Using urban big data in built environment research; a review of privacy and ethical challenges

Introduction

Motivation

Until around a decade ago, most urban-related data was generated using surveys, census, or basic administrative information (e.g., building permits, tax assessment rolls…etc.). These methods often provided aggregate high-level snapshots of city dynamics at specific moments in time that may quickly go out of date. Recently, new forms of urban-related data have emerged thanks to new technologies such as smart phones, RFID cards, motion sensors, drones, and social media among many others. These new forms of data fundamentally revolutionized the scope, frequency and resolution of data generated from cities, and offer immense un-tapped possibilities to better understand the dynamics of our urban environment. Until now, there are extensive of papers focusing on big data privacy issues of smart city, however, there is limited number of papers focusing on the privacy issue of built environmental research. Therefore, our motivation of writing this paper is to review the privacy challenges in terms of using urban big data in built environment research.

Background

Definition of built environment research and data and information flow

Built environment research, is a systematic and methodical process of enquiry and investigation aimed at dealing with buildings and infrastructure(Amaratunga et al. 2002). The built environment research applications of the era of big data relies on the corresponding enabling technologies to collect data from urban infrastructure. Then information is inferred through data mining and analysis, and finally knowledge can be obtained and used to improve our infrastructure. For example, sensor data acquisition is the first step along the way to harvest information from the built environment, and data analysis methods are needed to realize the end goals. Furthermore, the procedure of turning sensor data into useful knowledge can be further split into two steps: data-to-information transformation, and information-to- knowledge/action transformation (Dong et al. 2019). Through extensive literature review of smart city applications, we summarized four fields of built environment applications: Smart mobility, Smart waste and water system, Smart energy system, and Smart buildings. Nowadays, privacy issues associated with the IoT and our smart environment are starting to attract the attention of senior judges and standards bodies. For example, the US National Institute of Standards and Technology (NIST) has published guidelines for privacy and the smart grid, with the US energy industry recognizing that privacy must be a fundamental part of smart grid implementation rather than an afterthought(Boyes 2015). Therefore, knowing where is the data source and what type of data is used can help researchers better avoid potential privacy issues. In this paper, we will briefly discuss all these four built environment applications and data collected by these applications separately and then only focus on data that include private information.

Built environment research applications

1. Smart Mobility

There are four most typical applications of smart mobility according to the different application focus: smart parking; intelligent transportation system (ITS); app-based on-demand mobility services (transit apps); and Location-based service applications.*(i)* For smart parking applications, most common data sources are sensors and applications on mobile phones. Apart from the use of CCTV and license plate recognition sensors, most types of sensors can only acquire vehicle speed, presence/absence and other non-personal information that cannot be uniquely identified (Al-Turjman and Malekloo 2019). However, since the majority of smart parking solutions rely on web or mobile applications, they can collect not only location data, but also several other personal information such as the user's history of transaction and credit card information(Al-Turjman and Malekloo 2019). Such data can be further analyzed by service providers for improving the operational efficiency of the parking lot, such as deriving real-time pricing models, saving time looking for a parking space, emissions due to the vehicles' idle time. *(ii)* Being considered as a part of the Smart Mobility, Intelligent Transportation Systems (ITS) are the application of advanced technology to address transportation problems(Freitas et al. 2017). In ITS, data collected from diverse sources such as smart cards, sensors, CCTV and even social media etc. Although these data are mainly used by transportation research not strict built environment research, we would also discuss it because transportation system is the main infrastructure of a city. These data are used by the researches to extract knowledge and use it to improve the level of service for mobility. The improvement includes increasing the security, efficiency and sustainability of the transportation system(Zhu et al. 2019). For example, Smart Cards could collect information that could be correlated with criminal information to enhance transit security(Paul Stephen Dempsey 2019). In addition, floating car data (FCD) mainly refers to the vehicle mobility data at different locations in ITS, where customized detectors are embedded in vehicles (Huang 2010). These onboard sensors provide confident and efficient information for travel route selection and estimations(Zhu et al. 2019). *(iii)* Transit apps, which includes car-sharing (shared vehicle), ride-sharing (Car-pooling / Van-pooling), ride-sourcing (e.g. Lyft, Uber, and Sidecar), and e-hauling services (Normal Taxis) are another typical groups of applications under the umbrella of Smart Mobility(Asaad 2019). The implementation of transit applications requires the users to reveal not only their pick-up/drop-off locations but also the trip time and route, and these data can be used by researchers to describe user's daily commute routines(Bicocchi and Mamei 2014). *(iv)* Apart from these, ubiquitous positioning and mobile location-based services in smart phones are significant applications under the umbrella of Smart Mobility, and are the basis of several other smart transportation applications, and used by several built environment research that we will discuss here. The data collected by these applications can be used to cluster people whereabouts and discover hotspots of activities in the city, to extract the spatio-temporal dynamics of the city, highlighting where people usually go during the day(Reades, Calabrese, and Ratti 2009)(Calabrese, Fiore, and Ratti 2008), and to support on-demand mobility services(Eagle and Pentland 2009) etc.

