smart cities

MDPI

Communication

The Emergence of Anti-Privacy and Control at the Nexus between the Concepts of Safe City and Smart City

Zaheer Allam

Curtin University Sustainability Policy Institute, Curtin University, Perth, WA 6845, Australia; zaheerallam@gmail.com

Received: 13 February 2019; Accepted: 7 March 2019; Published: 11 March 2019

Abstract: The emergence of Big Data, accelerated through the Internet of Things (IoT) and Artificial Intelligence, from the emerging, contemporary concept of smart cities coupled with that of the notion for safe cities is raising concerns of privacy and good governance that are impacting on socio-economic and liveability dimensions of urban fabrics. As these gain ground, largely due to economic pressures from large ICT providers, there is a notable increase towards the need for inclusion of human dimensions, complemented by the use of technology. However, the latter is seen as catalysing elements of control and propaganda which are thriving through oversimplified and non-inclusive urban IT policy measures. This paper dwells on the intersecting subjects of smart and safe cities and explores the highlighted issues that are deemed to cause concern and further explore the need for transparency and inclusivity in urban processes and systems. This paper is oriented towards urban planners and policy makers looking at the implementation of smart and safe cities concepts.

Keywords: safe city; smart city; anti-privacy; liveability; propaganda; transparency

1. Introduction

Increasing conflicts in urban areas, coupled with an increasing urbanisation rate, is prompting new models for urban management and policing. Sarkar [1] expresses that the conflicts are facilitated by inequalities that range from skewed provision of basic services with inequitable policies, often oriented towards the urban poor. The same case is true with the availability of housing opportunities, education and economic opportunities amongst others. Moser and Mcilwaine [2] posit that these challenges have the potential to spurt different forms of conflicts and violence in cities as the surging population try to access limited resources [3]. The escalation of these challenges, thus affecting social, political and economic and environmental stability call for a change in the traditional ways in handling the security affairs of urban areas [4]. Amongst models that have been deemed potent is the concept of the safe city; which is rapidly gaining ground in many countries. Lacinák and Ristvej [5] note that the concept of safe city is explored with an aim of advancing the security status of cities by addressing issues like increasing urban conflicts, institutional and social crimes and in preventing violence prompted by factors like forced evictions, land conflicts and scramble for limited resources in the city. The authors also argue that the concept encapsulates preventive measures on environmental degradation and safety concerns arising from increasing natural disasters like flooding and extreme heat waves. By leveraging on technologies such as predictive analytics, Big Data and others that are enabled by IoT; which stands as the foundational structure of the concept of smart cities, the above safety and security concerns are better addressed, making cities safer.

Tripathi [6] posit that, in the majority of these cities, the safe city concept is promoted as being able to help achieve safety, security and privacy in cities amongst other things; hence, a plethora of

strategies are employed to achieve it. These strategies often include a paradigm shift to smart cities where different urban components and fabrics are interlinked through the help of ICT and a wide array of advanced technologies such as the Internet of Things (IoT) [7,8], Artificial Intelligence (AI) [9], Big Data [10,11] and Blockchain technology [12] amongst others [13]. In particular, the concept of smart cities is hailed for the emphasis on different smart sensors, cameras and other smart devices in various areas that help in capturing vital data paramount in securing both human and emerging patterns within cities. These devices make it possible for different agencies and stakeholders to gather and analyse data in real-time and in return, take quick action; hence promoting safety and the sense of privacy. Braun et al. [14] affirms that the availability of sensors and data from different sources, including from citizens themselves, have helped cities improve on their resilience, liveability and economic status and above all, on their safety indexes. IFSEC (International Fire and Security Exhibition and Conference) Global [15] support that, though the concept of safe city can be implemented as a standalone endeavour, it yields higher results where it has been implemented hand-to-hand with the concept of smart cities. This is particularly so, since smart city projects entail the deployment of a wide array of components generating substantial data, which is paramount in advancing safety and security but unequivocally presents challenges such as privacy concerns.

