Finding Balance between Technological Advancement, Cybersecurity, and Privacy: Ensuring Public Trust in Smart Cities

Kristina Gamache

Department of Cybersecurity

IDS 300W

Dr. Pete Baker

03/24/25

Over the last 30 years, there has been a growing drive towards the implementation of Smart Cities in urban and metropolitan areas. According to Caragliu in his review, "Smart Cities in Europe", defines smart cities as, "A city is smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance. Smart cities form a connection between technological advancement and urban development to improve the quality of life of the individuals living in the city. Often, the planning and management of these cities are quite extensive because of their multi-faceted nature (Albino et al., 2015). This makes issues involving smart cities complex and necessitates a collaborative approach to best address these issues. One of the primary issues is that due to a smart city's reliance on digital infrastructure, many individuals have expressed concerns regarding the security of the cyber networks that are backbones to these technologies (Alhalafi, N., & Veeraraghavan, P., 2023). Additionally, for smart cities to function properly, citizens must be willing to participate in the technology-based programs, while the city itself is challenged with ensuring its inhabitants maintain their "right to privacy" (Khan, 2021). It all comes down to how these smart cities are able to effectively balance the need for technological advancements with cybersecurity and privacy concerns. If this balance can be achieved, it should yield general public trust in smart cities.

The technological aspect is just one of many that give smart cities their multi-faceted nature when it comes to development and execution. It is often the initial component explored when delving into the world of smart cities. This is because it is the technology that establishes these smart cities and allows them to continue to operate. Technology is an intrinsic part of smart

cities. While there are several different kinds of technologies utilized, technological advancement for smart cities primarily focuses on Information and Communication Technologies (ICTs) and Internet of Things (IoT) devices (Sánchez-Corcuera, R., 2019). The National Institute of Standards and Technology (NIST) defines ICTs as "Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information" and IoTs as "The network of devices connected to the Internet that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information." (2020). Essentially, smart cities' prevalent technologies are ones that either store, process, or facilitate communication with other entities, including the Internet. One case study regarding smart city technology implemented in the city of Ottawa, Canada, describes the city's use of a salt management system. This automated system retrieves and compiles several factors, including road temperatures and weather forecasts, to help manage and determine the best course of action for the city's salt spreaders (Sánchez-Corcuera, R., 2019). This is an example of ICTs and IoT devices being used to help improve standards of living by ensuring the citizens of Ottawa have access to safe roads.

Yet, operating in a similar space, the city of Baltimore experienced a ransomware attack that compromised the city's Computer-Aided Dispatch system for approximately 17 hours; a system that automatically dispatches first responders based on proximity to the emergency (Reuters, 2018). This attack on an ICT system in Baltimore illustrates one of the major concerns surrounding the use of technological advancements in smart cities. These systems pose a cybersecurity risk to the city and its citizens. A cybersecurity risk refers to the loss of confidentiality, integrity, or availability of information, data, or information systems (NIST, 2020). Smart cities are reliant on the use of ICTs and IoTs because of their ability to

communicate with each other and countless devices around them. It is this interconnectedness of this technology that allows systems like salt management and Computer-Aided Dispatch to operate as intended, but also opens up vulnerabilities and exploits. In Sunday et al.(2024), several cybersecurity risks of smart cities are illustrated, including the use of IoT and ICT, as well as the interconnected web of communication between all these devices. There is a consensus in the IT community that, due to a lack of standardized security protocols for IoT devices, they are susceptible to exploitation by attackers. This consensus, combined with "Profit-driven businesses and time-to-market along with the short-age of related legislation have stimulated manufacturers to overlook security considerations and to design potentially vulnerable IoT device." (Neshenko et al., 2019) has led to several types of vulnerabilities found across the massive scale of IoT devices, including inadequate authentication and insufficient access controls (Neshenko et al., 2019). These types of vulnerabilities can be exploited by attackers to gain unauthorized access to not only the device itself, but also because of the interconnected nature of these devices in smart cities, may allow an attacker unauthorized access into the greater network of devices. Because of the prevalence of IoT devices in Smart cities and their associated cybersecurity risk, this creates conflict when attempting to balance technological advancement and cybersecurity concerns.

