James Madison Undergraduate Research Journal

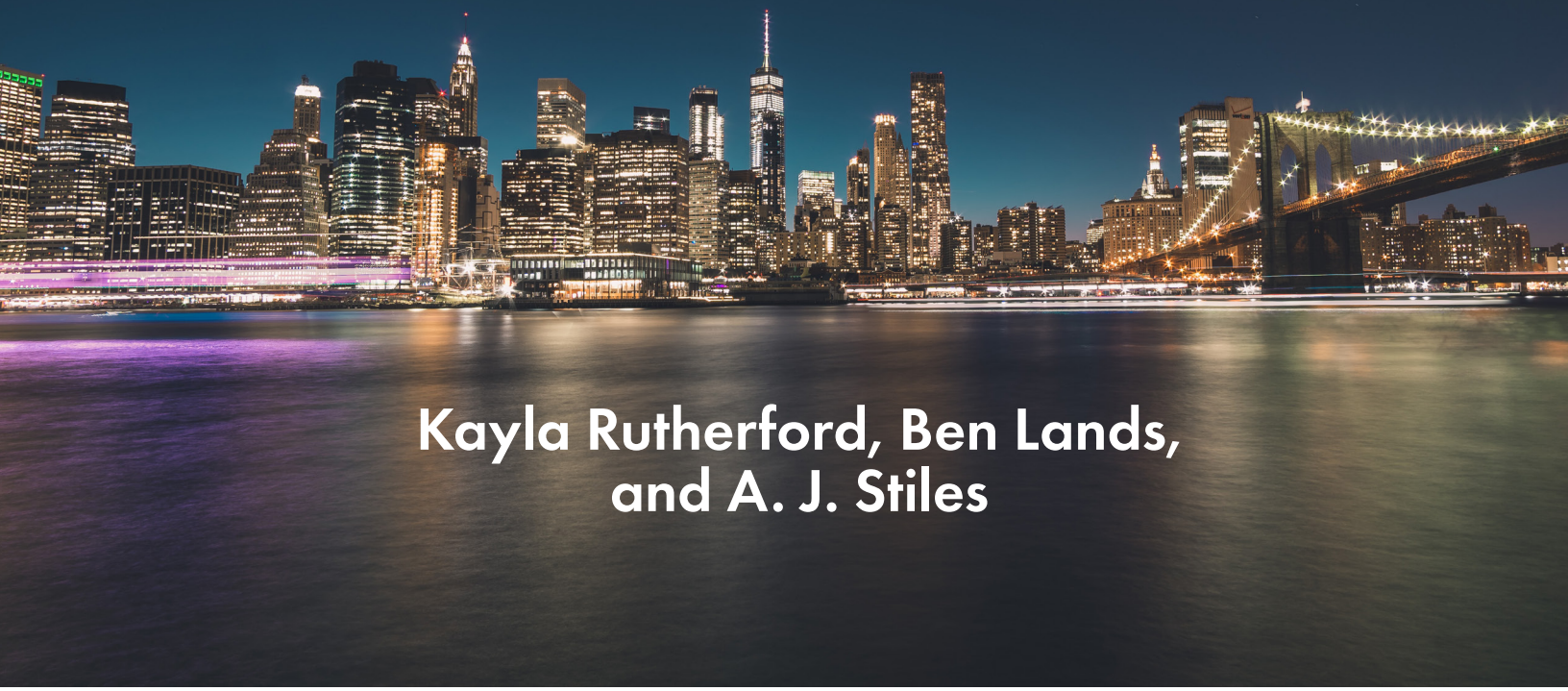
Volume 7 | Issue 1

2019-2020

An Analysis of Technological Components in Relation to Privacy in a Smart City

Kayla Rutherford, Ben Lands, and A. J. Stiles
James Madison University

An Analysis of Technological Components in Relation to Privacy in a Smart City



Kayla Rutherford, Ben Lands, and A. J. Stiles

A smart city is an interconnection of technological components that store, process, and wirelessly transmit information to enhance the efficiency of applications and the individuals who use those applications. Over the course of the 21st century, it is expected that an overwhelming majority of the world's population will live in urban areas and that the number of wireless devices will increase. The resulting increase in wireless data transmission means that the privacy of data will be increasingly at risk. This paper uses a holistic problem-solving approach to evaluate the security challenges posed by the technological components that make up a smart city, specifically radio frequency identification, wireless sensor networks, and Bluetooth. The holistic focus in turn permits a set of technical and ethical approaches that can combat malicious attacks and enhance data security across the networks that drive smart cities.

