Received: 31 October 2017 | Revised: 27 March 2018 | Accepted: 5 April 2018

DOI: 10.1002/app5.246

ORIGINAL ARTICLE

WILEY ASIA & THE PACIFIC POLICY STUDIES Australian National University

Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law

Fan Yang[1] | Jian Xu[2]

[1]School of Culture and Communication, University of Melbourne, Melbourne, Australia

[2]School of Communication and Creative Arts, Deakin University, Burwood, Australia

Correspondence
Fan Yang, School of Culture and Communication, University of Melbourne, Melbourne, VIC 3010, Australia.
Email: yang.f@unimelb.edu.au

Abstract

Many cities around the world are increasingly embedding technological infrastructure in urban spaces. These infrastructures aim to collect vast amounts of data from citizens with an apparent purpose of improving public services. This article discusses privacy concerns generated by China's nationwide smart city campaign and further investigates why China's latest Cybersecurity Law is not adequate to address the risks to citizens' privacy. We argue that there is no functional privacy law in China that would apply to most data collected by smart city infrastructure; nor is there any law that would protect any personal data collected under this framework. We therefore propose practical suggestions to better protect citizens' data in China's ongoing smart city campaign.

KEYWORDS

big data, China, Cybersecurity Law, privacy, smart cities

1 | INTRODUCTION

The pervasiveness of information technologies and the wide application of digital technology in urban planning has meant that urban conglomerates can no longer be sufficiently understood as materialities alone (Sassen, 1991). Instead, an interactive urban domain has emerged where citizens are empowered to shape their inhabitancy via mediated technological devices. Urban

reconstruction driven by information technologies has given rise to a worldwide smart city initiative, through which governments at different levels have started to imbue sensors, wireless technology, and cloud computing technology into services such as public transportation, banking services, e-government, and communications, which facilitates a moment that Saskia Sassen (1991) describes as "citizens talking back to the government," with the outcome presumed to be a better urban experience. In this article, we will first map out the emergence of the smart city and point to the differing interpretation of the meaning and goals of the smart city idea, before identifying the differing development and status quo of China's smart city campaign and point out possible citizen data risks that may emerge. We will then refer to the newly passed Cybersecurity Law to examine whether it could resolve citizen data risks.

2 | THE EMERGENCE OF SMART CITIES IN POLICY AND DISCOURSE

The development of the smart city concept has been shaped dramatically by changes in internetworking technology over the last three decades. A necessary precursor to the smart city can be found in the Internet of Things (IoT). The IoT envisions a widespread employment of interconnected network technology that has in some sense merged into the function of both conventional technology (such as microwaves, security systems, and cars) as well as new and developing technology (such as personal health technology and smart phones), and the idea has seen considerable uptake in the area of personal commercial technology (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). The objects within the IoT are generally connected to technology platforms either through the Internet or through local area networks; this enables these technologies to engage in communication with each other without an immediate need for human intervention to manage these emerging personal media systems (Wang, 2011, p. 718). The IoT is the conceptual precursor for the current state of smart cities policies and initiatives. The conscious adoption of "smart city" initiative originated with the ideas of the "Smart Earth" that IBM Corporation described as a part of its "Smarter Planet vision" in November 2008. The idea espouses a familiar idea: The penetration of information technology systems into all manner of physical objects in order to "*smartise*" urban experience for citizens (IBM 100, 2013). Smart city, backboned by the IoT, is one of the most important outcomes of Smart Earth (Hu & Li, 2012). The "smartness" of a city would appear to be contingent on the degree to which it is reliant on the networking technologies to facilitate communication in and throughout urban spaces.

The term "smart city" carries with it various definitions and connotations that are not necessarily consistent or informative. The smart city merges with other technical language about the contemporary urban context, including terms such as "intelligent," "innovative," "networked," "wired," "digital," "creative," "innovative," and "cultural," all of which are constantly used and conflated to illustrate city discourses (Nam & Pardo, 2011). There is a great deal of slippage among these terms—indeed the smart city is in quite a literal sense simply a rebranding of the earlier idea of the digital city—and, as a result, extracting a clear, distinct, and precise meaning from any of these terms can be difficult. This problem is compounded by the fact that scholars from different research fields discuss the smart city from different perspectives, with the interdisciplinary frameworks complicating any attempts at clarity. Saskia Sassen identifies a key aspect of the smart city as the capacity for citizens to "talk back" to the systems of government that oversee the urban space (1991). In this sense, the city is not a

closed system anymore but rather open and incomplete, within which citizen's responses, movements, and interactions within the city representing an organic logic that is reincorporated back into the predigital urban planner's conception of the city space. The predigital city is shaped by the networking experiences with digital black spots, and spaces of high digital intensity, creating a digital topology for the city that interacts reciprocally with the urban geography. The idea of the smart city is a conceptual extension of multiple personal digital contexts into a common reference point, suggesting that individuals are passively involved in city redesign and restructure (Nam & Pardo, 2011, p. 283). However, the involvement of citizens in the reshaping of the smart city is done in an aggregative manner that deprioritises individual demands within a generalising statistical model.

