Towards place-based privacy: Challenges and opportunities in the "smart" world

Hongyu Zhang
Platial Analysis Lab, Department of Geography
McGill University
Montreal, Canada
hongyu.zhang@mcgill.ca

Grant McKenzie
Platial Analysis Lab, Department of Geography
McGill University
Montreal, Canada
grant.mckenzie@mcgill.ca

***Abstract*—The emergence of "smart" technologies has given rise to new interaction models merging our physical realities with our digital environments. As a result, new privacy threats have emerged, substantially impacting both individuals and groups. In this short paper, we summarize many of the privacy challenges we face in the smart and connected world, and identify opportunities for further research. Drawing from the recent literature on geoprivacy, user-tailored privacy, and group privacy, we explore this topic through the lens of contextually aware, place-based, or platial, information analysis.**

***Index Terms*—privacy, place, smart world, geoprivacy, metaverse**

I. Introduction

In the 1992 book *Out of Control* [1], Kevin Kelly described his version of a techno-utopia and cemented the term cybernetics (or "control and communication in the animal and the machine" [2]) in popular culture. In the same year, Neal Stephenson presented a libertarian society [3] that is controlled by algorithms and private interests, both online and offline, in his novel *Snow Crash* [4]. This novel also provided the first use of the term "metaverse." The re-branding of Facebook in late 2021 drew renewed interest in the term as well as their revised version of the concept. While the sales pitch for immersive virtual interaction sounds exciting, the realization of the metaverse will likely lead to the emergence of a new era of surveillance and privacy intrusion. Historically, concerned geographers have expressed their opinions on related technologies by coining terms such as "geoslavery" [5], "data colonialism" [6], and "data horror" [7]. These reflect a shared concern over who controls the data. Indeed, privacy concerns have never dissipated in the physical world and have already extended to virtual environments (e.g., video games). With the continued improvement of artificial intelligence techniques, our society is being transformed into a *smart* world that is omni-connected and constantly computed. Our objective with this short paper is to spur a discussion on the future of privacy with respect to the concept of *place*. Here we explore existing and future privacy challenges in the smart world, review recent opportunities in theoretical privacy research, and propose a place-based privacy approach that complements current work on geo- and location privacy. Our goals are to highlight emerging trends and research frontiers in modern privacy and to enable researchers to think about personal and private information from a multi-dimensional, *platial* perspective.[1]

This work was supported by the Fonds de recherche du Québec - Société et culture (FRQSC).

II. Privacy challenges in the smart world

From smart homes to smart cities, our living environment has continuously increased "intelligence." So too has the pervasiveness of personal information collection. The emergence of the metaverse is, again, pushing the boundaries between online and offline (social) interactions and, one might argue, is facilitating a socio-technical shift towards a *smart world* [8]. Privacy, as a result, is facing unprecedented challenges in this "cyber-physical-social-thinking hyperspace" [9]. In this section, we provide an overview of current privacy issues within smart cities and smart homes (or physical spaces/places) and then identify future privacy challenges in the metaverse (or virtual spaces/places).

Current smart city applications are widespread and are easily identified in our everyday lives. From smart cards, smart utilities, to smart mobility, the wide-ranging applications have improved the convenience of accessing public services and the efficiency of resource management and traffic control [10]. Major concerns about data privacy arise from the fact that it is not feasible to operate outside of a smart sensor-enabled urban environment [10]. Zhang et al. [11] shared three types of security and privacy issues one faces in a smart city. These can be summarized in the three stages of data analysis: *collection*, *processing*, and *disclosure* [11]. First, although security enhancement measures are in place, surveillance devices may capture spatial-temporal patterns and habits of individuals (e.g., visits to specific points of interest) in addition to its original design goal (e.g., monitoring criminal activities). Second, privacy breaches can occur in data storage and processing due to the involvement of untrusted cloud servers and edge computing. Finally, trustworthy and dependable control is probably the biggest challenge. Individual and societal rights can be difficult to balance, leaving trust in government to dwindle as privacy concerns rise [12].

[1]Platial is to place, which is similar to what spatial is to space.

Smart homes can be understood as micro smart city ecosystems [11]. Internet of Things (IoT) technologies are often deployed in residential settings, ranging from small gadgets (e.g., smart thermostats) to large appliances (e.g., smart fridges). What is unique to a smart home is the increased level of user control over smart sensing devices – typically managed through smart home personal assistants (SPA; e.g., Amazon Echo and Google Nest). These, however, face their own security and privacy challenges including *weak authentication*, *weak authorization*, and *profiling* [13]. Many of these are surprisingly still related to the limitations in natural language processing. First, synthesized speech can activate smart home devices as SPA are often unable to differentiate between audio playback and human speech. Second, the multi-user environment, weak payment authorization scheme, as well as external parties all contribute to errors. Third, inferences based on individual behaviours and social-economic status can be notoriously problematic and difficult to correct. More details about profiling will be discussed in the next paragraph.