Though security is paramount and the aforementioned strategies have helped with improving and increasing urban safety, the concept of the safe city has not been universally embraced. Yigitcanlar et al. [16] argue that it has received a considerable amount of backlash from different quarters as questions related to its efficiency and its ability to compromise the privacy of individuals arise. The scathing questioning is especially pronounced in the case of smart cities [17–20]. There is an availability of numerous smart devices, enabled by IoT, that can be controlled remotely. But this is deemed by the critics as opening loopholes for intrusion into citizens' privacy by both ill-minded individuals and foreign agencies [21,22]. Privacy concerns also arise as people fear that Big Data, collected from different devices and that which is shared by different people and groups, could be used either by government agencies, individuals or third parties to gain access to sensitive personal data. Cui et al. [23] argue that though there are concerted efforts to secure devices and data gathered through such strategies like encryption, anonymity and the use of biometrics, the heterogeneity nature of protocols that each device and system use render them vulnerable to interference; hence, justifying the need for concern. The same view is maintained by Alomair and Poovendran [24], who explain that scalability and dynamic qualities of IoT architectures are not fool-proof to the tech savvy population that have the potential to bypass security measures guarding sensitive data and devices. Due to those direct security concerns, the safe city concept may face difficulties in its applicability as expressed by Mosenia and Jha [25]. Therefore, to ensure the success of both the safe city and smart city concepts, these underlying challenges need to be addressed to provide consumer confidence in regard to the security and safety of cities. This paper offers a perspective on the emerging challenges from the combined adoption of the two concepts.

2. The Safe City

According to PWC (Price Waterhouse Coopers) [26], a safe city could be defined as a system in place that ensures that citizens, business and properties, organisations and institutions are safe from both external and internal threats to their well-being. The emergence of this concept emerged by unconventional happenings in cities located in different geographical locations. At the beginning, as is explained by West and Bernstein [27], different cities, based on their specific issues, implemented their own strategies to combat the rising incidences of crime, violence and conflicts. PWC [26] express that the disparities and deprivations in cities lead to increased conflicts and crimes and also hamper any sustainable development agenda that may be in place. This prompts the need for spirited efforts to ensure that safety abounds in cities and that tranquillity driven by social, economic, environment is supported by appropriate policies [28]. These efforts are documented in the Sustainable Development Goals and specifically, SDG 11 dwells on the need to, among other things, focus on inclusivity, safety

and resilience in cities. This entails ensuring that citizens, organisations, institutions, properties and shared identities and cultures are secured from any forms of threats.

This is carefully done by leveraging on modern technologies and ICT, especially through the use of IoT, Big Data, Blockchain and Crowd Computing [29]. These technologies involve capitalizing on availability of numerous smart devices, sensors and social networks that generate valuable, Big Data, that when analysed, allow for the optimal use of time and tools to prevent, mitigate and respond to eminent threats. In the recent past, a sizeable number of safe city solutions have been developed and implemented [30]. A common approach includes the coupling of Video surveillance and Cloud Storage; which entails large-scale video networking across urban nodes or the entire urban fabric. As Ma et al. [31] explain, this concept has also been adopted in smaller urban developments and has allowed for quicker and efficient ways of extracting content from video recordings and for surveillance. This approach is supported by other technologies like the Wireless Broadband Trunking and working with 4G [32,33]. Different cities have also implemented Converged Command Centres where Data from different sources are received, analysed and relayed in real-time; prompting quick actions from informed decisions [34,35].

As noted above, despite their potential to increase the speed at which information is received and relayed to the relevant agency, citizens, who are the ultimate beneficiaries, are reported to be wary of their privacy. Elmaghraby and Losavio [36] explain how this approach is perceived as a government strategy to capture private data; hence, enforcing control. Alomair and Poovendran [24] also support that fears of citizens are also increased by the fact that digital systems have in the past, been infiltrated by hackers and unauthorized individuals and thus endangering whole urban systems [37]. As currently constituted, the managing of the safe city concept is also bound to encounter challenges especially in regard to control, partly because there is no uniformity in protocols that different devices rely on and there is a lack of centralized networks in many cities where data can be received and relayed. In most cases, cities have been observed to maintain multiple network servers, which adds to cost and complexity. Though the concept of safe city encapsulates numerous factors relating to safety, security and privacy, the concern in this paper is about reservations arising from its use by governments and private entities. A summary of identified related issues, as outlined in multiple documents, is presented in Table 1 below.

Table 1. Identified issues related to the safe city concept.