Against the position of the interventionist statistical model, other definitions highlight the role of technologies in the context of the smart city. Giffinger et al. (2007) argue that smart cities have a capacity to redistribute inequitable public allocation and access, aid in identifying inadequate or failing infrastructure, to address municipal services allocations (including water and energy shortages), pricing fluctuations on housing, and to identify and intervene in environmental issues. Giffinger et al.'s position becomes something of a techno-utopian perspective on the ability of the smart city to affect positive changes, and in doing so illustrates a situation that is both desirable and elusive.

Since 2011, China's rapid urbanisation combined with a digital transformation approach has meant that China has adopted the global trend and initiated a government-led smart city campaign. This campaign started within what the government has classified as “first-tier” cities, such as Beijing, Shanghai, and Guangdong; but this model has also swept into second- and third-tier cities as well. As such, cities such as Yinchuan, Tangshan, Yantan, and Urumqi, which are largely unknown outside of mainland China, have developed smart cities infrastructure at comparable levels to places such as Rotterdam and Melbourne.

China faces a situation with diverse outcomes. On the one hand, the smart city project contributes to solving contemporary urban issues in terms of negotiating energy and natural resources demand, expanding urban territorial restructure, and providing adequate infrastructure availability. This approach has a significant potential to improve quality of life for citizens. On the other hand, the technical requirements for the operation of smart cities—indiscriminate big data collection and analysis—comes at the expense of citizen's control over their personal data.

3 | SMART CITY IN CHINA

The start of China's smart city project can be traced back to the mid-1990s, predating IBM's idea of a “Smart Earth” in 2008. In the past three decades, China's smart city project has experienced rapid evolution, passing through three distinct phases of development, as identified by Nakagawa (2013). The smart city policies commenced with an urban informatisation plan called 八金计划 “bājīn jìhuà,” or literally “Eight Gold,” in 1995. The Eight Gold project aimed to developed informational infrastructure nationwide, signalling the beginning of an urban renewal predicated in digital technology. Since 1998, more than 300 cities in China have built up a some degree digital urban infrastructure framework. This first stage has been conceptualised as the *digital city*, whose major characteristic was the digitalisation of geo-locational information.

The digital city is replaced during second stage development with the *Internet city* or *wireless city*. This change is enabled by the development of the Internet infrastructure, broadband, and

wireless technologies, with construction of second stage smart cities in China largely commencing in 2005. During this phase, broad-spectrum internetworking infrastructure was deployed to governments, commercial and corporate settings, and residences. To provide more reliable and stable infrastructure support, at the end of 2008, the Chinese central government eventually restructured China's telecom carriers into three telecommunication giants: China Mobile, China Telecom, and China Unicom, with the Chinese central government claiming ownership of all three organisations. Immediately after this official reorganisation, the Chinese government released 3G mobile phone service licences to the three state-run telecommunication companies. This paved the way for the wide adoption of smart phones and digital connectivity after 2008 (Nakagawa, 2013, p. 221). Despite this, these digital systems did not immediately reach the vast majority of the Chinese public; this had to wait until personal smart devices uptake became more widespread in 2008.

Since 2008, China has witnessed a dramatic growth in the ownership of smart phones (Nakagawa, 2013). China went from 17 million personal smart phones in 2008 to around 1.09 billion phones in 2018 (QuestMobile, 2018). This represents a significant population of mobile users, which acts as the premise for the next iteration of China's smart city policies: the *sensor-networked smart city*. Sensors, in conjunction with high-density technologies, are embedded in public transportation systems, commercial services, energy sustainability, e-governance, and communications. The growing penetration of smart devices enables the rollout of the smart city campaign across China (Li, Lin, & Geertman, 2015; Martinez-Balleste, Perez-Martinez, & Solanas, 2013).

In 2011, the Chinese state released its 12th Five-Year Plan. The Five-Year Plan is a key official document outlining the projected future of China, which establishes a general framework for economic development (Yang, 2017, p. 3). The 12th iteration of this plan is the first one to explicitly involve smart city policies as a part of the future of China; the plan directs resourcing towards the development of industry application software, Internet technology infrastructure, smart devices and mobile solutions, enterprise application and infrastructure, smart-city operational services, and collaborative industries (The Central People's Government of the People's Republic of China, 2012; China Academy of Information and Communications Technology & EU-China Policy Dialogues Support Facility II, 2014, p. 44). In 2012, the Vice Minister of Housing and Urban–Rural Development released the *Notice of Implementing the National Smart City Pilot*, *National Interim Measures for Smart City Pilot*, and *Guidance on Promoting the Sustainable Development of Smart Cities* and approved 90 smart city pilot projects across China (Li et al., 2015, pp. 291–292). With the extraordinary progress of recent years, China's central government introduced another series of guidance notices for smart city strategies including *Notice to Speed up the Project Implementation of Smart Cities*, *National New Urbanistion Plan (2014–2020)*, and *Guidance on Promoting the Sustainable Development of Smart Cities*. These policies seek to further promote smart city projects in small- and medium-sized cities. On March 5, 2015, Premier Li Keqiang unveiled the "Internet Plus" strategy in his presentation at the annual session of the National People's Congress. The national strategy supports Internet-powered start-ups and the application of new technology to traditional industries and has further intensified the progress of Chinese digital urbanisation.