2. Smart Energy systems

In recent years, the terms "Smart Energy" and "Smart Energy Systems" have been used to express an approach that reaches broader than the term "Smart grid". Where Smart Grids focus primarily on the electricity sector, Smart Energy Systems take an integrated holistic focus on the inclusion of more sectors (electricity, heating, cooling, industry, buildings and transportation) and allows for the identification of more achievable and affordable solutions to the transformation into future renewable and sustainable energy solutions(Lund et al. 2017). In smart energy system, different applications require different granularity levels of energy consumption data. The majority of smart meters collect electricity consumption data at a frequency of every 15 minutes to each hour(Wang et al. 2019). In addition, the higher granularity load data provided by smart meters offer greater potential for improving the forecast accuracy (Wang et al. 2019). However, there has always been a tradeoff between accuracy and privacy with regard to time resolution, because high-resolution data will make the usage habits of an appliance easier to be detected, causing potential privacy issues(Eibl and Engel 2015). High-frequency readings of Smart Meters can be used to establish detailed consumer profiles, including the electric appliances used in a household, waking and sleeping habits(Langer et al. 2013). The dynamic discovery of these patterns is important for many decision-making processes, such as consumer energy consumption behavior analysis, demand response optimization as well as improving energy reduction recommendations(Singh and Yassine 2019).

3. Smart Buildings

One of the most important application of smart buildings is building energy and management system (BESM). The objective of BESM is to control, analyze, and optimize the building energy consumption and achieve better in-door environmental quality using different sensors and actuators. The use of various sensors and measure data for building energy saving and occupant comfort has attracted extensive interest by the researchers(Choi and Yeom 2017)(Cheng and Lee 2014) (Abdallah et al. 2016) (Kim, Schiavon, and Brager 2018). The main sources of data are sensors deployed in the home and wearable devices attached to occupants. The major types of measured data collected by a sensor are listed in the Table 2(Dong et al. 2019). Wireless sensors along with a computerized base station are used to detect abnormal behaviors, data are collected, then analyzed and transferred to a secure central web site for viewing by the carer/relative(Lotfi et al. 2012). For example, data collected from sensors attached to the front door and the back door of a house shows that for most days the front and back doors were opened for a short period of time. However, in some instances, if both doors were left open for a long period of time, it can be tagged as abnormal behaviors, which can be noticed by relatives or carer of an old man (Lotfi et al. 2012). In addition, smart security is another typical application. The smart security system processes various data collected through sensors, sends them to residents through their mobile phones and helps them make quick responses and better decisions on the incidents concerning their safety/security, such as fires, thefts(Hong, Yang, and Rong 2016), and flammable gas leakage(Fraiwan et al. 2011).

