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

Rehumanize geoprivacy: From disclosure control to human perception

Hongyu Zhang[1*] and Grant McKenzie[1]

[1*]Platial Analysis Lab, Department of Geography, McGill University, Montreal, Quebec, Canada.

*Corresponding author(s). E-mail(s): hongyu.zhang@mcgill.ca;
Contributing authors: grant.mckenzie@mcgill.ca;

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.

Keywords: geoprivacy, location disclosure, geosurveillance, privacy concerns, location-based services

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 behavioral 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 others correlate significantly with location (Zhong, Yuan, Zhong, Zhang, & Xie, 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 2 identifies people's geoprivacy concerns, elaborates recent anti-geosurveillance attempts, and redefines geoprivacy from a *platial* perspective. Section 3 discusses the current context behind geoprivacy perceptions and how people's behaviour is impacted in this revolutionary environment. Section 4 examines spatial variations of geoprivacy from cultural, demographic, and legal perspectives, while Section 5 presents geoprivacy from an economic view and explores how geoprivacy is priced. Finally, Section 6 concludes the article and provides an outlook of future trends.

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, Dinev, & Xu, 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 and 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, 1968). 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 1 (Li, 2011; Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011).

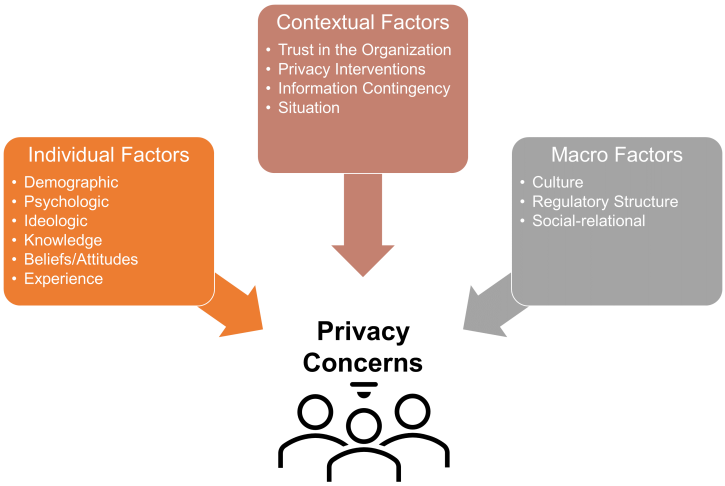

Fig. 1 Factors that influence an individual's perception of privacy (Adapted from Li, 2011; Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011)

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 and 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 (Crawford, 2014; Leszczynski, 2015). 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.

1.2 The privacy paradox

The privacy paradox describes the inconsistent nature between privacy attitudes and behaviour (Kar, Crowsey, & Zale, 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, Murayama, DeHaan, & Gladwell, 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.

2 Dimensions of geoprivacy

2.1 What are we afraid of?

Why do we care about geoprivacy, and what exactly are we afraid of? According to Culnan and Armstrong (1999), Milberg, Smith, and Burke (2000), and Malhotra, Kim, and Agarwal (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, Sitkin, Burt, & Camerer, 1998, p. 395). Trust has been found as a mediator (Malhotra et al., 2004; Metzger, 2004) or argued as a moderator (Joinson, Reips, Buchanan, & Schofield, 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, Elwood, & Goodchild, 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, Abdelmoty, El-Geresy, & Theodorakopoulos, 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, Yao, Liu, & Song, 2016), social relationships (Sadilek, Kautz, & Bigham, 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 dimensions (Figure 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.

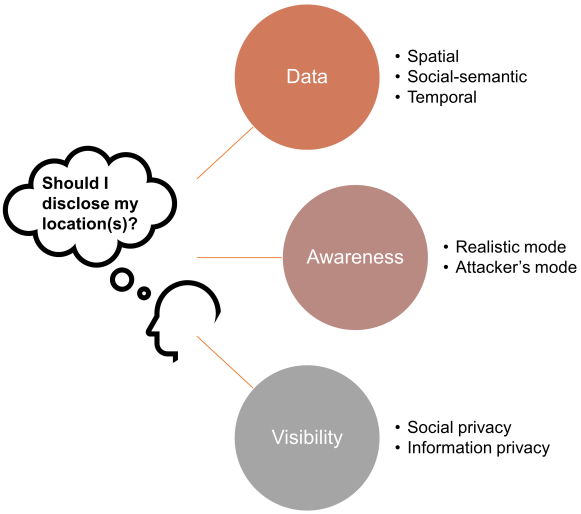

Fig. 2 Dimensions of the location disclosure problem (Adapted from Alrayes et al., 2020)

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?