Our discussion now turns to the metaverse, a three-dimensional space where virtual and reality interact and converge [14].[2] The combination of the Web, IoT, and extended reality (XR, which includes virtual (VR), augmented (AR), and mixed reality (MR) [15]) creates a shared online space for a plethora of social activities [16]. The emergence of the metaverse has brought about a brand new set of privacy concerns. The privacy challenges in the metaverse are threefold. First, virtual harassment and observation are much harder to identify than their physical equivalents [17]. The use of avatars (visible characters in the metaverse) [14] disguises real users and creates substantial concerns towards spying and stalking [17], doxing (the collection of private information for extortion or online shaming) [18], social engineering [17], and cyberbullying [19]. Second, the ability to conduct user profiling will reach an all-time high [19]. Web 2.0 is already capable of capturing online browsing activities such as the regions of interest and the amount of time a user spends on a web page or mobile app based on interaction. XR technologies enable additional streams of data collection, including body movements (e.g., eye tracking) and physiological responses (e.g., brainwaves), which allow platforms to study user behaviours with greater detail [19]. Lastly, the characteristics of the metaverse itself suggest underlying privacy issues. Its immersiveness and hyper spatiotemporality [20], for instance, can lead to users becoming disoriented and confused, resulting in unintended information disclosure. The decentralized and scalable nature of the technology [20], on the other hand, make adversary tracing a lot more complicated. The most concerning feature of which (in terms of privacy impacts) is probably interoperability [20], which once achieved (i.e., personal information is shared across all possible platforms in the metaverse) would essentially mean there is no place to hide.

[2]While the definition of the metaverse is a moving target (by design), here we use the term metaverse to broadly describe a societal shift towards increased interaction through virtual environments.

III. Opportunities in modern privacy research

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 as encryption (e.g., HTTPS), access control (e.g., two-factor authentication), and relay (e.g., Tor network) [21] may not all be applicable in the smart world. Other technical solutions to privacy also have their limitations [22]. In this section, we first analyze the constraints of existing privacy protection design principles, then introduce two emerging areas in privacy research, namely user-tailored privacy and group privacy.

There are many existing privacy-preserving solutions built into smart world applications. Though as Knijnenburg et al. [22] argued, plenty limitations have been recognized for these solutions (Table I). Take the three standards as examples. Even with privacy by design in place, privacy settings are still needed due to the fact that data collection is required to meet the primary design goals [23] and the variations of privacy preferences among users [24]. The notice-and-choice approach appears to offer options to users, but in reality, the legal jargon is time-consuming to read and difficult to understand [25], which to some degree forces users to make heuristic decisions [22]. Similarly, while privacy nudging can have a positive impact on disclosure behaviours, it creates an extra decision burden [22] for users who are already under information overload. Furthermore, technical countermeasures to privacy threats may not appeal (and therefore apply) to the designers of social networking applications [22] because personal information sharing is its key to success. Complementary methods are therefore required to combat the pervasive privacy risks.

TABLE I
THE LIMITATIONS OF POPULAR PRIVACY PRESERVING SOLUTIONS AS PRESENTED BY KNIJNENBURG ET AL. [22]

Categories	**Solutions**	**Limitations**
Architectures	Distributed systems	Slow
	Client-side personalization	Possible data loss and theft [26]
Standards	Privacy by design	Cannot replace privacy settings
	Notice & choice	Too long and complex
	Privacy nudging	Creates decision burden
Algorithms	Encryption	Slow
	Anonymization	Full anonymity not feasible [27]

Given the previously mentioned limitations, Kobsa [28] first introduced the concept of user-tailored privacy (UTP). The idea is different from personalized privacy [29], in which the model adjusts the degree of anonymity. Knijnenburg et al. [22] 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.

Thus far, our focus, and the majority of research, have been on individual privacy. However, the smart world and its ubiquitous data collection also pose privacy threats to groups and collectives [30]. 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 [31]), 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 [30]. In the latter category, individuals are unaware of their belongings 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) [30]. Multiple challenges remain to be addressed to better preserve group privacy. First, collaborative group privacy strategies face hindrance during the execution process because of the communication cost in multi-stakeholder decision-making environments [32]. Second, conflicts can happen when individual and group privacy rights contradict, and coordination fails within groups. Finally, it is uncertain how to properly manage the privacy of individuals who are unconscious of their group membership [33]. This will be a significant concern as the number of algorithmically determined groups boom in the metaverse.