1. Introduction

As cities become increasingly connected through smart technologies and as current big data collection practices continue to go unchecked, information privacy has the potential to diminish. If procedures on data handling and security are not standardized early in the implementation of cyber-physical systems and Internet of Things (IoT) systems, then privacy gaps and invasive data mining will likely arise. These threats have the potential to affect the advancement of smart cities, as citizens may feel their privacy rights are unduly compromised, which in turn may undermine public support. In order to protect the right to privacy from invasive attacks on vulnerable networks and devices in emerging smart cities, solutions that address both social and technical aspects of the issue must be devised and analyzed.

Smart cities are a collection of interconnected technologies that can communicate with one another to monitor, collect, interpret, and distribute data. These entwined devices make up the IoT, a global network of wirelessly-connected devices. A smart city is constructed of a network-based foundation that contains appliances and infrastructures that in turn contain sensors, software, and electrical components. The broader purposes of smart cities vary from customer convenience to power reduction. The technological foundation of smart cities rests on three primary elements: radio frequency identification (RFID) for identification and tracking, wireless sensor networks (WSN) which are stand-alone networks for measuring data, and Bluetooth for connecting separate devices.

To understand and develop a solution to a problem, one must understand the complexity of its dimensions. This is done through holistic problem solving, an approach for examining elements, relationships, and the system dynamics of a complex problem. According to the Penn State College of Agricultural Sciences (n.d.), a complex problem, also known as a "wicked" problem, cannot be solved by a single solution. The problem with privacy in a smart city is complicated because of the value placed on privacy, as well as the technological underpinnings within such cities. Multiple stakeholders with different levels of interest, connection, and power shape the problem. Data security may be presented in many alternative methods, so a single solution will be insufficient to address the various interests of stakeholders.

The first step of a holistic approach, and the focus of this paper, is to determine the problem through framing. Framing is describing and interpreting the problem by choosing which aspects to prioritize and which to leave in the background. Framing lessens the complexity of the problem by narrowing the scope to a specific area of interest, and thus allows for a more scientific problem statement (Bartee, 1973). Potential solutions must then be analyzed holistically to determine their effectiveness and to understand how they will impact the various stakeholders.

The larger problem is how to ensure users' rights to privacy in a growing technological world. Using a holistic problem-solving approach, this paper identifies technical solutions that employ existing and emerging RFID, WSN, and Bluetooth technologies, along with policy solutions that begin to address the social and ethical issues involved in building smart cities.

2. Framing the Issue

2.1 Smart Cities and Privacy

Smart cities are designed to improve the lives of citizens by creating an environment that continuously adapts and monitors data collection (Cui et al., 2018; Eckhoff & Wagner, 2018; Sookhak et al., 2019). Amsterdam implemented its smart city plan with the intent of reducing CO_2 emissions among infrastructure and people through smart building management systems, ship-to-grid power connections, and climate streets that feature LED lights, waste reduction systems, and smart meters (Šťáhlavský, 2011; Alaverdyan, 2018). Vienna proudly advertises its commitment as a smart city to "digital data (mined using state-of-the-art technologies and analytical methods) to support decision-making and for real-time management of urban systems" (Stadt Wien, n.d.). China alone has more than 200 smart city plans in progress (Cui et al., 2018).

In these cities, multiple data sources from different data holders, devices, and applications can be combined to achieve city efficiency. However, doing so increases the risk of information being intercepted, which can have severe consequences (Eckhoff & Wagner, 2018). Applications which can collect highly sensitive data like citizen location or private documents may be used by system hackers (Sookhak et al., 2019). For instance, the Dyn company was hit with denial-of-service attacks in 2016 that saturated its infrastructure and disrupted host services (Khatoun & Zeadally, 2017). Additionally, a 2015 study demonstrated that a 2014 Jeep Cherokee could be hacked and controlled wirelessly by exploiting the vehicle's Uconnect system (Miller & Valasek, 2015). This shows that the harm of infringing on someone's privacy—for example, by locating an individual within a particular vehicle—can be immediate and physical.

2.2 Privacy and Security

Privacy is jeopardized by malicious attacks. There are two primary types of attacks: physical and system. Physical attacks take advantage of a device in a physical manner and are not associated with network intervention. Examples of physical attacks include disabling devices, modifying devices, and cloning tags (Khattab et al., 2017). System attacks use malicious software to acquire information (Attacks, 2015). There are several common types of system attacks:

- Spoofing - impersonating another individual or computer system
- Insertion - sending new messages from a host
- Replay - repeating or delaying data
- Relay - intercepting/manipulating messages between two parties
- Denial-of-Service (DoS) - disrupting services of a network-connected host
- Skimming - capturing information from a cardholder

3. Smart City Technologies

3.1 RFIDs, WSNs, and Bluetooth

While privacy issues are raised by data collection practices used by smart cities and the companies they support, problems may also occur through potential security breaches. Smart cities track the identity and movement of objects through RFID tags, which combine a microchip and an antenna to store, process, and then relay or actively send data (Dominikus & Kraxberger, 2011; Juels et al., 2003). Data in RFID tags is processed and sent through a vulnerable wireless network that connects each tag to its reader (Singh, 2013). The reader sends an electromagnetic wave that drives the internal circuit of the tag to send data to the user if the signal is strong enough (Singh, 2013).

