media. Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (Accessed: 2023-03-06)

State Council. (2017). *Notice of the state council on issuing the plan for market regulation during the 13th five-year plan period.* China Law Info. Retrieved from http://lawinfochina.com/Display.aspx?lib=law&Cgid=289420 (Accessed: 2023-03-06)

Stock, K. (2018). Mining location from social media: A systematic review. *Computers, Environment and Urban Systems*, *71*, 209–240.

Strahilevitz, L. J. (2005). A social networks theory of privacy. *University of Chicago Law Review*, *72*(3), 919–988.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*(1), 590–598.

Stutzman, F. D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 2.

Suh, J. J., & Metzger, M. J. (2022). Privacy beyond the individual level. In B. Knijnenburg, X. Page, P. Wisniewski, H. Lipford, N. Proferes, & J. Romano (Eds.), *Modern socio-technical perspectives on privacy* (pp. 91–109). Springer, Cham.

Sui, D., Elwood, S., & Goodchild, M. (2012). *Crowdsourcing geographic knowledge: volunteered geographic information (VGI) in theory and practice*. Springer.

Sun, C., Fan, W., & Ji, H. (2022). *Is it necessary for Weibo to disclose users' IP location to the exact province? Is it an invasion of privacy?* Southern Metropolis Daily. Retrieved from `https://m.mp.oeeee.com/a/BAAFRD0000202203266654 70.html` (Accessed: 2023-03-18)

Sunstein, C. R. (2006). *Infotopia: How many minds produce knowledge*. Oxford University Press.

Surden, H. (2007). Structural rights in privacy. *Southern Methodist University Law Review*, *60*(4), 1605–1629.

Swanlund, D., & Schuurman, N. (2019). Resisting geosurveillance: A survey of tactics and strategies for spatial privacy. *Progress in Human Geography*, *43*(4), 596–610.

Sweeney, L. (2000). Uniqueness of simple demographics in the US population. *LIDAP-WP4, 2000*.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826.

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research*, *22*(2), 211–233.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 2053951717736335.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies*. Springer.

Tear, A. (2020). Geotagging matters? The interplay of space and place in politicized online social media networks. In *Proceedings of the 2nd international symposium on platial information science* (pp. 61–72).

Tenbrink, T. (2020). The language of place: Towards an agenda for linguistic platial cognition research. In *Proceedings of the 2nd international symposium on platial information science* (pp. 5–12).

Thatcher, J. (2017). You are where you go, the commodification of daily life through 'location'. *Environment and Planning A: Economy and Space*, *49*(12), 2702–2717.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990–1006.

Thrift, N. (2004). Remembering the technological unconscious by foregrounding knowledges of position. *Environment and Planning D: Society and Space*, *22*(1), 175–190.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1–12.

Ting-Toomey, S. (1991). Intimacy expressions in three cultures: France, Japan, and the United States. *International Journal of Intercultural Relations*, *15*(1), 29–46.

Tobler, W. (1970). A computer movie simulating urban growth in the Detroit region. *Economic geography*, *46*(sup1), 234–240.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. Hert (Eds.), *Reforming european data protection law* (pp. 333–365). Springer.

Tuan, Y.-F. (1976). Humanistic geography. *Annals of the Association of American Geographers*, *66*(2), 266–276.

Tuan, Y.-F. (1977). *Space and place: The perspective of experience*. University of Minnesota Press.

Tuan, Y.-F. (1990). *Topophilia: A study of environmental perceptions, attitudes, and values*. Columbia University Press.

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society*, *9*(2), 300–318.

Twigger-Ross, C. L., & Uzzell, D. L. (1996). Place and identity processes. *Journal of Environmental Psychology*, *16*(3), 205–220.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157–178.

Wacks, R. (2015). *Privacy: A very short introduction*. Oxford University Press.

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age*. Cambridge University Press.

Wang, L. (2021). Harmonious but different: Demarcation and application of privacy and personal information rules. *Law Review*, *2021*(2), 15–24.

Wang, L. (2022). *Personality law (fourth edition)*. China Renmin University Press.

Wang, T., & Liu, L. (2009). From data privacy to location privacy. In P. Yu & J. Tsai (Eds.), *Machine learning in cyber trust* (pp. 217–246). Springer.

