Sunyup Park
University of Maryland, College Park, United States of America

Citizens' Right to Privacy and Right to Information Access in Smart Cities: Evaluating the Smart City Initiative of West Baltimore

Abstract

This paper will detail smart city initiatives in West Baltimore and evaluate different approaches to ensure the right to privacy and the right to information access of lower-income communities of color. After evaluating these approaches, this paper proposes recommendations to facilitate the right to privacy and the right to information access in lower-income communities.

1. Introduction

Smart cities utilize the Internet of Things (IoT) and big data to collect, analyze, and distribute citizens' data in order to enhance quality of life (Kitchen, 2016). The smart city initiative in West Baltimore, Maryland (USA) focuses on solving the chronic issues of complex and lengthy public transportation trips. Transportation is not only important in terms of quality of living, but can also be an indicator of economic mobility, as researchers state that long commute times can negatively impact residents' economic mobility over time (Chetty et al., 2015). Thus, smart cities not only aim to enhance citizens' quality of life, but also strive towards social justice. In order to realize this vision, smart cities need to address privacy concerns that arise from data utilization (Kitchen, 2016). This paper argues that smart cities often fail to address citizens' privacy concerns and citizens' right to privacy and right to information access should be guaranteed.

The concept of privacy varies depending on the context of the technology that it is situated in. Traditional definitions of privacy emphasize self-determination and communication of one's information (Warren & Brandies, 1890; Westin, 2003) that can be applied to the smart city context as the right to "accessing and disclosing personal and sensitive information about a person which includes locational and movement privacy" (Kitchen, 2016, p. 25).

Along with the right to privacy, individual access rights are critical drivers for establishing trust and support in new connected technologies, such as smart cities (Tene & Polonetsky, 2013). In the context of smart cities, access to one's data means "providing individuals with access to their data in a usable format and allowing them to take advantage of third-party applications to analyze their own data and draw useful conclusions" (Tene & Polonetsky, 2013). Thus, in terms of fulfilling civil liberty in a democratic society and facilitating a participatory democracy, the right to privacy and the right to information access in smart cities can be seen as two sides of the same coin.

This paper will look into the smart city initiative in West Baltimore with the population of lower-income communities of color in terms of residents' right to privacy and right to information access.

2. Smart cities' impact on lower-income communities: Case of West Baltimore

Lower-income communities are more likely to be impacted by the infringement upon the right to privacy and the right to information access from smart city technologies. Upon investigating the intersection of privacy and poverty, Madden et al. (2017) stated that "many surveillance systems that surround the poor are purposefully designed to deliver a message of stigma to the subject while reinforcing societal stereotypes about dependency" (p. 61), demonstrating how new technologies can be used to discourage the poor from engaging fully in the society. Madden (2014) also notes that lower-income and less educated populations are less informed about privacy issues and thus vulnerable to data privacy breaches. Against this backdrop, however, when investigating residents' concerns about smart city data in West Baltimore, Lung-Amam et al. (2019) found that residents wanted access to the data collected about their neighborhood. For example, residents wanted to better inform city officials about what data is missing or can be improved about the neighborhood. In other words, data subjects demanded participation throughout the process. Thus, understanding residents' privacy and data concerns and providing mechanisms for their right to privacy and information access are necessary for both successful implementation of smart city initiatives and for social justice.

The West Baltimore region consists predominantly of African Americans (96%), and most residents are less educated and lower-income (Lung-Amam et al., 2018). According to the U.S. Department of Transportation (U.S. DOT), Baltimore City was listed in the ten worst cities in America for the longest commute times, with residents spending an average of 55 minutes to commute using public transportation (The City of Baltimore, 2016). Along with neighborhood concerns on public safety and job opportunities, there was a need for high-quality and reliable transportation (Lung-Amam et al., 2018). For example, teens were affected by a month-long subway closure that increased their commute times to school (Lung-Amam et al., 2018). The public transit use and quality of service that residents experience in West Baltimore strengthen the socio-economic disparity that residents face (Kaufman et al., 2015).