	Privacy	Control	Costs	Awareness	Propaganda	Privatisation
Alomair and Poovendran [24]	X					
Abouelmehdi, et al. [38]	X	X				
McKinsey and Company [39]	X			X		
Pinto [40]		X	X	X	X	
Lam and Ma [41]	X	X				
Martínez–Ballesté, et al. [42]	X	X				
Lim, et al. [43]	X	X		X		
Kummitha and Crutzen [44]		X		X		
van Zoonen [45]	X	X		X		
Grossi and Pianezzi [46]	X	X		X		X
Bhadani [47]						
Sun, et al. [48]	X	X				X
Anisetti, et al. [49]	X	X				X
Guerrini [50]		X	X		X	
Calzada and Cowie [51]	X	X		X	X	X

The term ‘awareness’ in the table entails the knowledge that citizens have about issues relating to private data collection and how such data is used by security agencies. A practical example is the city of Rio de Janeiro which had numerous cameras, smart devices and sensors capturing and gathering data including private data and sending it in real-time to security agencies. However, urban dwellers, including visitors, were not aware that they were being monitored in the various activities they were engaged in [52]. The term ‘propaganda,’ on the other hand, is used here to show the use of misleading

information to advance the idea of safe city at the expense of the citizen. This can be made to happen when the government supports a safe city project while, the project is financed and implemented by private entities like in the case of payphone transformation in NYC in what was called LinkNYC Kiosks [40]. The cost entails the financial budget that is incurred to fund the project.

It is understood that issues like personal privacy, use of data as a means of control and the lack of awareness of the way governments use collected data are concerns that challenges the adoption of the safe city concept. Other issues like privatization of the process; hence, delegate the use of data to third parties and the use of data for propaganda, though not widely documented, play a critical role in its adoption and acceptance.

3. The Smart City

Unlike the safe city, which has an almost universal definition, the smart city has numerous definitions but most of them converge at the point of interlinkage of city fabrics through the help of technology through the bias of 'smart' components and 'smart' systems. Amongst the advanced technologies that are employed in the management of urban centres is that of IoT, whose protocols and infrastructure have greatly benefited the concept of smart cities [18,20,53,54]. The availability and advancement of IoT technology has allowed the development of a wide variety of smart devices, sensors, social networks and systems [55,56]. All these components are integrated in the running, control and management of different aspects of urban fabric and since a majority of them are interlinked in one way or the other, they form a complex system rendering urban centres as 'Smart.' In particular, in the course of their operation and usage, a substantial amount of data that is captured, analysed and generated through Big Data technology, which allow different stakeholders in the management of the city to obtain unique insights as to how different fabrics interact with each other and, most importantly, with urban dwellers [13,17,19]. Those allow for real-time, efficient and cost-effective actions in addressing various urban issues. From data gathered, it is understood that a sizeable amount contains sensitive and personal data; which present itself as issue that does not augur well with the city dwellers, as expressed by Elmaghraby and Losavio [36]. The concern over personal data is more pronounced when it relates to finance or health information, since a majority portend that if the same falls into the hands of third parties, they can be used to jeopardize the livelihood, reputation or any other individuals' rights [57].

The primary notable issue is that the wide array of devices and components used to gather data are not solely controlled by the public sector but are often collected by large private companies [13,17,20], contracted by the governments. Those types of agreement are geared by Public Private Partnerships (PPP) which facilitate the installation and management of devices and processing of collected data [58]. As is evident in the work of Cruz and Sarmento [59], though the adoption of PPP structures is deemed as both an innovative and appropriate for the concept of smart cities to succeed in most economies, the citizens' reservations are justified since their data is not solely in the hands of the government but also in the hands of some private entities. According to these authors, for PPPs to work in the collection, analysis and management of these massive and sensitive data they require substantial restructuring. Edwards [60] explain that some PPP model for data management in smart cities also faces the challenge of lack of universal standards, hence, making it hard for the governments to have full control on the intended purpose of the data from the private sector. Boyer and Van Slyke [61] explain that, however, PPPs are not always well received by public, especially when agreements are not made public to facilitate the public awareness of role of the private sector with public data. Thus, the fear of perceived use of the collected data by companies for profit making has been a primary concern [62]. The argument is that the data need to be purely used for urban management and not profit making. Hamilton and Zhu [63] contend that a clear balance in the use of public data by the private sector especially due to the challenge of privacy and protection of the said data need to be in place. Abouelmehdi, Beni-Hessane and Khaloufi [38] support this proposal and adds that there is no justification for use of sensitive data, especially those related to medical information for any other

purposes. Thus, even though there are PPPs and the private sector is involved in the installation and management of data, there need to be limits where data can be privately used.