4. Smart waste and water systems

Flood control, smart bin and smart irrigation are typical applications we will discuss in this paper. Weather related data like temperature, rain, humidity, pressure, wind speed and water levels at rivers, lakes, dams, and other reservoirs is collected to facilitate better flood control(Rathore et al. 2016). However, according to Chen and Irwin's research, Weatherman localizes coarse (one-hour resolution) energy consumption, wind, and solar data to within 16.68km, 9.84km, and 5.12km, respectively, on average(Chen and Irwin 2018). Although these weather data could give some information as every location on the Earth has a distinct weather signature that uniquely identifies it (Chen and Irwin 2018), we consider that this resolution would not pose any potential privacy issue to citizens. In addition, data collected by the sensing nodes, involved in the ground and environmental sensing, considering soil moisture, soil temperature, air temperature, Ultraviolet (UV) light radiation, and relative humidity of the crop field are used to predict the irrigation requirements of a field, thereby achieving optimum water-resource utilization in the precision farming landscape(Goap et al. 2018).

Definition of privacy

In the context of smart city built environment research, the most important issue that people are concerned is privacy. The approach to privacy in legal and regulatory regimes focuses on protecting personal data, including health, financial, and communications data. However, in a smart-built environment, privacy concerns might predominantly relate to location and life-pattern data (Boyes 2015). Researchers should know how to avoid privacy issues during the research process. People should also clearly know what data is being used by researchers and whether it will threaten their privacy. Before discussing privacy issues, we should first give a definition of privacy in the context of built environment research. In fact, in the era of big data, all aspects of citizen's privacy are at stake. In this paper, we will use the five types of privacy categorized by David Eckhoff et al. (Eckhoff and Wagner 2018), they can be described as follows:

Privacy of Location. Location information is usually defined as the spatial-temporal information and how long the location was visited. Violating location privacy can reveal a person's home and workplace, but also allow inferences about other types of privacy, for example habits, purchase patterns, or health. In addition, co-location information allows inferences about a person's social life (Eckhoff and Wagner 2018).

Privacy of State of Body & Mind. The state of body and mind encompasses a person's bodily characteristic including biometrics, health genome, mental states, emotions, opinions, and thoughts. Violating this type of privacy can cause discrimination by insurance company or employers.

Privacy of Social Life. This includes what they said in the conversation on the social media platform, also the mega data of these conversation, for example who a person interact with, when and for how long. Violating this type of privacy can pose privacy issue on people's everyday life.

Privacy of Behavior & Action. The privacy of behavior and action includes a person's habits, hobbies, actions, and purchase patterns. Often, this information allows to draw far-reaching conclusions about the user's life and therefore other types of privacy.

Privacy of Media. Media privacy includes image, video and audio data about a person. Usually, redistributing or creating user-related media without consent constitutes a privacy violation.

Problem Statement

Although there has been a lot of research on the privacy of smart cities, there is no generalization about privacy in the study of the built environment. Therefore, we would like to write a paper summarizing the privacy of the built environment.

Objectives

This paper mainly focuses on three aspects of built environment research: 1) identify built environment research applications that rely on urban big data, which including future/potential applications in built environment research that would rely on using data generated from smart phone applications or IoT devices. 2) identify approaches used to address privacy and ethical issues when using urban big data in built environment research. 3) proposing a risk assessment tool of privacy issue in terms of built environment research.

Literature review

Privacy protection in built environment research

Smart mobility

After extensive literature review, we summarized data collection of applications in terms of smart mobility as table 1. For vehicle-related data collected for mainly smart parking application, we noticed that only CCTV and vehicle license recognition sensors have potential privacy issue to customers. CCTV and other image processing sensors can pose threats on people's privacy of media. In addition, although the vehicle license recognition sensor seems not directly collect private data, we think it can still pose private issue to their users because the license is an unique identification of an vehicle which can be linked to its owner. Apart of vehicle-related data, we found that smart mobility applications generally collect users' GPS data, which can reveal the spatiotemporal data of users and pose significant privacy issues. Many of researchers such as Dara proposed that personal trajectory data are increasingly collected for a variety of academic and recreational pursuits. As access to location data widens and locations are linked to other information repositories, individuals become increasingly vulnerable to identification (Dara E. Seidl 2016). Obfuscation of point data, or masking, is a solution that aims to protect privacy and maximize preservation of spatial pattern. Dara proposed two methods of obfuscation for personal GPS data: grid masking and random perturbation. We found that obfuscation of GPS data can effectively address its privacy issue. Moreover, for smart transportation applications such as smart card to bus or metro, trip data and financial data can be linked to the owner and revealed by research, therefore, the anonymity of these data is crucial.