3. Current practices and regulations to protect the right to privacy in smart cities

Privacy laws in the U.S. are sectoral, and data privacy is protected by the Fair Information Practice Principles (FIPPs) set by the Organisation for Economic Co-operation and Development (OECD). FIPPs was established in response to the development of automatic data processing and transmission of data between nations in order to prevent violations of human rights regarding data privacy (OECD, 2013). Since smart city technology utilizes personal data, it falls under the FIPPs principles for protection and regulation. FIPPs include eight basic principles that serve as a basis for national implementation, including collection limitation, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability (OECD, 2013). The U.S. Federal Trade Commission (FTC) adopted four out of eight principles, which are choice, notice, security, and access (Federal Trade Commission, 2000).

However, critics have argued that FIPPS have fallen behind technology, especially with the rise of IoT and big data (Barocas & Nissenbaum, 2014). Accordingly, amendments were made in

2012, and the revised FIPPs were proposed in the Consumer Privacy Bill of Rights (The White House, 2012). The main revision was to break from the traditional notion of "notice and choice" that assumes a passive user to "transparency and control" that assumes an active individual in achieving autonomy. Under the notice and consent scheme, the user would read long, complex legal documents and agree to terms and conditions, which are usually non-negotiable (e.g., end user license agreements). Under the transparency and control scheme, the focus is on effective design spaces for notice and increased control features for users. The revised FIPPs also acknowledge privacy as an evolving concept influenced by technological development. Lastly, rather than gathering all possible data, the new FIPPs promote data minimization in order to prevent possible misuse of data.

4. Evaluating Smart City Technology in West Baltimore in Accordance with FIPPs

The core of the smart city project in West Baltimore lies in its use of users, vehicles, and cell phones as probe sensors to collect location data in order to support customized, real-time travel information, passenger and freight trip planning, performance monitoring, and decision-making (The City of Baltimore, 2016). These probe sensors are embedded in everyday objects, which makes data collection ubiquitous and pervasive, thus difficult for users to be aware. The City of Baltimore has partnered with various private-public information organizations to accomplish its vision.

Considering that the intelligent sensor-based infrastructure is the core of Baltimore's smart city vision of utilizing citizens' data from their smartphones, there is a strong need to examine stakeholders' privacy policies. In this section, the CitiStat program, RITIS, and Google/Waze's privacy policy was reviewed based on FIPPs. First, CitiStat program violates the principle of transparency and access in FIPPs because the dashboard content is optimized for personal computer (PC) view. This is problematic since the majority of the residents in West Baltimore did not own a PC but relied on smartphones (Lung-Amam et al., 2018). Second, RITIS violates the access and accuracy principles of FIPPs as it provides little or no way of participation for its users to erase or modify their data. Additionally, RITIS infringes upon both transparency and control, and focused collection principles, as it claims to perpetually store data without clear explanations of its purpose. Last, behind the lengthy description of its privacy policy, Google/Waze violates the respect for context principle because its data usage is beyond its primary navigational purposes. Additionally, information is gathered as much as possible, violating the focused collection principles.

5. Recommendations

Based on the evaluation of West Baltimore's smart city program, the following recommendations will better address citizens' right to privacy and right to information access for smart city initiative in West Baltimore:

- The initiative should increase transparency and control in its privacy policies with detailed descriptions of what and how the data is collected and address them in a mobile-friendly manner to reach its intended audience.
- When there is the potential for increased access to user data, such as through mobile phones, there should also be features that allow users to erase or modify their data.
- Stakeholders should engage in data minimization and limit data collection to what they need for their intended services and purposes. If they want to collect data for additional

purposes, they should communicate it to the residents in advance with simple and straightforward language.

This paper acknowledges that FIPPs are principles that information organizations are encouraged to follow regarding data privacy and are not legally binding. Thus, this paper suggests governance and management-level solutions should supplement the lack of legislative enforcement regarding data privacy in smart city technologies. Having strong, principle-led governance and management will maximize the benefits of a smart city and minimize its harms (Kitchin, 2016).