Tracking and identifying objects within a smart city is necessary to provide inventory accuracy, advanced security, and efficiency for everyday usage. For instance, RFID tags are used for monitoring and analyzing locations, such as a greenhouse environment, or information stored on health devices (Subramanian et al., 2005). RFID tags can also be used to gain access to a compound or facility because the reader is able to locate the corresponding tag to gain access. The tags function in the same manner in cases that require bus entry, card access, or personnel tracking. RFID tags are also capable of detecting small concentrations of explosives and other dangerous chemicals (Subramanian et al., 2005).

Smart cities may also rely on WSNs, spatially diverse collections of sensors that monitor and gather data through connecting networks to support a range of operations (Conti, 2016). These operations include surveillance, rescue support, fire prevention, and air pollution monitoring (Conti, 2016). WSNs have a vast range of sensor nodes and data storage receivers that can monitor physical and environmental conditions.

Additionally, smart cities may use Bluetooth technology to transfer data between devices. Bluetooth is based on a primary/replica relationship between devices. This means that one device has unidirectional control over the other. Using this relationship, Bluetooth can create ad hoc short-range networks whose wireless traffic can be observed by malicious users within a densely populated area. Securing this wireless communication can increase the privacy individuals have when communicating on these channels.

3.2 Privacy Implications

RFID tags are inexpensive, and connecting them to the IoT is relatively easy; however, security protocols and frameworks must be analyzed to secure the data transmission within a network. Due to the use of these tags in a connected city, data must be secured properly to prevent hacking. RFID tags store information as well as track and monitor objects or people. This can result in a violation of one's privacy if this information is obtained. However, due to the constraints of RFID tags, such as limitations in memory size, energy, and response time, only specific security protocols can be implemented (Dominikus & Kraxberger, 2011). RFID tag memory can be increased, but it would be costly. Currently, RFID tags can hold an average of 64 kB of data depending on the type of tag (Dominikus & Kraxberger, 2011). According to Dominkus and Kraxberger (2011), these limitations of memory "could be a problem for the proposed security layer protocols" (p. 2647).

Security protocols can be different for the different types of RFID tags available: active, semi-active, and passive. Active and semi-active tags are powered by a battery; however, active tags automatically send information while semi-active remain dormant until receiving a reader signal (Dominikus & Kraxberger, 2011). In contrast, passive tags do not have a power source and require energy from the reader to send information (Dominikus & Kraxberger, 2011). Each of these tags has different byte sizes and ranges to account for when looking at its security framework (Singh, 2013). Because passive tags hold less memory and are cheaper to produce, they are more susceptible to attacks compared to active and semi-active tags (Singh, 2013).

WSNs provide high accessibility to data flows, but the "open" nature of the channel makes them prone to hacking (Khan & Mauri, 2014). WSNs are multivariate, meaning they are immune to computer attacks, which increases their security. However, adding mobility to any technology increases its vulnerability to security threats. Data is sent over the network with a larger range, increasing the time it takes for data to be received.

With any technical device, there are constraints on its security implementation. That is to say, all security devices have resource requirements. For WSNs, there are limitations such as memory and power. The memory of a WSN can only hold 178 bytes for code storage in a TelosB with a 10K RAM, 48K program memory, and 1024K flash storage, thus providing limited storage for implementing security protocols (Conti, 2016). Additionally, encryption, decryption, and the transmission and storage of security data all consume power. This energy consumption limits the life span of the node (Khan & Mauri, 2014). Multi-hop routing, network congestion, and node processing can lead to greater latency in the network (Conti, 2016). High latency makes it difficult to achieve synchronization among sensor nodes.

Bluetooth Low Energy (BLE) can be a cost-, time- and energy-efficient way of securely pairing mobile devices within a smart city where they are able to join or leave a network dynamically (Garcia, 2018). The security of each device is essential to the security of the entire network. If the devices of a network are not endowed with the same level of security, this creates a backdoor which can allow malicious activity to enter the network. Malicious attacks can cause technologies to be susceptible to detailed scans exposing informational parameters, service profiles, or even personal data (Haase & Handy, 2004).

4. RFID Technical Solutions

If smart cities rely on RFID technologies, as is expected, security measures must be analyzed to ensure that data being sent over a wireless network is secure. Sensitive data is often found in devices that track information on an object, provide access to facilities, and transmit across the network. Security solutions have been devised at both the network and physical levels.