Table 1. Smart mobility data collection

Data Types	Sensor Type/Specific Data	Personal/Privacy Data Involved
Vehicle-related data	Active infrared Sensor	None
	Ultrasonic sensors	None
	CCTV & image processing	Directly
	Vehicle license recognition	Indirectly

	Passive infrared sensor	None
	LDR sensor	None
	Inductive loop detector	None
	Piezoelectric sensor	None
	Pneumatic road tube	None
	Magnetometer	None
	Vehicle-in-motion sensors	None
	Microwave radar	None
	RFID	None
	Acoustic sensor	None
GPS data	Real-time location	Directly
Trip data	Trip time/route	Directly
	Travel patterns	Indirectly
Financial data	Credit card information	Directly
	History of transaction	Directly
Marketing data	Consumption habit	Indirectly
Other data	Name	Directly
	Address	Directly
	Contact Information	Directly

Smart building

As shown in Table 2, we summarized three categories of data collected by smart building applications. For smart building, the occupancy data indicating the number of people and their presence in a building are playing an increasingly important role in energy consumption, optimization processes, and indoor air quality by built environment researchers. Ahmad et al. summaries 6 main techniques in terms of occupancy detection: video cameras, infra-red, ultrasonic, radio frequency, data obtained from multiple sensors; such as CO2 and other environmental sensors, and Wireless Local Area Network (WLAN), WIFI and Bluetooth. Among these techniques, although occupancy measurement via camera and RFID are most accurate techniques that can not only detect occupancy but also count the number of people, however, they are considered having potential privacy threats to occupants (Ahmad et al. 2018). Moreover, data collected by thermostats and HVAC systems can be used to not only understand energy usage patterns, but also predict occupant behavior patterns in buildings(John et al. 2018). By addressing this problem, Ahmad et al. proposed an encryption scheme, which can hide and encrypt the region of interest (ROI) and hence preserve the privacy of an individual during monitoring and counting process. The proposed scheme was tested and showed that it can effectively solve privacy issues (Ahmad et al. 2018). It is worth noticing that we found all other types of sensor can collect private data such as wearable sensors, smart phones, or other sensors can collect physical data of their users.

Table 2. Smart building data collection.

Data Type	Sensor Type/Specific Data	Personal/Privacy Data Involved
Occupancy data	Image based sensor	Directly
	Passive Infrared sensor	None
	Radio-based sensor	Directly
	Threshold and mechanical sensor	Indirectly
	Chair sensor	Directly
	Pressure mats	Directly
	Camera sensor	Directly
	Photo sensor	Directly
	Ultrasonic doppler	None
	Microwave doppler	None
	Ultrasonic ranging	None
Built environment data	CO2 sensor	None
	Air Temperature sensor	None
	Humidity sensor	None
	Thermo-fluidic sensor	None
	Sound sensor	Directly
	Light sensor	None
	Volatile organic compound sensor	None
	Particulate Matter (PM) sensor	None
	Air velocity sensor	None
Other types of data	Wearable sensor	Directly
	Smart Phones	Directly
	Heart Rate sensor	Directly
	Fingerprint sensor	Directly
	Mobile pupilometer	Directly
	Skin Temperature sensor	Directly