References

Baltimore City Information & Technology. (n.d.). *Open data policy*. City of Baltimore. https://technology.baltimorecity.gov/open-data-policy

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In Lane, J., Stodden, V., Bender, S., & Nissenbaum, H (Eds.), *Privacy, big data, and the public good frameworks for engagement* (pp. 44-75). Cambridge University Press. http://dx.doi.org/10.1017/CBO9781107590205.004

Boyles, J. L., Smith, A., & Madden, M. (2012, September 5). *Privacy and data management on mobile devices*. Pew Research Center. http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). Smart privacy for the smart grid: Embedding privacy into the design of electricity conservation. *Identity in the Information Society, 3*(2), 275–294. https://doi.org/10.1007/s12394-010-0046-y

Chetty, R., Hendren, N., Kline, P., & Saez, E. (2015). *Economic mobility.* The Stanford Center on Poverty and Inequality. http://cpi.stanford.edu/media/sotu/SOTU_2015_economic-mobility.pdf

Federal Trade Commission. (2000, May). *Privacy online: Fair information practices in the electronic marketplace.* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

Goodman, E. P., & Powles, J. (2019). Urbanism under google: Lessons from sidewalk Toronto. *Fordham Law Review, 8*(2), 457–498.

Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly, 27*(4), 371–376. https://doi.org/10.1016/j.giq.2010.05.003

Kaufman, S. M., Moss, M. L., Hernandez, J., & Tyndall, J. (2015, November). *Mobility, economic opportunity and New York City neighborhoods.* NYU Rudin Center. https://wagner.nyu.edu/files/rudincenter/2015/11/JobAccessNov2015.pdf

Kitchin, R. (2016, January 28). *Getting smarter about smart cities: Improving data privacy and data security*. Department of the Taoiseach. http://mural.maynoothuniversity.ie/7242/1/Smart

Kitchin, R., Cardullo, P., & Di Feliciantonio, C. (2019). Citizenship, justice, and the right to the smart city. In Cardullo, P., Feliciantonio, C. D., & Kitchen, R (Eds.), *The right to the smart city*. Emerald Publishing Limited. https://osf.io/preprints/socarxiv/b8aq5

Lukács, A. (2016). *What is privacy? The history and definition of privacy*.

http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf
Lung-Amam, W., Bierbaum, A., Parks, S., Stamm, L., Sunderman, G., & Knaap, G. (2018, October). *Smart cities, connected communities: Using technology to meet the needs of West Baltimore residents*. https://www.umdsmartgrowth.org/city/wp-content/uploads/2018/12/Final-Smart-Cities-West-Baltimore-Report.pdf
Lung-Amam, W., Bierbaum, A. H., Parks, S., Knaap, G., Sunderman, G., & Stamm, L. (2019). Toward engaged, equitable, and smart communities: Lessons from West Baltimore. *Housing Policy Debate*, 1–19. https://doi.org/10.1080/10511482.2019.1672082
Madden, M. (2014, November 12). *Public perceptions of privacy and security in the post-Snowden era*. Pew Research Center. http://pewinternet.org/2014/11/12/public-privacy-perceptions
Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: matrix of vulnerabilities for poor americans. *Washington University Law Review*, 95(1), 53-126. OECD. (2013). *The oecd privacy framework.* https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
Office of Performance & Innovation. (n.d.). *About CitiStat*. https://www.baltopi.com/about-citistat
RITIS. (n.d.). *RITIS introduction*. https://www.ritis.org/intro
Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), [xxvii]-274.
The City of Baltimore. (2016). *B'smart: Connecting communities to opportunities in Baltimore for a safe, efficient, sustainable, equitable and economically competitive smart city.* https://cms7.dot.gov/file/59336/download?token=uX3Lrdgq
The White House. (2012, February). *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy.* https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf
van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. https://doi.org/10.2307/1321160
Waze. (n.d.). *Waze - Privacy policy*. https://www.waze.com/legal/privacy
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072
Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742. https://doi.org/10.1002/sec.795