4.1 RFID Authentication and Eavesdropping

At the network level, RFIDs need to be authenticated properly to prevent hackers from eavesdropping on data transmission.One suggestion has been to make "Smart RFID" tags that generate their own random pseudo IDs so that a passive eavesdropper cannot encrypt the signal being sent by the reader (Juels et al., 2003; Sobti & Geetha, 2012). In this approach, A-TRAP protocols exchange three values generated pseudo-randomly between the tag and server (Le et al., 2007). The server checks to ensure that a designated value is in the database before accepting the tag as authentic. A-TRAP protocols offer "secure authentication, forward-anonymity, availability, and key-indistinguishability," but cannot withstand sustained attacks or instances when the tag is lost (Le et al., 2007, p. 13). Later proposed protocols generated four and five pseudo-random values to anonymize the communication between the server and the tag and to prevent replay attacks (Le et al., 2007). Despite the growing sophistication of these key mechanisms, as Avoine et al. (2011) pointed out a decade ago, they remain vulnerable to compromise in open communities with more open networks.

4.2 RFID Denial-of-Service Attacks

Connecting tags to the IoT system in a smart city makes them prone to attacks in an open network. One possibility is to use IPv6 to defend RFID tags against DoS attacks (Dominikus & Kraxberger, 2011). IPv6 is the most recent version of the Internet Protocol, and it uses 128-bit addresses to identify and locate devices on the network and route traffic across the Internet (Dominikus & Kraxberger, 2011). According to Dominikus and Kraxberger (2011), a reader could track the communication with a mobile IPv6-enabled tag while also blocking attacks from suspicious nodes. Timeout values, which end one connection and accept new connection attempts, can also be randomized to defend against hackers.

4.3 Physical Solutions to RFID Attacks

The ability to "kill" RFID tags when a good is purchased can be useful because dead RFID tags cannot collect consumer data (Juels et al., 2003). Similarly, the ability to put RFID tags to sleep allows users to turn tags on and off when desired (Sitlia et al., 2009). A more secure method of defending against physical attacks is through blocker tags. Blocker tags are RFID tags that can block readers from reading the identification of tags that exist in the blocker tag's range (Juels et al., 2003; Sitlia et al., 2009).

5. WSN Technical Solutions

Wireless sensor networks continuously monitor an environment to gather and organize sensitive information regarding city infrastructure. If this data were intercepted or if the technologies were hacked, one could obtain control over a spatial environment. Solutions have been devised to secure these technologies and their data.

5.1 WSN Authentication and Confidentiality

Public-key cryptosystems are an effective method for securing WSN authentication and confidentiality. Some of the major techniques used in public-key cryptosystems are the Rivest, Shamir, and Adleman scheme (RSA), Elliptic Curve Cryptography (ECC), and Multivariate Quadratic Quasigroups (MQQ) (Gligoroski et al., 2008). Each of these techniques provides different efficiency, security, and memory usage, shown in Table 1. The design of ECC is tough to develop, but its complexity makes the system difficult to crack (Quirino et al., 2012).

Table 1: *Public-Key Cryptosystem Comparisons*

	RSA	ECC	MQQ
Current Implementations and Uses	Widely used for transactions on the Internet Can be used to encrypt and create digital signatures	Primarily developed for solving discrete logarithm problems on elliptic curves	Has a system of multivariate quadratic polynomials over a finite field as a public key
Processing Characteristics	Slower processing Enciphering consumes more time than deciphering	Equivalent time of encryption and decryption Energy efficient	Fastest processing time Enciphering consumes more time than deciphering
Memory Characteristics	More memory required compared to ECC and MQQ	Consumes less memory and processing resources	Economical in memory consumption

Note. Adapted from "Asymmetric Encryption in Wireless Sensor Networks" by G. Quirino, A. Ribeiro, and E. Moreno, 2012, (https://doi.org/10.5772/48464).

5.2 ECCE Protocol

One experimental solution for WSN security concerns proposed by Conti et al. (2007) is an Enhanced Cooperative Channel Establishment (ECCE). The purpose of this protocol is to allow a secure wireless channel between two sensors that do not share any pre-deployed key (Conti et al., 2007). According to Conti et al. (2007), "in comparison with other protocols, ECCE performs effectively in "channel existence and channel resilience" when faced with an attacker (p. 61).

5.3 SPINS

A third solution is the use of SPINS, a secure communication protocol proposed by Perrig et al. (2002) that prevents eavesdropping and active attacks in wireless sensor networks. There are "two secure building blocks" associated with the SPINS protocol: SNEP and μTesla (Perrig et al., 2002, p. 521).