4. Combined Adoption of Smart City and Safe City

Besides the few concerns attributed to the PPP model of financing the smart cities concept, the strategy remains to be amongst the most potent and viable. This is true especially noting the sizeable amount of financial resources required to implement an effective smart city [64]. Milenković et al. [65] posit that through this model, the city management and governments do not only benefit from the private financial means but also from the expertise and extended network of experience possessed by the private sector. They argue that the role of government while in such an agreement is to facilitate and supervise the execution of the plan while the private partners undertake the rest of the work until the actualization of the project. Fishman and Flynn [64] reveal that out of the many cities in the world, only 16% have the potential to self-fund to the levels commensurate to smart cities standards; hence, the idea of turning to PPPs is justifiable, especially when the projects, being privately financed, have the potential to strengthen the safety, security and privacy in the city. Cruz and Sarmento [59] laud the role PPP play in promoting the improvement of smart city infrastructures and that of others like the safe city concept, though he proposes the need to restructure them to ensure they align with the need of the cities.

As such, a sizeable number of cities around the world have adopted both the smart city and the safe city concepts and welcomed the idea of PPP financing to fast track implementation. To explain this further, the example below represents cities that have adopted both concepts, the words of Doyle [66] comes into play. According to him, with the concept of smart cities in place, it is easy to adopt the safe city concept as the components dedicated to 'smartness' also plays a key role in pursuing the desired safety dimensions. For instance, when data from 'smart' devices are analysed and information sent to relevant components/departments, those that pertains to safety and security are likewise availed. A pointer to this is the safe city index report 2018 [67,68] and the smart city 2018 report [69]. Table 2 below highlights some of those cities and captures the concerns from the implementation of the concepts. All the cities captured in Table 2 have both introduced the safe city and the smart city concepts and are being and/or having been implemented. The category of issues included in the table are not conclusive but represent the most pressing ones, especially in regard to security matters.

Table 2. Notable issues facing both the smart and safe city concepts.

City	Safe City	Smart City	Concern			Source
			Privacy	Control	Propaganda	
Tokyo	X	X	X			[70,71]
Singapore	X	X	X	X		[72]
Cairo	X	X		X		[73]
Copenhagen	X	X	X			[74]
Brussels	X	X		X		[75]
New York City	X	X			X	[40]
Yinchuan	X	X	X		X	[50]
Milan	X	X		X	X	[46]
Barcelona	X	X	X			[76]

5. An Agenda for Urban Comfort

In the course of implementing both the smart and safe city, it has been established that a significant number of urban areas have been confronted by a varied number of issues especially those relating to privacy, control and propaganda. Baig et al. [77] posit that these challenges are prompted by the increase in the number security loopholes opened by availability of components that are employed in the cities to help in achieving 'Smartness.' In their words, the availability of Smart Grids, automated building systems, unmanned aerial vehicles and sensors that are enabled by IoT and cloud platforms are all geared towards rendering a more comfortable urban life. Nevertheless, the heterogeneity of

the platforms and protocols that allows for a smooth application of all these systems exposes security threats, especially to hackers, terrorists, scammers and other ill-minded groups [78]. The challenges are even more pronounced in regard to the Big Data generated by these diverse components. Gupta et al. [79] express that the vulnerability of the data may even lead to maliciously activities such as espionage, compromising the availability and integrity of data and opening to threats of financial exploitation. In other scenarios, access to data may lead to physical damage of installed devices and systems and blockage of collection or relaying of data to relevant authorities or agencies.

The concerns about privacy, control and propaganda in relation to the use of data do not only arise due to unauthorised persons but also by the way government agencies and third parties are mandated to collect, analyse and make use of said data, as it is seen that this availability provides the ability for government agents to control and even sometimes intrude on citizen's privacy. van Zoonen [45] explains that this control sometimes allows governments access to public data with no restriction, hence, giving room for private use of data by some private companies.