IV. A MOVE TOWARDS PLACE-BASED PRIVACY

Both user-tailored privacy 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 [34], and through the continued practice of "Geo*X*" (geo-labeling of scientific subjects), the field of geoprivacy emerged [35]. 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 as well as emotional attachments [36]. Place and privacy can therefore be linked together when thinking from a cognate-based viewpoint [37] (i.e., in terms of privacy, "it is the belief that I am being watched that's my grievance" [38]). McKenzie et al. [39] 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 area than masking locations alone. Building on previous work [37], place-based privacy concerns are *culturally situated*, *location-dependent*, *time-variant*, and *people-centred* (Figure 1). Its key characteristics differentiate the concept from contextual privacy [25], 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 [40], in addition to self-constituted and algorithmically determined groups (see Section III). When places are broader regions or online communities, privacy concerns differ substantially based on cultural backgrounds [41] such as religions, histories, and sense of belonging. When places suggest points, privacy concerns are also location-dependent [39]. A higher degree of concerns 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 [42]. Finally, place-based privacy is people-centred. Places do not exist without human activities or imaginations [37], 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.

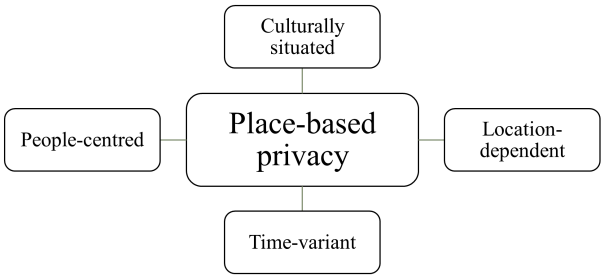

Fig. 1. Key characteristics of place-based privacy

V. CONCLUSION

From location privacy to geoprivacy, previous research has demonstrated that geographers and data scientists have an appetite for data privacy. The emergence of smart cities and the vision of metaverse are pushing concerns over actual and perceived privacy exposure to the next level. From urban sensing in smart cities to software-driven avatars in the metaverse, privacy threats prevail in many aspects of our daily lives. Globally, we must be prepared to adapt to the fast-changing technologies. Existing privacy-preserving solutions have their limitations, which may be overcome by incorporating user-tailored privacy and group privacy as supplementary design

philosophies. A shift towards place-based privacy furthers the discussion as it merges the core ideas of the two philosophies from a geographical perspective. Questions remain as to how we should balance privacy, design goals, and overfitting in automated privacy recommender systems. While underestimation compromises privacy, over-estimation also negatively impacts algorithmic performance. The future may not be as bleak as Kevin Kelly and Neal Stephenson described in their books, however. The transformation towards the smart world is not an overnight process, which means that we still have time to strengthen our technologies, educate and engage with both users and designers, and facilitate a broader discussion related to many of the forthcoming privacy threats.

REFERENCES

[1] K. Kelly, *Out of control: The rise of neo-biological civilization*. Addison-Wesley Longman Publishing Co., Inc., 1992.

[2] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*. MIT press, 1948.

[3] R. Leenes, "Privacy in the metaverse," in *IFIP International Summer School on the Future of Identity in the Information Society*, pp. 95–112, Springer, 2007.

[4] N. Stephenson, *Snow crash: A novel*. Spectra, 1992.

[5] J. E. Dobson and P. F. Fisher, "Geoslavery," *IEEE Technology and Society Magazine*, vol. 22, no. 1, pp. 47–52, 2003.

[6] J. Thatcher, D. O'Sullivan, and D. Mahmoudi, "Data colonialism through accumulation by dispossession: New metaphors for daily data," *Environment and Planning D: Society and Space*, vol. 34, no. 6, pp. 990–1006, 2016.

[7] D. Romm, H. Zhang, P. Verma, G. McKenzie, and E. Chen, ""data horror": Mapping (spatial) data privacy violations onto a cognitive account of horror," in *Spatial Data Science Symposium*, 2021.

[8] J. Ma, L. T. Yang, B. O. Apduhan, R. Huang, L. Barolli, and M. Takizawa, "Towards a smart world and ubiquitous intelligence: a walkthrough from smart things to smart hyperspaces and ubickids," *Journal of Pervasive Computing and Communications*, pp. 53–68, 2005.

[9] H. Liu, H. Ning, Q. Mu, Y. Zheng, J. Zeng, L. T. Yang, R. Huang, and J. Ma, "A review of the smart world," *Future generation computer systems*, vol. 96, pp. 678–691, 2019.