While there are risks associated with IoT and ICT use in smart cities, it is because of these devices and systems that smart cities can function as intended. The accessibility and convenience of data transmission and communication would not be possible without these devices. Therefore, the increased cybersecurity risk brought about by IoT and ICT use may be mitigated by enhancing other security measures and implementing regulations in an effort to harden the entire digital infrastructure. This can be accomplished through a combination of

practices, including but not limited to: implementing strong encryption protocols, solid authentication methods, network segmentation, Role-based access control (RBACs), conducting regular vulnerability testing, and enforcing regulations (Sunday et al., 2024). Authentication methods require the user to verify their identity prior to granting access, which lowers the risk of an attacker gaining unauthorized access. As for encryption protocols, network segmentation, and RBACs, these all prevent an unauthorized user from either moving around into other locations in the network or accessing sensitive data. Vulnerability testing allows those responsible for maintaining the system and networks to try and find the issues before attackers can. Lastly, implementing and enforcing regulations ensures that specific devices, protocols, or practices that are best suited for the Smart city environment are the ones being utilized (Sunday et al., 2024). These practices address many of the risks and concerns of ICT and IoT use in smart cities, while still allowing them to operate normally. While the risk is not eliminated, enacting enhanced security measures can help alleviate some of the cybersecurity concerns regarding technological advancements in Smart cities.

Cybersecurity is not the only concern when addressing issues related to the technology of smart cities. Privacy is another sizable concern to consider. Van Zoonen (2016) expressed in their article “Privacy concerns in smart cities” how the privacy concerns centered on two major elements: how an individual perceived their particular data, and for what the data was being collected for. Essentially, if an individual believed a specific piece of information to be more personal or sensitive, they were more likely to express concern regarding the privacy of that information. Additionally, individuals expressed increased privacy concerns when the purpose of the data collection was for surveillance rather than a service. These two elements of privacy concerns are grounded in the psychological needs and desires for privacy. But psychology is not

the only influence over smart city privacy concerns. There is also a legal right to privacy recognized by most countries. Depending on the location of the city, privacy concerns could extend as far as an infringement on an individual's right to privacy. For the purpose of this paper, we will focus on privacy rights pertaining to the United States. The concept of privacy from both a legal standpoint and a psychological one is an instance of conflict for technological advancements in Smart cities. Certain levels of privacy may not always be a possibility when it comes to data collection, analysis, and storage requirements needed to facilitate a functioning smart city.

Several definitions within the psychology community attempt to define the concept of privacy. Westin (1968) captures the essentials with, “People need control over their transactions with others (to varying degrees) to experience the well-being that is associated with intimacy and emotional release.” People need to have a sense of control over both whether or not they interact with others, as well as how to navigate interactions they do have, to truly experience the well-being obtained from being with oneself. Essentially, if an individual does not have control over who, how, and when they interact with others, the individual will be unable to experience the level of comfort and emotional ease of just being alone. Without control, they will also be under the impression that someone else is in the vicinity.

References

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, *22*(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities*, *6*(3), 1523–1544. https://doi.org/10.3390/smartcities6030072

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, *18*(2), 65–82. https://doi.org/10.1080/10630732.2011.601117

Khan, M. A. (2021). A formal method for privacy‐preserving in cognitive smart cities. *Expert Systems*, *39*(5). https://doi.org/10.1111/exsy.12855

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702–2733. https://doi.org/10.1109/comst.2019.2910750

NIST. (2020). *Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary

Reuters. (2018, March 18). *Baltimore's 911 emergency system hit by cyberattack*. NBC News. https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876

Sánchez-Corcuera, R., Nuñez-Marcos, A., Sesma-Solance, J., Bilbao-Jayo, A., Mulero, R., Zulaika, U., Azkune, G., & Almeida, A. (2019). Smart cities survey: Technologies, application domains and challenges for the cities of the future. *International Journal of*

Distributed Sensor Networks, *15*(6), 155014771985398. https://doi.org/10.1177/1550147719853984

Sunday, J., Biu, W., & Obi, C. (2024). SECURING THE SMART CITY: A REVIEW OF CYBERSECURITY CHALLENGES AND STRATEGIES. *Engineering Science & Tecnology Journal*, *5*(2), 496–506. https://doi.org/10.51594/estj.v5i2.827

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

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