Smart Energy System

The smart energy system mainly use the data collected by smart meter to find the Energy consumption pattern of customers thereby optimizing the delivery of electricity, gas, and thermal energy. Actually, according to the smart meter data, users living pattern can be revealed easily by analyzing these data. Therefore, Since optimizing energy supply is primarily for users in a community, we do not recommend using household water meter data, but rather using a community's smart meter data for analysis and optimization. This effectively resolves personal privacy issues. If total water meter data is not available, we can choose to anonymous user information to reduce the risk of privacy breaches. For example, the smart meter acts as a sensor node and records the consecutive electricity consumption (kilo watt hour [kWh]) and time of use (TOU) (National Energy Technology Laboratory (NETL) 2007). In addition, data collected by sensors in smart grid can be used to monitor the generation of electricity, power quality throughout the grid, equipment health and capacity, fault locations, meter tampering, vegetation intrusion, and also load balance between the grid and Demand Energy Response (DER) or renewal energy resources in the energy cycle(Griffith, Souryal, and Golmie 2010). Data sensing in the smart grid requires sensing of parameters such as voltage, current, temperature, moisture, continuity, and phase to calibrate and control various equipment on the basis of the fluctuations of these parameters(Nipendra Kayastha, Dusit Niyato 2015).

Smart waste and water systems

Some types of smart bins only involve a sensor that measures the fullness of waste, whereas others enable the simultaneous authentication of the user through smart card access(van Zoonen 2016). We consider this can pose serious privacy threat to citizens, because the researcher's main purpose of collecting capacity data through smart trash bins is to use these data to plan more efficient urban garbage collection routes and improve urban operation efficiency. However, the personal authentication would not add much value to users that giving these private information. In addition to ground and environmental data, the water usage data record collected by a smart water meter could be analyzed to show the vacancy of a specific household and reveal water habits of end-users, which could have potential privacy concerns. This issue is highly depending on who can access these data and how these data will be used and reported. For example, if the trend of water-saving was promoted widely, groups or locations for unusual or excessive water usage can be stigmatized by others(Giurco, White, and Stewart 2010). Above all, in generally speaking, data collected by smart waste and water system applications would not pose privacy issue if no personal or identifiable information linked to these data. For example, if smart bins only collected the fullness of waste without the simultaneous authentication of the user, there is no potential privacy issue can be posed.

Reference

Abdallah, Moatassem, Caroline Clevenger, Tam Vu, and Anh Nguyen. 2016. “Sensing Occupant Comfort Using Wearable Technologies.” *Construction Research Congress 2016: Old and New Construction Technologies Converge in Historic San Juan - Proceedings of the 2016 Construction Research Congress, CRC 2016*, no. May 2019: 940–50. https://doi.org/10.1061/9780784479827.095.

Ahmad, J., H. Larijani, R. Emmanuel, M. Mannion, and A. Javed. 2018. “Occupancy Detection in Non-Residential Buildings – A Survey and Novel Privacy Preserved Occupancy Monitoring Solution.” *Applied Computing and Informatics*. https://doi.org/10.1016/j.aci.2018.12.001.

Al-Turjman, Fadi, and Arman Malekloo. 2019. “Smart Parking in IoT-Enabled Cities: A Survey.” *Sustainable Cities and Society* 49 (December 2018). https://doi.org/10.1016/j.scs.2019.101608.

Amaratunga, Dilanthi, David Baldry, Marjan Sarshar, and Rita Newton. 2002. “Quantitative and Qualitative Research in the Built Environment: Application of ‘Mixed’ Research Approach.” *Work Study* 51 (1): 17–31. https://doi.org/10.1108/00438020210415488.

Asaad, Islam Nasser. 2019. “The Cognitive and Affective Antecedents to Consumer Behavior towards On-Demand Transportation Services in Egypt.”

Bicocchi, Nicola, and Marco Mamei. 2014. “Investigating Ride Sharing Opportunities through Mobility Data Analysis.” *Pervasive and Mobile Computing* 14: 83–94.

https://doi.org/10.1016/j.pmcj.2014.05.010.