These criticisms and reservations have the potential to create urban discomfort of city users and residents. Svenonius [80] showcases that some of the strategies like surveillance via different tools and devices that are undertaken to secure an urban city may evoke negative effects such as fear amongst citizens; hence, they are not comfortable participating in the safe city agenda. The perception that their data is not solely handled by the government but by private agencies is an agent against urban comfort, which is also shown as counter-productive to urban efforts to drive liveability levels [81]. Furthermore, Jackson et al. [82] showcase that a majority of smart devices, sensors and systems that support the safe city concept still faces numerous challenges and are not synchronised in a homogenous platforms and systems, thus, posing the challenge of reliability especially when security of data is paramount. They argue that such heterogeneity of systems impacts on the trust that citizens have on the concept and this could only be reversed with increased transparency in the way data is utilized. Edwards [60] affirms this and adds that with numerous strategies and devices for data collection, chances for individuals to consent on how personal data is to be processed or used are unfortunately not catered for. The author pinpoints the issue specifically to the privatisation of data, infrastructure and its storage. Maple [83] adds to this and argues that until proper policies, standards and governance structures are put in place, the advent of data usage and processing as seen in both the smart and safe city concepts would be made to compromise urban comfort.

From this discussion and the literature above, it is clear that urban comfort can partly be achieved with the careful re-actualisation of the combined concepts of smart and safe city so that they can fully address the concerns of privacy, security and control.

6. Conclusions

The idea of coupling the concepts of the smart city and the safe city is seen to have, in some cases, faced strong resistance from the general public despite the clear promise this strategy brings security and policing to cities. The uncertainty around data usage is one of the primary concerns that prompts resistance towards their combined adoption. In particular, this emanates from the initial implementation structure in the form of Public Private Partnerships (PPP) that a sizeable number of cities are seen to have adopted. There is a clear call for increased data policies and control by the state on how data can be used by private corporations and how personal data can be shared across agencies and companies. In order to pursue this, there is a need to deconstruct both concepts for the identification of key dimensions that are a deterrent to liveability dimensions in the form of privacy and security. The crafting of policies oriented to address both concepts is seen as paramount. However, in this pursuit, it will be important that new proprietary technology is not sought as the alternative, as those will ultimately only generate additional profits for private corporations and provide a short-term solution to local city councils, without consideration of societal needs and concerns.