Secure Network Encryption Protocol (SNEP) uses a two-party authentication protocol that provides confidentiality between the two corresponding parties (Perrig et al., 2002). A common protocol used for data authentication is the Message Authentication Code (MAC), which sends a message and a signature (Ullah et al., 2009). When the message has been obtained, the receiver performs a computation on the message and compares the generated message's MAC value to the sent MAC value to determine if the message is from a legitimate user (Ullah et al., 2009). This process makes it feasible to use the SNEP protocol for the network system. SNEP "has low communication overhead" and "only adds 8 bytes per message" (Perrig et al., 2002, p. 524). Therefore, it wouldn't take up too many resources to use this protocol in a wireless sensor network.

μTesla, an experimental, "'micro' version of the Timed Efficient Streaming Loss-tolerant Authentication protocol (TESLA), [provides] authenticated screening broadcast" (Ullah et al., 2009, p. 333). μTesla uses asymmetry through a delayed disclosure of symmetric keys, which results in an effective broadcast authentication scheme (Ullah et al., 2009). Asymmetric cryptographic mechanisms by themselves are resource-intensive and require a significant amount of computation (Perrig et al., 2002). By using μTesla, this issue can be efficiently resolved.

6. Bluetooth Technical Solutions

There are two key Bluetooth protocols: traditional Bluetooth and Bluetooth Low Energy (BLE). Bluetooth resides within the IEEE 802.15 protocol family dedicated for personal area networks (i.e., the networks for connecting an individual person's devices). If Bluetooth is to be implemented within smart cities on a wide scale, traditional Bluetooth will not suffice. Traditional Bluetooth design requires one watt of power consumption and operates at a data transmission rate of 25 Mbps while BLE is ~2 Mbps (Bulíc et al., 2019). Unfortunately, a reduced capacity for security follows suit with this reduced data transmission rate and lowered power consumption, similar to most wireless device communications.

During the pairing process, devices exchange their specific security and functionality capabilities. If the device-relative

capabilities are supported, the primary device will generate a temporary key, which will be used to produce the short-term key. The short-term key is then used to encrypt the data transferred between devices.

By contrast, the bonding process does persist across connections between devices to bypass the pairing phase on subsequent connections. In order to bond two devices to each other, they must engage in an initial pairing process. Bonding uses a long-term key stored on each device to encrypt the communication channel between them.

The different levels of security for Bluetooth depend on the capabilities of each device. If Bluetooth v4.2 or later is used, then the connection can be further secured, though not 100% secured. BLE v4.2 offers an enhanced security process utilizing the Diffie-Hellman algorithm, which allows two devices to generate a shared key on each side. Still, the security of the locally stored keys is imperative to BLE security (Kainda et al., 2009).

Unfortunately, Bluetooth devices authenticate devices rather than the users of devices. To investigate and enhance user authentication, a study was conducted in 2009 to test the usability of different methods for pairing secure devices (Kainda et al., 2009). Kainda et al. (2009) found that the "Compare & Confirm" method shown in Table 2 is the easiest for users to interface with as they pair unfamiliar devices. In addition, no security failures arose during the study using the "Compare & Confirm" method, suggesting that it is promising for increasing security (Kainda et al., 2009).

To help the general public realize that these low energy devices result in low security, they should be informed of their vulnerabilities. However, the public should also be made aware of possible methods for securing Bluetooth devices.

When pairing Bluetooth devices, Out-of-Band (OOB) channels should be implemented with personal identification numbers as opposed to link keys. This approach should prevent persistent man-in-the-middle attacks in an open environment where attackers can snoop for keys sent between devices. Additionally, these PINs should be set to a longer value that includes both letters and numbers. However, this technique would be restricted to devices which have displays.

An active attack increases the amount of power it consumes as a result of the increased traffic it receives and potentially distributes. Even if the attack is unsuccessful, the increased power consumption renders the targeted device offline, thereby reducing the capabilities of the Bluetooth network. Restricting a device's power consumption rate will reduce the propensity for this issue to occur.

Table 2: *Potential Bluetooth Pairing Methods*

Mechanism	Description
Compare & Confirm	A user compares strings, sounds, melodies, or images displayed on both devices and presses a button to indicate a match or a disparity
Compare & Select	A string is displayed on one device and four strings of the same format are displayed on the other device.
Copy & Enter	A device displays a string while the other asks the user to enter the same string
Barcode	One device displays a QR code while the other automatically activates its camera function and asks the user to point the camera at the QR code and take a snapshot of it.

Note. Adapted from "Usability and Security of Out-of-Band Channels in Secure Device Pairing Protocols" by R. Kainda, I. Flechais, and A. Roscoe, 2009, (https://doi.org/10.1145/1572532.1572547).

7. Ethical Frameworks for Privacy and Cybersecurity

The big questions concerning the ethics of big data not only pertain to what information is being collected, but also "who and what is subjected to analysis" (Crawford et al., 2014, p. 1666). That is, might some people be subjected to more scrutiny than others? Questions of justice must be considered when the benefits and risks of data collection in a smart city are unevenly distributed.