Boyes, Hugh. 2015. "Security, Privacy, and the Built Environment," 25–31.

Calabrese, Francesco, Filippo Dal Fiore, and Carlo Ratti. 2008. "Digital Footprinting:," 36–43.

Chen, Dong, and David Irwin. 2018. "Weatherman: Exposing Weather-Based Privacy Threats in Big Energy Data," 1079–86. https://doi.org/10.1109/bigdata.2017.8258032.

Cheng, Chin Chi, and Dasheng Lee. 2014. "Smart Sensors Enable Smart Air Conditioning Control." *Sensors (Switzerland)* 14 (6): 11179–203. https://doi.org/10.3390/s140611179.

Choi, Joon Ho, and Dongwoo Yeom. 2017. "Study of Data-Driven Thermal Sensation Prediction Model as a Function of Local Body Skin Temperatures in a Built Environment." *Building and Environment* 121: 130–47. https://doi.org/10.1016/j.buildenv.2017.05.004.

Dara E. Seidl, Piotr Jankowski & Ming-Hsiang Tsou. 2016. "Privacy in the Smart City Preservation in Masked GPS Trajectory Data." *International Journal of Geographical Information Science*.

Dong, Bing, Vishnu Prakash, Fan Feng, and Zheng O'Neill. 2019. "A Review of Smart Building Sensing System for Better Indoor Environment Control." *Energy and Buildings* 199: 29–46. https://doi.org/10.1016/j.enbuild.2019.06.025.

Eagle, Nathan, and Alex Sandy Pentland. 2009. "Eigenbehaviors: Identifying Structure in Routine." *Behavioral Ecology and Sociobiology* 63 (7): 1057–66. https://doi.org/10.1007/s00265-009-0739-0.

Eckhoff, David, and Isabel Wagner. 2018. "Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions." *IEEE Communications Surveys and Tutorials* 20 (1): 489–516. https://doi.org/10.1109/COMST.2017.2748998.

Eibl, Gunther, and Dominik Engel. 2015. "Influence of Data Granularity on Smart Meter Privacy." *IEEE Transactions on Smart Grid* 6 (2): 930–39. https://doi.org/10.1109/TSG.2014.2376613.

Fraiwan, Luay, Khaldon Lweesy, Aya Bani-salma, and Nour Mani. 2011. "A Wireless Home Safety Gas Leakage Detection System," 11–14.

Freitas, Andre, Lina Brito, Karolina Baras, and Jose Silva. 2017. "Smart Mobility: A Survey." *Internet of Things for the Global Community, IoTGC 2017 - Proceedings*, no. 351. https://doi.org/10.1109/IoTGC.2017.8008972.

Giurco, Damien P., Stuart B. White, and Rodney A. Stewart. 2010. "Smart Metering and Water End-Use Data: Conservation Benefits and Privacy Risks." *Water (Switzerland)* 2 (3): 461–67. https://doi.org/10.3390/w2030461.

Goap, Amarendra, Deepak Sharma, A. K. Shukla, and C. Rama Krishna. 2018. "An IoT Based Smart Irrigation Management System Using Machine Learning and Open Source Technologies." *Computers and Electronics in Agriculture* 155 (September): 41–49. https://doi.org/10.1016/j.compag.2018.09.040.

Griffith, David, Michael Souryal, and Nada Golmie. 2010. "Wireless Networks for Smart Grid Applications." *Smart Grid Communications and Networking* 9781107014: 234–62. https://doi.org/10.1017/CBO9781139013468.011.

Hong, Xin, Chenhui Yang, and Chunming Rong. 2016. "Smart Home Security Monitor System," 5–9. https://doi.org/10.1109/ISPDC.2016.42.

Huang, Enyang. 2010. "Algorithmic and Implementation Aspects of Online Calibration of Dynamic Traffic Assignment." *MSc - MIT*.

John, Camille, Charalampos Vallianos, José Candanedo, and Andreas Athienitis. 2018. "Buildings and Urban Environments."