Wang, Z., & You, Y. (2016). The arrival of critical citizens: Decline of political trust and shifting public priorities in China. *International Review of Sociology*, *26*(1), 105–124.

Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of big data: The survey and countermeasures. *Computer Law & Security Review*, *31*(6), 782–792.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Watson, J., Lipford, H. R., & Besmer, A. (2015). Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *22*(6), 1–20.

Weibo Data Centre. (2020). *Weibo 2020 user development report.* Weibo. Retrieved from `https://data.weibo.com/report/file/view?download_name=4a774760-40fe-5714-498e-865d87a738fe&file-type=.pdf` (Accessed: 2023-04-12)

Weiser, P., & Scheider, S. (2014). A civilized cyberspace for geoprivacy. In *Proceedings of the 1st ACM SIGSPATIAL international workshop on privacy in geographic information collection and analysis* (pp. 1–8).

Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*, *25*(2), 227–252.

Werner, H., & Kaplan, B. (1963). *Symbol formation*. Wiley.

Westin, A. (1967). *Privacy and freedom*. Athenum.

Westin, A. (1984). The origins of modern claims to privacy. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthropology* (pp. 56–74). Cambridge University Press.

Westin, A. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research*, *16*(4), 362–369.

Wicker, S. B. (2012). The loss of location privacy in the cellular age. *Communications of the ACM*, *55*(8), 60–68.

Witthuhn, B. (1979). Distance: An extraordinary spatial concept. *Journal of Geography*, *78*(5), 177–181.

World Bank. (2021). *Individuals using the internet (% of population) - China.* The World Bank Group. Retrieved from `https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CN` (Accessed: 2023-06-28)

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897.

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the US and China. *Telecommunications Policy*, *35*(7), 603–616.

Xiao, X., & Tao, Y. (2006). Personalized privacy preservation. In *Proceedings of the 2006 ACM SIGMOD international conference on management of data* (pp. 229–240).

Xie, R., Chu, S. K. W., Chiu, D. K. W., & Wang, Y. (2021). Exploring public response to COVID-19 on Weibo with LDA topic modeling and sentiment analysis. *Data and Information Management*, *5*(1), 86–99.

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*(1), 42–52.

Yan, J., & Wang, L. (1996). Legal protection and compensation for damage of the citizens' right to privacy. *Modern Law Science*, *1996*(2), 86–92.

Young, L.-C. (1988). Regional stereotypes in China. *Chinese Studies in History*, *21*(4), 32–57.

Youxia News. (2022). *Do not want to display your IP location on Weibo? Customer support gives a way to hide.* Youxia. Retrieved from `https://www.ali213.net/news/html/2022-4/672333.html` (Accessed: 2023-04-12)

Yuan, Y., Wei, G., & Lu, Y. (2018). Evaluating gender representativeness of location-based social media: A case study of Weibo. *Annals of GIS*, *24*(3), 163–176.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? In *Proceedings of the 5th annual ACM web science conference* (pp. 463–472).

Zhan, X. (2022). *Full implementation of IP location, experts: No invasion of privacy.* https://www.sohu.com/a/542710749_121284943. Jimuxinwen. (Accessed: 2023-02-15)

Zhang, H. (2023). Place-based privacy: A humanistic reflection on solitude and anonymity. In *Proceedings of the 8th conference on spatial knowledge and information canada.* https://skiconference.ca/2023/papers/SKI2023_paper_20.pdf.

Zhang, H., & Malczewski, J. (2019). Quality evaluation of volunteered geographic information: The case of OpenStreetMap. In M. Khosrow-Pour (Ed.), *Crowdsourcing: Concepts, methodologies, tools, and applications* (pp. 1173–1201). IGI Global.

Zhang, H., & McKenzie, G. (2023). Rehumanize geoprivacy: From disclosure control to human perception. *GeoJournal*, *88*(1), 189–208.

Zhang, K., & Kizilcec, R. (2014). Anonymity in social media: Effects of content controversiality and social endorsement on sharing behavior. In *Proceedings of the international AAAI conference on web and social media* (Vol. 8, pp. 643–646).

Zhang, M., Zhao, P., & Qiao, S. (2020). Smartness-induced transport inequality: Privacy concern, lacking knowledge of smartphone use and unequal access to transport information. *Transport Policy*, *99*, 175–185.