Funding: No funding was received for this study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sarkar, S. Urban scaling and the geographic concentratin of inequalities by city size. *Environ. Plan. B Urban Anal. City Sci.* **2018**. [CrossRef]
2. Moser, C.O.N.; Mcilwaine, C. New frontiers in twenty-first century urban conflict and violence. *Environ. Urban.* **2014**, *26*, 331–344. [CrossRef]
3. Peerzado, M.B.; Magsi, H.; Sheikh, M.J. Land use conflict and urban sprawl: Conversion of agriculture lands into urbanization in hyderabad, pakistan. *J. Saudi Soc. Agric. Sci.* **2018**, in press. [CrossRef]
4. Ianoş, I.; Sorensen, A.; Merciua, C. Incoherence of urban planning policy in bucharest: Its potential for land use conflict. *Land Use Policy* **2017**, *60*, 101–112. [CrossRef]
5. Lacinák, M.; Ristvej, J. Smart city, safety and security. *Procedia Eng.* **2017**, *192*, 522–527. [CrossRef]
6. Tripathi, V. Achieving urban sustainability through safe city. *J. Hum. Ecol.* **2017**, *59*, 1–9. [CrossRef]
7. Bruneo, D.; Distefano, S.; Giacobbe, M.; Minnolo, A.L.; Longoa, F.; Merlino, G.; Mulfari, D.; Panarello, A.; Patanè, G.; Puliafito, A.; et al. An iot service ecosystem for smart cities: The #smartme project. *Internet Things* **2019**, *5*, 12–33.
8. Bibri, S.E. The iot for smart sustainable cities of the future: An analytical framework for sensor-based big data applicaitons for environmental sustainability. *Sustain. Cities Soc.* **2018**, *38*, 230–253. [CrossRef]
9. Bini, S.A. Artificial intelligence, machine learning, deep learning, and cognitive computing: What do these terms mean and how will they impact health care? *J. Arthroplast.* **2018**, *33*, 2358–2361. [CrossRef] [PubMed]
10. Bassoo, V.; Ramnarain, S.; Hurbungs, V.; Fowdur, T.P.; Beeharry, Y. Big data analytics for smart cities. In *Internet of Things and Big Data Analytics toward Next-Generation Intelligence. Studies in Big Data*; Dey, N., Hassanien, A., Bhatt, C., Stapathy, S., Eds.; Springer: Cham, Switzerland, 2018; Volume 30.
11. Barkham, R.; Bokhari, S.; Saiz, A. *Urban Big Data: City Management and Real Estate Markets*; MIT Center for Real Estate and DUSP: New York, NY, USA, 2018.
12. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of trust: A decentralized blockchain based authentication system for iot. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
13. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91. [CrossRef]
14. Braun, T.; Banjamin, C.M.F.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
15. IFSEC Global. Why a Smart City must also Be Safe City. Available online: https://www.ifsecglobal.com/safe-cities/smart-city-must-also-safe-city/ (accessed on 20 February 2019).
16. Yigitcanlar, T.; Kamruzzaman, M.; Buys, L.; Ioppolo, G.; Sabatini-Marques, J.; da Costa, E.M.; Yun, J.J. Understanding "smart cities": Intertwining development drivers with desired outcomes in a multidimensional framework. *Cities* **2018**, *81*, 145–160. [CrossRef]
17. Allam, M.Z. Redefining the Smart City: Culture, Metabolism and Governance. Case Study of Port Louis, Mauritius. Ph. D. Thesis, Curtin University, Perth, Australia, 2018.
18. Allam, Z. Contextualising the smart city for sustainability and inclusivity. *New Des. Ideas* **2018**, *2*, 124–127.
19. Allam, Z. On smart contracts and organisational performance: A review of smart contracts through the blockchain technology. *Rev. Econ. Bus. Stud.* **2018**, *11*, 137–156. [CrossRef]
20. Allam, Z.; Newman, P. Redefining the smart city: Culture, metabolism & governance. *Smart Cities* **2018**, *1*, 4–25.
21. Yang, F.; Xu, J. Privacy concerns in china's smart city campaign: The deficit of china's cybersecurity law. *Asia Pac. Stud.* **2018**, *5*, 533–543. [CrossRef]
22. Finch, K.; Tene, O. Smart cities: Privacy, transparency, and community. In *Cambridge Handbook of Consumer Privacy*; Selinger, E., Polonestsky, J., Eds.; Cambridge University Press: Cambridge, UK, 2018.
23. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and privacy in smart cities: Challenges and opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
24. Alomair, B.; Poovendran, R. Efficient authentication for mobile and pervasive computing. *IEEE Trans. Mob. Comput.* **2014**, *13*, 469–481. [CrossRef]
25. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet of things. *IEEE Trans. Emerg. Top. Comput.* **2017**, *5*, 586–602. [CrossRef]