Swanlund and 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 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 (Amini et al., 2011; Niu, Li, Zhu, Cao, & Li, 2015).

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, Yanagisawa, & Satoh, 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 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).

Table 1 Types of anti-geosurveillance tactics (Reassembled from Jiang et al., 2021; Swanlund & Schuurman, 2019).

Types	Descriptions	Examples
Minimization	Transfers less data	Cash transactions Caching (Niu et al., 2015)
Obfuscation	Adds random noise	Cloaking (Chow, Mokbel, & Liu, 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, Damgård, et al., 2015) Private information retrieval (Chor, Goldreich, Kushilevitz, & Sudan, 1995)

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, Janowicz, & Seidl, 2016). Additional studies on user profiling also explored home (Gu et al., 2016) or current location identification (Bellatti et al., 2017; Pontes, Vasconcelos, Almeida, Kumaraguru, & Almeida, 2012), future check-in location prediction (H. Gao, Tang, & Liu, 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 orientation) (Rossi & Musolesi, 2014; Zhong et al., 2015). Weiser and 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.

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, Winter, & Kuhn, 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, Winter, & Tomko, 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, Janowicz, McKenzie, & Li, 2013). Table 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.

Table 2 Space vs. place (S. Gao et al., 2013; Harrison & Dourish, 1996; Hillier, 2007; Tuan, 1977).

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

As a result, the notion of *place* is more relevant to our discussion of *geoprivacy* because of its subjective, qualitative, and emotional aspects (Cloke, Crang, & Goodwin, 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 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, 2005). 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, Floridi, & Van der Sloot, 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 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.

3.1 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" (Elwood & Leszczynski, 2011; Rose-Redwood, 2006), 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, O'Sullivan, & Mahmoudi, 2016) to emphasize the lack of control of personal location data in the 21st century. Table 3 lists the definitions of these concepts.

Table 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 and 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, Lau, Atkin, & Lin, 2011) and

was argued to be a major obstruction of location-based services (LBS) dissemination (Gupta, Xu, & Zhang, 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.

3.2 Deception and behavioural influences

Access to public location information about friends and strangers influences our behaviour and daily interaction with others (Dearman, Hawkey, & Inkpen, 2005; Michael & Michael, 2011). 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, Gross, & Acquisti, 2013). In recent years we have seen a rise in social media users deleting connections, comments, or even their applications (Alrayes & Abdelmoty, 2014; Boyles, Smith, & Madden, 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; Hassandoust, Akhlaghpour, & Johnston, 2021; Naous, Kulkarni, Legner, & Garbinato, 2019; Xu, Luo, Carroll, & Rosson, 2011). 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, Ryschka, and Bick (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.

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, Leimeister, & Bick, 2012; Kummer, Recker, & Bick, 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.

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, Hofstede, & Minkov, 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., Bellman, Johnson, Kobrin, & Lohse, 2004; Milberg et al., 2000; Posey, Lowry, Roberts, & Ellis, 2010). 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, Burke, Smith, & Kallman, 1995; Milberg et al., 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.

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, Bellotto, Hart, Russo, & Serra, 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 (Asai & Barnlund, 1998; G.-M. Chen, 1995). 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.

4.3 Demographic factors

Although social norms (Venkatesh, Thong, & Xu, 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, Rivera-Sánchez, and Lim (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, King, Li, & Turow, 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, Zhao, & Qiao, 2020) and internet experience (Hong, Chan, & Thong, 2019) 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).

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)."[1] 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

[1] https://www.facebook.com/policy.php

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 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, Shi, Dudley, & Graham, 2020). The integrity of information privacy laws, especially those targeting the private sector, will thus improve in China in the coming years.

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.

5.1 Surveillance capitalism

Location data can be viewed as a commodity traded in exchange for services (McKenzie et al., 2016; Prudham, 2009). Schneier (2015) called this kind of surveillance "a business model". Indeed, the "privacy information markets" (Crampton, 2015; Keßler & McKenzie, 2018; Thatcher, 2017) 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 20th 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).