Zhang, P. (2008). Revitalizing old industrial base of northeast China: Process, policy and challenge. *Chinese Geographical Science*, *18*, 109–118.

Zhang, Y., & Van der Schaar, M. (2012). Reputation-based incentive protocols in crowdsourcing applications. In *IEEE INFOCOM 2023 - IEEE conference on computer communications* (pp. 2140–2148).

Zhong, Y., Yuan, N. J., Zhong, W., Zhang, F., & Xie, X. (2015). You are where you go: Inferring demographic attributes from location check-ins. In *Proceedings of the eighth ACM international conference on web search and data mining* (pp. 295–304).

Zhou, H. (2021). Parallel or overlap: Relationships between personal information protection and privacy protection. *Peking University Law Journal*, *33*(5), 1167–1187.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283–289.

Zuo, Y. (2022). *Who is still wearing the "emperor's new clothes" after showing IP location?* China News. Retrieved from https://www.chinanews.com.cn/cj/2022/05-07/9748106.shtml (Accessed: 2023-02-15)

Appendix A

Online Survey

A.1 Internet Experience

Q1. Which of the following options is not a popular online social media platform in China?

- WeChat
- Douyin
- QQ
- Xiaohongshu
- Parking lot
- Sina Weibo
- Baidu Tieba
- Kuaishou
- Zhihu

[Q2] Scale 1-6: (1) Never (2) Less than one hour per week (3) At least one hour per week (4) At least five hours per week (5) At least ten hours per week (6) At least fifteen hours per week

Q2. How much time do you spend browsing the following social media platforms?
Platforms covered: Sina Weibo, Douyin, WeChat, Others

[Q3] Scale 1-6: (1) Never (2) Less than once per month (3) At least once per month (4) At least once per week (5) At least once per day (6) At least five times per day

Q3. How often do you participate in discussions (including posting, reposting, commenting and liking content) on the following social media platforms?
Platforms covered: Sina Weibo, Douyin, WeChat, Others

Q4. How often have you experienced some form of privacy breach in the last five years?

- Never
- Once or twice

- Three to five times
- More than five times
- Not sure/Don't know

A.2 Location Privacy Knowledge

Q5. To the best of your knowledge, which of the following methods could mobile social media applications use to collect location data from users? (Select all that apply)

- Satellite-based location sensors (e.g., GPS, Beidou)
- Internet Protocol (IP) addresses
- Browsing history
- Purchasing habits
- Usage patterns (e.g., screen time)
- Photographs
- Self-disclosed geotags (e.g., "From...")
- Textual contents (e.g., reviews, microblogs)
- Not sure/Don't know

China's PIPL is the country's first comprehensive legislation regulating the protection of personal information and data of "natural persons" located within China.

Q6. Are you aware of China's Personal Information Protection Law (PIPL), which went into effect on Nov. 1, 2021?

- I am not aware
- I have heard about the law, but am not sure about the details
- I have heard about the law and have basic understanding of what it covers
- I have heard about the law and fully understand my rights (e.g., obtaining consent; right to delete)
- I know all the details of the law

Q7. To the best of your knowledge, which of the following methods could protect one's location privacy? (Select all that apply)

- IP Proxy
- Virtual Private Network (VPN)
- Tor
- Turning off your phone
- Use a backup phone number
- Not sure/Don't know

A.3 Location Privacy Attitude

[Q8.1-8.4] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q8. Do you agree with the following views?

1. It bothers me to give location information to social media platforms.
2. Pervasive location information collection makes me worry about my location privacy when accessing social media platforms.
3. Compared to five years ago, I am more concerned about location privacy on the internet.
4. I believe other people (e.g., netizens and media) are too concerned with location privacy issues.