26. PWC. *Safe Cities: The India Story*; The Associated Chambers of Commerce and Industry of India (ASSOCHAM)/PWC: New Delhi, India, 2013.
27. West, D.M.; Bernstein, D. *Benefits and Best Practices of Safe City Innovation*; Center for Technology Innovation at Brookings: Washington, DC, USA, 2017.
28. Ruoso, L.-E.; Plant, R. A politics of place framework for unravelling peri-urban conflict: An example of peri-urban sydney, australia. *J. Urban Manag.* **2018**, *7*, 57–69. [CrossRef]
29. Allam, Z. Building a conceptual framework for smarting an existing city in mauritius: The case of port louis. *J. Biourbanism* **2017**, *4*, 103–121.
30. Singapore Police Force. Mid-year crime statistics for January to June 2018. In *Police News Release*; Singapore Police Force: Singapore, 2018; pp. 1–8.
31. Ma, S.; Chen, X.; Li, Z.; Yang, Y. A retrival optimized surveillance video storage system for campus application scenarios. *J. Electr. Comput. Eng.* **2018**, *2018*, 3839104.
32. Trinks, A.; Scholtens, B.; Mulder, M.; Dam, L. Fossil fuel divestment and portfolio performance. *Ecol. Econ.* **2018**, *146*, 740–748. [CrossRef]
33. Bai, J. Bulding an open platform for safe cities. In *Safe City: The Road to Collaborative Public Safety*; Huawei Enterprise, Ed.; Huawei Online: Shenzhen, China, 2018.
34. Guades, A.L.A.; Alvarenga, J.C.; Goulart, M.D.S.S.; Rodriguez, M.V.R.; Soares, C.A.P. Smart cities: The main drivers for increasing the intelligence of cities. *Sustainability* **2018**, *10*, 3121. [CrossRef]
35. Huawei. Huawei Safe City Solution: Safeguards Serbia. Available online: https://e.huawei.com/en/case-studies/global/2018/201808231012 (accessed on 8 February 2019).
36. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in smart cities: Safety, security and privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [CrossRef] [PubMed]
37. White, M.; Margolies, J.; Ronanki, R.; Steier, D.; Tuff, G.; Bhattacharya, A.; Gupta, N.; Saif, I. Exponential technology watch list: Innovation opportunities on the horizon. In *Tech Trends: The Symphonic Enterprise*; Deloitte Insight, Ed.; Deloitte Insight: Washington, DC, USA, 2018.
38. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H.J. Big healthcare data: Preserving security and privacy. *J. Big Data* **2018**, *5*. [CrossRef]
39. McKinsey & Company. *Smart Cities: Digital Solutions for a More Liveable Future*; McKinsey & Company: Brussel, Belgium, 2018; pp. 1–152.
40. Pinto, N. Google Is Transforming Nyc's Payphones into a 'Personalized Propaganda Engine'. Available online: https://www.villagevoice.com/2016/07/06/google-is-transforming-nycs-payphones-into-a-personalized-propaganda-engine/ (accessed on 10 February 2019).
41. Lam, P.T.I.; Ma, R. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities* **2018**, in press. [CrossRef]
42. Martínez-Ballesté, A.; Pérez-Martínez, P.A.; Solanas, A. The pursuit of citizens' privacy: A privacy—aware smart city is possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [CrossRef]
43. Lim, C.; Kim, K.-J.; Maglio, P.P. Smart cities with big data: Reference models, challenges and considerations. *Cities* **2018**, *82*, 86–99. [CrossRef]
44. Kummitha, R.K.R.; Crutzen, N. How do we understand smart cities? An evolutionary perspective. *Cities* **2017**, *67*, 43–52. [CrossRef]
45. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
46. Grossi, G.; Pianezzi, D. Smart cities: Utopia or neoliberal ideology? *Cities* **2017**, *69*, 79–85. [CrossRef]
47. Bhadani, A.J. Big data: Challenges, opportunities and realities. In *Effective Big Data Management and Opportunities for Implemention*; Singh, M.K., Kumar, D.G., Eds.; IGI Global: Hershey, PA, USA, 2016; pp. 1–24.
48. Sun, Y.; Zhang, J.; Xiong, Y.; Zhu, G. Data security and privacy in cloud computing. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [CrossRef]
49. Anisetti, M.; Ardagna, C.; Bellandi, V.; Cremoni, M.; Frati, F.; Damaini, E. Privacy-aware big data analytics as a service for public health policies in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 68–77. [CrossRef]
50. Guerrini, F. *Cities Cannot Be Reduced to just Big Data and Iot: Smart City Lessons from Yinchuan, China*; Forbes: Yinchuan, China, 2016.
51. Calzada, I.; Cowie, P. Beyond smart and data-driven city-regions? Rethinking stakeholder-helixes strategies. *Reg. Mag.* **2017**, *308*, 25–28. [CrossRef]