One issue with big data is the ability to link specific information with an identity. However, if an identity is not associated with information, is it ethical to use this data for analysis? The answer may vary depending on whether it serves civil, commercial, or private interest. Civil interest would include, for example, estimating the number of people by pinging devices for public transportation in the

interest of efficiency. This would not link identity, but rather the number of devices in a specific location.

Commercial interest describes collecting and analyzing data for a profit motive, which may include using Internet browsing history and recent purchases to predict what a user would most likely be interested in. This practice links an identity to data, which could be deemed unethical depending whether the practice is transparent and done with user consent. Ethical dilemmas regarding data analysis will be raised by smart cities. It is important for the public to assess the dangers of unethical data usage early on in the development of smart cities so that policymaking does not lag too far behind the technological advancement these cities will bring. Once smart cities are already built, it will be much more difficult to rethink how they address privacy.

8. Policy Approach

Smart cities are still in the early stages of development. This means that privacy and security concerns will continue to arise, but it also means there is an opportunity now to build smart cities with stakeholders' interests in mind. The severity of privacy issues will depend on how smart cities are governed. In this section, we weigh the best policy scenarios for a developing smart city.

Smart cities will involve vast amounts of information, processed by artificial intelligence or people for the sake of learning individual or societal trends. This information will be analyzed for a range of purposes, from running more efficient in-city transportation to supporting company profit motives (Walker, 2019). Private information, such as one's daily routine, hobbies, and interests, could be acquired by different actors for different purposes. Unlike traditional urban areas, "smart cities have become data-centric projects focusing on the constant generation, collection, and processing of data" (What Are Smart Cities?!, 2008). With information constantly relaying from device to device, proper security protocols and management of this information needs to be regulated by governing entities to ensure privacy and security for citizens, companies, and governments are maintained.

There is a growing push to regulate data for privacy purposes. For example, there is a movement within the United States "calling on the federal government to create an entirely new federal agency tasked with data privacy protection" (Krishan, 2019). An approach in the context of smart cities would be to create mandatory government authorizations to handle different types of information. Additionally, there should be rules and procedures governing the use and sharing of data. A state level government agency should oversee data flow along with issuing these authorizations to ensure local control in the smart city developing process. Its purpose would be to inspect and investigate companies suspected of illegal information practices. This will make data harder to obtain while also punishing individuals or companies who mishandle it.

Table 3: *Data Priority Tiers*

Tier Level	Description
Tier 1	Involves data that is not linked to an identity. This would be the least sensitive type of data.
Tier 2	Includes data linked to an identity. The higher tier would prevent unauthorized access to someone's social media account, web history, location, etc.
Tier 3	Deals with encrypted information. Breaching unauthorized encrypted data should be looked at as a major offense.
Tier 4	Deals with encrypted information. Breaching unauthorized encrypted data should be looked at as a major offense.

Note. Adapted from "District of Columbia Data Policy" by Office of the Mayor, April 27, 2017, (https://octo.dc.gov/sites/default/files/dc/sites/octo/page_content/attachments/2017-115_District-of-Columbia-Data-Policy.pdf).

Data makes a smart city function. Therefore, it is important to help the public recognize that not all data has the same level of sensitivity. To do this, data could be classified into tiers like those displayed in Table 3. Smart cities might consider creating data regulatory agencies to oversee this classification system. As Washington D.C. has done with its dataset classification levels, higher tiers could correspond to greater security risks and greater offenses if information is mishandled or stolen (Office of the Mayor, 2017). For example, Tier 1 could include data not linked to individual identity. The data regulatory agency might determine that accessing this tier of data does not need authorization except for specific cases. de Groot (2019) summarizes three principles for classifying data: context, content, and user. Context-based classification looks for sensitive information; content-based classification

"looks at application, location, or creator," and user-based classification "relies on user knowledge and discretion at creation, edit, review, or dissemination" (de Groot, 2019).

Authorizations to handle this information would be issued by the data regulatory agency. These authorizations would ensure proper care for the different types of data and hold those accountable who use it incorrectly or jeopardize its privacy/integrity. The agency could also coordinate inspections to make sure companies and other entities are complying with proper data protocols.

Predicting the future outcomes of a smart city will steer development as well. A societal shift concerning the importance of data must be viewed as an important step in smart city development. An informed public should be the first step toward protecting privacy. Smart cities involve uncertainties which means many legislative decisions may be made in a reactive manner; however, steps can be taken to proactively protect privacy at this early stage of development. This can be done through planning and the construction of a data governing framework. This should push the citizens affected by the new framework to better understand the system and what it means for them.