Q9. *If participants respond positively to Q8.3, Q9.1 will be displayed. Conversely, if participants respond negatively to Q8.3, Q9.2 will be displayed. Q9 will be skipped if participants choose "Not sure" for Q8.3.*

1. I am more concerned about location privacy issues on the internet than I was five years ago because:
   - I know more about location privacy risks online
   - I have more to lose if my location privacy were violated
   - I have had an experience that has changed my mind about location privacy
   - Some other reasons (please specify)
   - Not sure/Don't know
2. I am less concerned about location privacy issues on the internet than I was five years ago because:
   - Government regulations on data privacy have been strengthened
   - I feel safe even when my location information is disclosed
   - I feel powerless to make meaningful changes
   - Some other reasons (please specify)
   - Not sure/Don't know

IP location refers to the use of IP (Internet Protocol) addresses to identify the true geographic location of devices, such as cell phones and computers. On March 4, 2022, Sina Weibo debuted an IP location feature to counter disinformation about the crisis in Russia and Ukraine. The feature was introduced to several social media platforms (including Douyin, WeChat, Zhihu, Xiaohongshu, etc.) in April of the same year.

Q10. Which of the following screenshots does not contain the user's IP location information? *Screenshots from:* Sina Weibo, Douyin, WeChat, Xiaohongshu, Bilibili

[Q11.1-11.9] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q11. Do you agree with the following views?

1. I am concerned that my location information published online might be used for purposes other than how I originally intended.
2. I am concerned that my location information collected by social media platforms might be used for purposes other than how I originally intended.
3. I believe other people (e.g., netizens and media) are too concerned with location privacy issues.
4. Compared to five years ago, I am more concerned about location privacy on the internet.
5. My level of privacy concerns will be reduced if the IP location feature is only available on specific topics/users/posts/keywords (e.g., sensitive topics such as the Russia-Ukraine war).
6. Public IP location is less intrusive than public GPS location.
7. I believe that online location privacy is invaded when the IP location feature cannot be turned off.
8. It is important to me that I am informed about how my IP location information is determined.
9. I am satisfied with the steps that social media platforms take to ensure that the published IP location is accurate.

Q12. At which geographic scale do you think the IP location feature would achieve the best balance between privacy protection and anti-disinformation?

- No IP location
- Country (e.g., USA)
- Region (e.g., south China)
- Province (e.g., Guangdong)
- City (e.g., Shenzhen)
- District (e.g., Futian District)
- Street (e.g., Fuhua 1st Rd)

Q13. Do you have any other points to make about IP location and location privacy?

A.4 Location Privacy Behaviour

[Q14.1-14.6] Scale 1-6: (1) Never (2) Rarely (3) Sometimes (4) Often (5) Always (6) Not sure/Don't know

Q14. Which of the following frequencies best matches my Internet behaviour?

1. The location services on my mobile device are turned on.
2. I share my locations through social media applications.
3. I allow an application to access my current location when prompted.
4. I purposefully enter inaccurate address information when required by social media platforms.
5. I use the IP location function to follow the latest locations of celebrities.
6. I test whether my IP location was accurately displayed on the social media platforms.

[Q15] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q15. I stop using certain social media platforms (or deleted applications) after the introduction of mandatory IP location disclosure (after April 2022).

A.5 Demographic Variables

Q16. Gender

- Male
- Female
- Non-binary
- Prefer not to answer

Q17. Age

- 19 and younger
- 20-24
- 25-29
- 30-34
- 35-39
- 40-44

- 45-49
- 50 and older
- Prefer not to answer

Q18. Your current location

- *A list of Chinese provinces*
- Prefer not to answer

Q19. Education level

- Middle school and below
- High school or technical school
- College degree
- Bachelor's degree
- Master's degree and above

Q20. Monthly income (Chinese Yuan)

- Less than 1500
- 1501-3000
- 3001-5000
- 5001-8000
- 8001-10000
- 10001-15000
- 15001-20000
- $>$ 20001
- Prefer not to answer

Q21. What is your marital status?

- Single
- Married
- Divorced
- Prefer not to answer

Q22. How many children do you have?

- 0
- 1
- Two or more children
- Prefer not to answer

Appendix B

Consent Form

Please read this document before continuing to the survey. Submitting your study responses indicates that you consent to participate in this study. Please save or print a copy of this document to keep for your reference.

Researcher:
Hongyu Zhang
PhD Candidate
Department of Geography, McGill University
hongyu.zhang@mcgill.ca

Supervisor:
Grant McKenzie
Assistant Professor
Department of Geography, McGill University
grant.mckenzie@mcgill.ca

Title of Project: Survey on Online Location Privacy

Sponsor: Fonds de recherche du Québec - Société et culture (FRQSC)

Purpose of the Study: The purpose of the study is to analyze public opinions towards mandatory and voluntary location disclosure on Chinese online platforms.