52. Edwards, L. *Privacy, Security and Data Protection in Smart Cities: A Critical eu Law Perspective*; CREATe: London, UK, 2015.
53. Tzafestas, S.G. Synergy of iot and ai in modern society: The robotics and automation case. *Robot. Autom. Eng. J.* **2018**, *31*, 1–15.
54. Čolaković, A.; Hadžialić, M. Internet of things (iot): A review of enabling technologies, challenges, and open research issues. *Comput. Netw.* **2018**, *144*, 17–39. [CrossRef]
55. Kim, T.-H.; Ramos, C.; Mohammed, S. Smart city and iot. *Future Gener. Comput. Syst.* **2017**, *76*, 159–162. [CrossRef]
56. Botta, A.; Donato, W.D.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
57. Denton, S.W.; Pauwels, E. *There's Nowhere to Hide*; Synenergene: Elangana, India, 2018; pp. 1–28.
58. Allam, Z.; Newman, P. Economically incentivising smart urban regeneration. Case study of port louis, mauritius. *Smart Cities* **2018**, *1*, 53–74. [CrossRef]
59. Cruz, C.O.; Sarmento, J.M. Reforming traditional ppp models to cope with the challenges of smart cities. *Compet. Regul. Netw. Ind.* **2017**, *18*, 94–114. [CrossRef]
60. Edwards, L. Privacy, security and data protection in smart cities: A critical eu law perspective. *Eur. Data Prot. Law Rev. (Lexxion)* **2016**, *2*, 28. [CrossRef]
61. Boyer, E.J.; Van Slyke, D.M. Citizen attitudes towards public-private partnerships. *Am. Rev. Public Adm.* **2018**, 1–16. [CrossRef]
62. Sanseverino, E.R.; Sanseverion, R.R.; Anello, E. A cross-reading approach to smart city: A european perspective of chinese smart cities. *Smart Cities* **2018**, *1*, 26–52. [CrossRef]
63. Hamilton, S.; Zhu, X. *Funding and Financing Smart Cities*; Deloitte: London, UK, 2018.
64. Fishman, T.D.; Flynn, M. Part two: Funding and financing smart cities series. In *Using Public-Private Partnerships to Advance Smart Cities*; Deloitte Center for Government Insights: London, UK, 2018; pp. 1–10.
65. Milenković, M.; Rašić, M.; Vojković, G. Using public private partnership models in smart cities—proposal for Croatia. In Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; IEEE: Opatija, Croatia, 2017.
66. Doyle, P. Making Smart Cities into Safe Cities. Available online: https://gcn.com/articles/2016/10/11/safe-smart-cities.aspx (accessed on 4 March 2019).
67. London, E. The World's Safest Cities Ranking. 2018. Available online: https://ceoworld.biz/2018/09/19/the-worlds-safest-cities-ranking-2018/ (accessed on 5 March 2019).
68. Gallup. 2018 global law and order. In *Gallup World Polls*; Gallup: Washington, DC, USA, 2018; pp. 1–11.
69. Berrone, P.; Ricart, J.E. *IESE Cities in Motion Index*; IESE Business School, University of Navara: Pamplona, Spain, 2018.
70. Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 489–516. [CrossRef]
71. Eco-Business. Japan 'Smart' Cities Relyon Public-Private Partnerships. Available online: https://www.eco-business.com/news/japan-smart-cities-rely-on-public-private-partnerships/ (accessed on 10 January 2019).
72. Ter, K.L. Singapore's cybersecurity strategy. *Comput. Law Secur. Rev.* **2018**, *34*, 924–927. [CrossRef]
73. Loideain, N.N. Cape town as a smart and safe city: Implications for governance and data privacy. *Int. Data Priv. Law* **2017**, *7*, 314–334. [CrossRef]
74. *Co-Creating the Cities of Tomorrow—Danish Smart City Competencies in Singaporean Market*; Ministry of Foreign Affairs of Denmark, United Square: Singapore, 2015.
75. van den Hurk, M. Public-private partnerships: Where do we go from here? A belgian perspective. *Public Works Manag. Policy* **2018**, *23*, 274–294. [CrossRef]
76. Calzada, I. (smart) citizens from data providers to decision-makers? The case study of barcelona. *Sustainability* **2018**, *10*, 3252. [CrossRef]
77. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensic. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
78. Altman, M.; Wood, A.; O'Brien, D.R.; Gasser, U. Practical approaches to big data privacy over time. *Int. Data Priv. Law* **2018**, *8*, 29–51. [CrossRef]

79. Gupta, A.; Anpalagan, A.; Carvalho, G.H.S.; Guan, L.; Woungang, I. Prevailing and emerging cyber threats and security practices in iot-enabled smart grids: A survey. *J. Netw. Comput. Appl.* **2019**, in press. [CrossRef]
80. Svenonius, O. The body politics of the urban age: Reflections on surveillance and effect. *Palgrave Commun.* **2018**, *4*, 2. [CrossRef]
81. Allam, Z.; Jones, D. Promoting resilience, liveability and sustainability through landscape architectural design: A conceptual framework for port louis, mauritius; a small island developing state. In *IFLA World Congress Singapore 2018*; International Federation of Landscape Architects: Singapore, 2018; pp. 1599–1611.
82. Jackson, S.; Yaqub, M.; Li, C. The agile deployment of machine learning models in healthcare. *Frontier* **2018**, *1*, 7. [CrossRef]
83. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]