9. Conclusions

Smart cities prioritize efficient systems over privacy. This will continue to be the case "as the amount of data gathered via the IoT continues to grow" (Newman, 2019). Privacy will always be a major concern in smart cities due to the vast collection of data through many systems. Many of these systems link identity with the data. This poses a threat to privacy and raises questions: Who owns and analyzes this data, and, as Newman (2019) asked, "At what point does the data collection become too much?" and "When is privacy more important than convenience?"

With a society that is constantly connected to a network, privacy will be a concern due to the prevalence of data breaches and hackings. Devices constantly collect and analyze data whether citizens have agreed to it or not. To implement security practices that ensure data integrity and confidentiality, a holistic analysis is required to understand the interconnected systems that collectively comprise a smart city. If a holistic approach is not taken, many "well-intentioned efforts [could] lead to policy resistance, where our policies are delayed, diluted, or defeated by unforeseen reactions" (Sterman, 2000). Additionally, while technical solutions can address and even anticipate hackers' security attacks, only policy planning can control how data will collected and design how it will be used.

Complex problems rarely have simple solutions; therefore, it is important to assess all dimensions of a smart city before implementing change. It is also important to understand what these changes might do to the system because none of the proposed solutions work independently from one another. They are all a part of the same system to combat the interference of hacking and the invasion of privacy. Due to the complex nature of the problem, technical and regulatory solutions must be devised to work hand in hand to protect privacy as smart cities progress.

Authors' Note

Kayla Rutherford ('20) graduated with a degree in Integrated Science and Technology and a concentration in Energy and Environment. She is currently pursuing her master's degree in Environmental Engineering at Old Dominion University. She loves hiking, kayaking, or any other activity that involves exploring the outdoors. She was a member of the JMU Club Quidditch team; she helped found JMU's Theta Tau Colony and served as President during the 2019-2020 year.

Not pictured: Ben Lands and A. J. Stiles

References

Alaverdyan, D., Kučera, F., & Horák, M. (2018). Implementation of the smart city concept in the EU: Importance of cluster initiatives and best practice cases. *International Journal of Entrepreneurial Knowledge*, *6*(1), 30-51. https://doi.org/10.2478/ijek-2018-0003

Avoine G., Coisel I., Martin T. (2010) Time measurement threatens privacy-friendly RFID authentication protocols. In S. B. O Yalcin (Ed.), *Radio frequency identification: Security and privacy issues* (pp. 138-157). Springer. https://doi.org/10.1007/978-3-642-16822-2_13

Attacks on computer systems. (2015, November 25). *Australian Cybercrime Online Reporting Network*. https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems

Bartee, E. (1973). A holistic view of problem solving. *Management Science*, *20*(4), 439-448. https://doi.org/10.1287/mnsc.20.4.439

Bulíc, P., Kojek, G., & Biasizzo, A. (2019). Data transmission efficiency in Bluetooth Low Energy versions. *Sensors*, *19*(17). https://doi.org/10.3390/s19173746

Conti, M. (2016). *Secure wireless sensor networks: Threats and solutions*. Springer-Verlag New York. https://doi.org/10.1007/978-1-4939-3460-7

Conti, M., Di Pietro, R., & Mancini, L. V. (2007). ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. *Ad Hoc Networks, 5*(1), 49-62. https://doi.org/10.1016/j.adhoc.2006.05.013

Crawford, K., Gray, M. L., & Miltner, K. (2014). Critiquing big data: Politics, ethics, epistemology: Special section introduction. *International Journal of Communications*, *8*, 1663-1672. http://ijoc.org/index.php/ijoc/article/view/2167/1164

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access, 6*, 46134-46145. https://doi.org/10.1109/ACCESS.2018.2853985

de Groot, J. (2019, July 15). What is data classification? A data classification definition. *Digital Guardian*. https://digitalguardian.com/blog/what-data-classification-data-classification-definition

Dominikus, S., & Kraxberger S. (2011). Secure communication with RFID tags in the Internet of Things. *Security and Communication Networks*, *7*, 2639–2653. https://doi.org/10.1002/sec.398

Eckhoff, E., & Wagner, I. (2018). Privacy in the smart city—Applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials, 20*(1), 489-516. https://doi.org/10.1109/COMST.2017.2748998

Garcia, L., Jiménez, J., Taha, M., & Lloret, J. (2018). Wireless technologies for IoT in smart cities. *Network Protocols and Algorithms, 10*(23), 23-64. https://doi.org/10.5296/npa.v10i1.12798

Gligoroski, D., Markovski, S., & Knapskog, S. J. (2008). *A public key block cipher based on multivariate quadratic quasigroups.* https://eprint.iacr.org/2008/320.pdf

Haase, M., & Handy, M. (2004, September 7-10). *BlueTrack–Imperceptible tracking of Bluetooth devices [Poster Presentation].* Conference on Ubiquitous Com-puting, Nottingham, England. http://www.ubicomp.org/ubicomp2004/adjunct/posters/haase.pdf