Study Procedures: Your participation will involve filling out a short online questionnaire regarding your opinions of location disclosure on Chinese online platforms. Questions will ask about your knowledge and past experience of location privacy, your attitudes and behaviours towards location sharing, and several demographic indicators. The survey will take approximately 7 to 10 minutes to complete, and you will receive three Chinese Yuan as compensation for your participation in this survey.

Voluntary Participation: You must be over the age of 18 to participate in this survey. Participation is voluntary, and you may refuse to participate in any part of the study. You may decline to answer any question and may withdraw from the study at any time, for

any reason. Your responses will be kept confidential and will only be associated with your Credamo ID number. If you decide to withdraw from the survey, your participant data will be deleted. Two months after the completion of data collection, data will be de-identified, and your Credamo ID number will be removed from the database. Once de-identified, data can no longer be withdrawn.

Potential Risks: There are no anticipated risks to you by participating in this research.

Compensation: You are eligible to receive three Chinese Yuan as compensation upon completion of the survey. A code to redeem the payment through Credamo will be provided upon completion of the survey. Confidentiality: Your Credamo ID number will be collected as part of the survey to ensure you are able to be compensated for your participation. Data will be de-identified (your Credamo ID number will be removed from the survey results) two months after the completion of data collection. Additionally, the survey will ask for your age group, gender, income group, and educational level. De-identified survey results will be stored for seven years on a password-protected computer, in a separate encrypted password-protected computer file only accessible by the researchers (the Principal Investigator and his supervisor). Survey results will be amalgamated with those of other participants and analyzed using statistical software. The results of this research will be disseminated as part of a doctoral thesis project in the Department of Geography at McGill University.

Dissemination of Results: Results of this study will be disseminated in academic publications and/or presentations in both English and Chinese.

Questions: If you have any questions or require clarifications about the project, please contact hongyu.zhang@mcgill.ca. If you have any ethical concerns or complaints about your participation in this study and want to speak with someone not on the research team, please contact the Associate Director, Research Ethics at 514-398-6831 or lynda.mcneil@mcgill.ca citing REB file number **22-11-005**.

Note: The consent form was translated into simplified Chinese before being uploaded to Credamo for the survey.

Appendix C

Supplementary Regression Tables

Table C.1: Supplementary Regression Results

Model	Response Variable	Predictor	Estimate	SE	Z	*p*
9	A7	K2	0.327	0.092	3.560	<.001
10	A9	E4	0.215	0.060	3.590	<.001
		K2	-0.196	0.098	-2.000	0.045
		K3	0.395	0.100	3.940	<.001
11	A10	E2	-0.211	0.100	-2.110	0.035
		E3	0.276	0.112	2.470	0.013
		K1	0.278	0.103	2.710	0.007
		K2	0.292	0.105	2.780	0.005
12	A11	E2	-0.211	0.094	-2.241	0.025
		E3	-0.332	0.105	-3.179	0.001
		E4	0.252	0.062	4.065	<.001
		K2	-0.881	0.110	-7.975	<.001
		D3: East – Northeast	0.732	0.377	1.942	0.052
		Central – Northeast	1.049	0.446	2.355	0.019
		North – Northeast	0.530	0.407	1.303	0.193
		South – Northeast	0.772	0.411	1.877	0.060
		Northwest – Northeast	0.395	0.587	0.673	0.501
		Southwest – Northeast	1.254	0.492	2.548	0.011
18	B5	E1	0.391	0.106	3.700	<.001
		E2	0.438	0.097	4.530	<.001
		A1	-0.439	0.089	-4.950	<.001
		A4	-0.292	0.066	-4.440	<.001
19	B6	E2	0.517	0.092	5.630	<.001
		K1	0.190	0.096	1.980	0.048
		K2	0.493	0.098	5.040	<.001
		D1	0.329	0.169	1.950	0.051
		D2	-0.113	0.055	-2.060	0.039

Table C.2: Supplementary Regression Model Summary

Model	**Response Variable**	**Deviance**	**AIC**
9	A7	1326	1336
10	A9	1323	1337
11	A10	959	975
12	A11	1232	1260
18	B5	1346	1362
19	B6	1354	1372

Note: AIC = Akaike information criterion.