Kim, Joyce, Stefano Schiavon, and Gail Brager. 2018. “Personal Comfort Models – A New Paradigm in Thermal Comfort for Occupant-Centric Environmental Control.” *Building and Environment* 132: 114–24. https://doi.org/10.1016/j.buildenv.2018.01.023.

Langer, Lucie, Florian Skopik, Georg Kienesberger, and Qin Li. 2013. “Privacy Issues of Smart E-Mobility.” *IECON Proceedings (Industrial Electronics Conference)*, 6681–87. https://doi.org/10.1109/IECON.2013.6700238.

Lotfi, Ahmad, Caroline Langensiepen, Sawsan M. Mahmoud, and M. J. Akhlaghinia. 2012. “Smart Homes for the Elderly Dementia Sufferers: Identification and Prediction of Abnormal Behaviour.” *Journal of Ambient Intelligence and Humanized Computing* 3 (3): 205–18. https://doi.org/10.1007/s12652-010-0043-x.

Lund, Henrik, Poul Alberg Østergaard, David Connolly, and Brian Vad Mathiesen. 2017. “Oviloe2egrkgtlep,Glgr;Gl3[Rpl4-Olre[Gplep[Lepglrrppe[Ogrp[Glrrp4-Fo[Sv;Ff;Fkkedlw’;Q\]w’123lk,f.v,Fb,f.V12456---6789knbghglgglmflb;Fl=l0-0-1-2-303040-5-6-7-8-9-0nlb/n,Mnb./Lbkh.j.k,m,/Hlm,;Lj,Yl;k’t.--;Lljkhjlg-,Gl;j,;l[Tkp[Lkp’lu[Klku=[;g’;h]Hkh-Yytyyhre.” *Energy* 137: 556–65. https://doi.org/10.1016/j.energy.2017.05.123.

Nipendra Kayastha, Dusit Niyato, Ekram Hossain and Zhu Han. 2015. “Smart Grid Sensor Data Collection, Communication, and Networking: A Tutorial.” *Wireless Communications and Mobile Computing*, no. February 2015: 421–30. https://doi.org/10.1002/wcm.

Paul Stephen Dempsey. 2019. “PRIVACY ISSUES WITH THE USE OF SMART CARDS” 1: 1–18. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3295908.

Rathore, M. Mazhar, Awais Ahmad, Anand Paul, and Seungmin Rho. 2016. “Urban Planning and Building Smart Cities Based on the Internet of Things Using Big Data Analytics.” *Computer Networks* 101 (2016): 63–80. https://doi.org/10.1016/j.comnet.2015.12.023.

Reades, Jonathan, Francesco Calabrese, and Carlo Ratti. 2009. “Eigenplaces: Analysing Cities Using the Space - Time Structure of the Mobile Phone Network.” *Environment and Planning B: Planning and Design* 36 (5): 824–36. https://doi.org/10.1068/b34133t.

Singh, Shailendra, and Abdulsalam Yassine. 2019. “Mining Energy Consumption Behavior Patterns for Households in Smart Grid.” *IEEE Transactions on Emerging Topics in Computing* 7 (3): 404–19. https://doi.org/10.1109/TETC.2017.2692098.

Wang, Yi, Qixin Chen, Tao Hong, and Chongqing Kang. 2019. “Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges.” *IEEE Transactions on Smart Grid* 10 (3): 3125–48. https://doi.org/10.1109/TSG.2018.2818167.

Zhu, Li, Fei Richard Yu, Yige Wang, Bin Ning, and Tao Tang. 2019. “Big Data Analytics in Intelligent Transportation Systems: A Survey.” *IEEE Transactions on Intelligent Transportation Systems* 20 (1): 383–98. https://doi.org/10.1109/TITS.2018.2815678.

Zoonen, Liesbet van. 2016. “Privacy Concerns in Smart Cities.” *Government Information Quarterly* 33 (3): 472–80. https://doi.org/10.1016/j.giq.2016.06.004.