Juels, A., Rivest, R., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. *Proceedings of the 10th ACM conference on computer and communications security.* https://doi.org/10.1145/948109.948126

Kainda, R., Fléchais, I., & Roscoe, A. W. (2009). Usability and security of out-of-band channels in secure device pairing protocols categories and subject descriptors. *SOUP's '09: Proceedings of the 5th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/1572532.1572547

Khan, S., & Mauri, J. L. (Eds.). (2014). *Security for multihop wireless networks.* CRC Press.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*(3), 51-59. https://doi.org/10.1109/MCOM.2017.1600297CM

Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M. (2017). *RFID security threats and basic solutions.* In RFID security: A lightweight paradigm. (pp. 27-41). Springer International Publishing.

Krishan, N. (2019, January 18). Consumer groups want a new government agency created to protect data privacy. Mother Jones. https://www.motherjones.com/politics/2019/01/consumer-groups-want-a-new-government-agency-created-to-protect-data-privacy/

Le, T. V., Burmester, M., & de Medeiros, B. (2007). *Forward-secure RFID authentication and key exchange.* IACR Cryptology ePrint Archive. https://eprint.iacr.org/2007/051.pdf

Miller, C., & Valasek, C. (2015, August 10). *Remote exploitation of an unaltered passenger vehicle.* Illmatics. http://illmatics.com/Remote%20Car%20Hacking.pdf

Newman, D. (2019, January 23). *Are privacy concerns halting smart cities indefinitely?* Futurum. https://futurumresearch.com/privacy-concerns-for-smart-cities/

Office of the Mayor. (2017, April 27). *District of Columbia data policy*. https://octo.dc.gov/sites/default/files/dc/sites/octo/page_content/attachments/2017-115_District-of-Columbia-Data-Policy.pdf

Penn State College of Agricultural Sciences. (n.d.). *Complex or "wicked issues."* https://aese.psu.edu/research/centers/cecd/engagement-toolbox/problems/complex-or-wicked-issues

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, *8*(5), 521-534. https://doi.org/10.1023/A:1016598314198

Quirino, G. S., Ribeiro, A. R. L., & Moreno, E. D. (2012). Asymmetric encryption in wireless sensor networks. In M. A. Matin (Ed.), *Wireless sensor networks: Technology and protocols.* (pp. 217-232). http://dx.doi.org/10.5772/48464

Singh, K. (2013). Security in RFID networks and protocols. *International Journal of Information and Computation Technology*, *3*(5), 425-432. http://www.irphouse.com/ijict_spl/10_ijictv3n5spl.pdf

Sitlia, H., Hamam, H., & Selouani, S. A. (2009). *Technical solutions for privacy protection in RFID.* https://www.researchgate.net/publication/242605065

Sobti, R., & Geetha, G. (2012). Cryptographic hash functions: A review. *International Journal of Computer Science Issues, 9*(2), 461-479. https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2019). Security and privacy of smart cities: A survey, research issues and challenges. *IEEE Communications Surveys & Tutorials, 21*(2), 1718-1743. https://doi.org/10.1109/COMST.2018.2867288

Šťáhlavský, R. (2011, May 24). *Amsterdam Smart City project* [Slides].http://www.top-expo.cz/domain/top-expo/files/tee/tee-2011/prednasky/prednasky%202.%20den/2-3%20stahlavsky%20roman%20-%20amsterdam%20smart%20city%20project.pdf

Sterman, J. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. McGraw-Hill Education.

Stadt Wien (n.d.). *The dimensions, headline goals and thematic fields of the Smart City Wien Framework Strategy.* https://smartcity.wien.gv.at/site/files/2020/05/SCWFS_objectives_overview.pdf).

Subramanian, V., Frechet, J. M. J., Chang, P. C., Huang, D. C., Lee, J. B., Molesa, S. E., Murphy, A. R., Redinger, D. R., & Volkman, S. K. (2005). Progress toward development of all-printed RFID tags: Materials, processes, and devices. *Proceedings of the IEEE*, *93*(7), 1330-1338. https://doi.org/10.1109/JPROC.2005.850305

Ullah, F., Mehmood, T., Habib, M., & Ibrahim, M. (2009, July 10-12). *SPINS: Security protocols for sensor networks.* International Conference on Machine Learning and Computing, Perth, Australia. https://www.researchgate.net/publication/312626436_SPINS_Security_Protocols_for_Sensor_Networks

Walker, J. (2019, January 31). *Smart city artificial intelligence applications and trends.* Emerj. https://emerj.com/ai-sector-overviews/smart-city-artificial-intelligence-applications-trends/

What are smart cities?! (2018, May 4). Privacy International. https://privacyinternational.org/explainer/1864/what-are-smart-cities