[10] D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489–516, 2017.

[11] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[12] R. Kitchin, "The real-time city? big data and smart urbanism," *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014.

[13] J. S. Edu, J. M. Such, and G. Suarez-Tangil, "Smart home personal assistants: a security and privacy review," *ACM Computing Surveys (CSUR)*, vol. 53, no. 6, pp. 1–36, 2020.

[14] S.-M. Park and Y.-G. Kim, "A metaverse: taxonomy, components, applications, and open challenges," *IEEE Access*, pp. 4209–4251, 2022.

[15] A. Çöltekin, I. Lochhead, M. Madden, S. Christophe, A. Devaux, C. Pettit, O. Lock, S. Shukla, L. Herman, Z. Stachoň, *et al.*, "Extended reality in spatial sciences: A review of research challenges and future directions," *ISPRS International Journal of Geo-Information*, vol. 9, no. 7, p. 439, 2020.

[16] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv:2110.05352*, 2021.

[17] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52–61, 2018.

[18] P. Snyder, P. Doerfler, C. Kanich, and D. McCoy, "Fifteen minutes of unwanted fame: Detecting and characterizing doxing," in *Proceedings of the 2017 internet measurement conference*, pp. 432–444, 2017.

[19] R. Di Pietro and S. Cresci, "Metaverse: Security and privacy issues," 2021.

[20] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *arXiv:2203.02662*, 2022.

[21] K. Seamons, "Privacy-enhancing technologies," in *Modern Socio-Technical Perspectives on Privacy*, pp. 149–170, Springer, Cham, 2022.

[22] B. P. Knijnenburg, R. G. Anaraky, D. Wilkinson, M. Namara, Y. He, D. Cherry, and E. Ash, "User-tailored privacy," in *Modern Socio-Technical Perspectives on Privacy*, pp. 367–393, Springer, Cham, 2022.

[23] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS quarterly*, pp. 13–28, 2006.

[24] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home iot privacy," *Proceedings of the ACM on human-computer interaction*, vol. 2, no. CSCW, pp. 1–20, 2018.

[25] H. Nissenbaum, "A contextual approach to privacy online," *Daedalus*, vol. 140, no. 4, pp. 32–48, 2011.

[26] A. Kobsa, H. Cho, and B. P. Knijnenburg, "The effect of personalization provider characteristics on privacy attitudes and behaviors: An e laboration l ikelihood m odel approach," *Journal of the Association for Information Science and Technology*, vol. 67, no. 11, pp. 2587–2606, 2016.

[27] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 111–125, IEEE, 2008.

[28] A. Kobsa, "Tailoring privacy to users' needs," in *International Conference on User Modeling*, pp. 301–313, Springer, 2001.

[29] X. Xiao and Y. Tao, "Personalized privacy preservation," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, pp. 229–240, 2006.

[30] J. J. Suh and M. J. Metzger, "Privacy beyond the individual level," in *Modern Socio-Technical Perspectives on Privacy*, pp. 91–109, Springer, Cham, 2022.

[31] A. Hern, "Fitness tracking app strava gives away location of secret us army bases," *The Guardian*, 2018.

[32] H. Jia and H. Xu, "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, 2016.

[33] M. Loi and M. Christen, "Two concepts of group privacy," *Philosophy & Technology*, vol. 33, no. 2, pp. 207–224, 2020.

[34] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[35] P. Weiser and S. Scheider, "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, 2014.

[36] S. Gao, K. Janowicz, G. McKenzie, and L. Li, "Towards platial joins and buffers in place-based gis," 2013.

[37] H. Zhang and G. McKenzie, "Rehumanize geoprivacy: from disclosure control to human perception," *GeoJournal*, pp. 1–20, 2022.

[38] R. Wacks, *Privacy: A very short introduction*. OUP Oxford, 2015.

[39] G. McKenzie, K. Janowicz, and D. Seidl, "Geo-privacy beyond coordinates," in *Geospatial Data in a Changing World*, pp. 157–175, Springer, 2016.

[40] B. Wellman, "Physical place and cyberplace: The rise of personalized networking," *International journal of urban and regional research*, vol. 25, no. 2, pp. 227–252, 2001.

[41] S. Petronio, *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

[42] J. Lin, M. Benisch, N. Sadeh, J. Niu, J. Hong, B. Lu, and S. Guo, "A comparative study of location-sharing privacy preferences in the united states and china," *Personal and ubiquitous computing*, vol. 17, no. 4, pp. 697–711, 2013.