5.2 Valuation of privacy

The value of privacy has been explored by researchers in psychology, economics, and management. Keßler and 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 questions are asked (Acquisti, John, & Loewenstein, 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 and 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 and 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, Kumpost, Matyas, & Danezis, 2006; Danezis, Lewis, & Anderson, 2005). J.-S. Lee and 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, Casteleyn, Moradi, & Pebesma, 2018). For future research, attention should be placed on helping participants making sensible decisions and controlling the quality of collected information (Restuccia, Das, & Payton, 2016). Specific incentive mechanisms for location-sensing also need to be developed because of the unique and complex nature of geoprivacy.

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 rehumanize 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 significant 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, Thompson, Hale, Lowry, & Greer, 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, Lin, & Miller, 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, Lipford, & Besmer, 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.

Declarations

- **Acknowledgements:** This work was supported by the Fonds de Recherche du Québec - Société et Culture (FRQSC) and the Canadian Internet Registration Authority (CIRA). The authors would like to gratefully acknowledge the reviewers of the manuscript, in its various forms.
- **Author contributions:** Hongyu Zhang conducted the literature review, crafted the arguments, and wrote the content. Grant McKenzie recommended readings, critically reviewed the manuscript, and provided detailed guidance and feedback. Both authors revised the manuscript before its submission.
- **Conflict of interest:** The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

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? *Interact* (pp. 214–221).

Adams, B., & Janowicz, K. (2012). On the geo-indicativeness of non-georeferenced text. *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. *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. *ICIS 2008 Proceedings*, 7.

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*(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.* 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.* Retrieved from http://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport

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. *Key concepts in geography*, 165–186.

Caverlee, J., & Webb, S. (2008). A large-scale study of myspace: observations and implications for online social networks. *Icwsm.*

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. *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*, *30*.

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

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

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. *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? *Weis* (Vol. 5).

Davies, S.G. (1997). Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. *Technology and privacy: The new landscape*, *143*, 144.

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 (JGIM)*, *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. *Dynamic & mobile GIS: investigating change in space and time*, *3*, 35–51.

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. *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. *ACM SIGSPATIAL COMP'13*.

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

Gu, Y., Yao, Y., Liu, W., Song, J. (2016). We know where you are: Home location identification in location-based social networks. *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. *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. (2019). Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *Journal of Business Ethics*, 1–26.

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 (CSUR)*, *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. *International symposium on spatial and temporal databases* (pp. 239–257).

Kido, H., Yanagisawa, Y., Satoh, T. (2005). Protection of location privacy using dummies for location-based services. *21st international conference on data engineering workshops (icdew'05)* (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. *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. *International conference on ubiquitous computing* (pp. 273–291).

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

Lee, L.T. (2007). Digital media technology and individual privacy. *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*(1), 28.

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. *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.* 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. (2005). The spatial construction of youth cultures. *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.* 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. *Eighth international conference on geographic information science.*

McKenzie, G., Janowicz, K., Seidl, D. (2016). Geo-privacy beyond coordinates. *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), JCMC942.

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. *Fortieth international conference on information systems.*

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 (CSUR)*, *48*(1), 1–44.

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

Pee, L.G. (2011). Attenuating perceived privacy risk of location-based mobile services. *ECIS 2011 Proceedings*, 238.

Pontes, T., Vasconcelos, M., Almeida, J., Kumaraguru, P., Almeida, V. (2012). We know where you live: privacy characterization of foursquare behavior. *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. *Proceedings of the 5th annual acm web science conference* (pp. 306–315).

Prudham, S. (2009). Commodification. *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. *Stan. L. Rev. Online*, *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. *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. *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*, 989–1015.

Solove, D.J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*, 477.

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 Science & Business Media.

Surden, H. (2007). Structural rights in privacy. *SMUL Rev.*, *60*, 1605.

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* (Vol. 126). Springer.

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

Tenbrink, T. (2020). The language of place: Towards an agenda for linguistic platial cognition research. *Proceedings of the 2nd international symposium on platial information science (platial-19)* (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*. U 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*. OUP Oxford.

Wang, T., & Liu, L. (2009). From data privacy to location privacy. *Machine Learning in Cyber Trust*, 217–246.

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. *Proceedings of the 1st acm sigspatial international workshop on privacy in geographic information collection and analysis* (pp. 1–8).

Westin, A.F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

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. *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. *2012 proceedings ieee infocom* (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. *Proceedings of the eighth acm international conference on web search and data mining* (pp. 295–304).