From the trajectory of China's smart city development, we can see that the smart city initiative is a top-down national project initiated by the central government that aims to manage China's urban space effectively with the aid of digital technologies. The smart city campaign demonstrates China's centralisation of urban transformation in order to achieve national modernisation and development goals (Cartier, 2015; Tomba, 2017). However, the nationwide

implementation of the smart city project relies on a relatively decentralised method of urban governance, that is, municipal governments involved in the smart city project have authority to manage their own projects under the guidance of relevant central ministries. The centralisation of decision-making and decentralisation of implementation mark the characteristics of China's smart city initiative.

The smart cities framework has been highly influential within China. By 2015, 285 cities had raised proposals to participate in the smart city project, according to the China Communications Industry Association (EUSME CENTRE, 2015, p. 2). In 2018, China has about 500 smart city pilots, outnumbering other countries in the world that operate smart city pilots (Xinhua, 2018). Although the two-decade development cycle may seem comparatively long, this marks a very rapid change in urban policy and in the composition of a wide array of cities in China.

Data generated within smart cities by user interaction with sensors, Wi-Fi, and other technology is an important part of data accumulation for government. Not only will the transmission of data be expected to enhance the hyper-connectivity of digital media companies, citizens, and governments, but this type of data also has the capacity for formulating sophisticated forms of surveillance and control that make it very valuable for business and urban governance (Zhang et al., 2017). Digital cities facilitate a high density of digital services and mobile applications, each of which is ready to perform a range of possible tasks for citizens, which in turn generates data about user behaviour. In aggregate, this produces comparatively high volumes of geolocative data about city populations. Although citizens give a fragmented part of their data based on the media platform they use and the sensors with which they connect, this partial information and the continuous tracking of data make the identity of individuals reidentifiable (McQuire, 2008, p. 89). This retention and use of citizen data can raise privacy concerns and debates. As Jose van Dijk (2014, p. 205) argues, data surveillance is a far-reaching proposition with profound consequences for the social contract between corporate platforms and government agencies as surveilling bodies, and citizens as the surveilled.

4 | PERSONAL DATA CONCERNS IN CHINA

China is not the first country where a wide discussion of citizens' online privacy in smart cities has arisen. Public interrogation of privacy issues has been ongoing in the USA since the Internet was made public. In 2013, Edward Snowden revealed the US government's systematic, routine, and focused attention to personal details in collaboration with tech giants (Lyon, 2014, p. 2). The National Security Agency was spying on American citizens with the help of telecommunication companies and PRISM who granted National Security Agency access to the servers of US high-tech companies such as Google, Facebook, Microsoft, and Apple (Greenwald, 2013).

People in China are caught in a bind between semiresponsive urban planning policies that passively incorporate their behaviours into urban planning and a mass surveillance system that accumulates data about a wide range of activities. At the beginning of 2018, when online shoppers using the Sesame Credit company attempted to check their annual transaction records, they noticed that their confidential information was not well protected by the terms and agreement, yet the parent company claimed that they do not take any responsibility for user data destroyed or requested by third parties (Cui, 2018). Online shopping data are highly controversial in China but also a significant player in China's smart city campaign. In March 2016, the vice president of Sesame Credit, Hu Tao, gave a speech claiming that "Technology plus credits are the future of the smart city" (Tech, 2016). Tao sought to maintain close collaboration with

China's government by stating that if the government could open and share citizens' data with them, they would be able to help the government improve e-government management by measuring citizens "social inclusiveness score" (Tech, 2016). In 2018, the fears about surveillance represented by Sesame Credit scores have been recently intensified by the Apple computing company recently handing over management of the Chinese portion of its cloud computing services to companies run by the Chinese state. In passing over control to a state-run company, public concern was raised around the possibility of state surveillance (Xiaobai, 2018). Crucially, government agencies in China now have legal authority to request information regarding iCloud users (Nellis & Cadell, 2018), which represents roughly 20% of the Chinese mobile market (Statista, 2018). Corporate involvement in smart city technology is not limited to personal computing technology. ZTE, a telecommunications company, was awarded a contract worth approximately US$500 million to provide technology services for smart cities in China, covering 13 subsystems over 3 years and includes smart transportation, smart community, and environmental improvement, an all-in-one citizen card, smart tourism, IT enterprises, smart government, and a big data analysis centre (Dahad, 2016). A full-spectrum digital network supported by ZTE and city governments covers the entire city.

For years, little could be done to address privacy concerns raised in relation to the smart city campaign due to the lack of a legal framework for privacy issues in China. Of the limited legal documents, the Cybersecurity Law, passed in 2017, is perceived as the most comprehensive safeguard for Chinese citizens' online privacy rights. Yet this document has limitations that hinder its ability to solve the growing privacy problems.

5 | CYBERSECURITY LAW: PROMISES AND LIMITATIONS

Prior to the implementation of the Cybersecurity Law in 2017, a few decisions had been made to guarantee Chinese citizens' online privacy, these included China's *Decision on Strengthening Protection of Online Information* (hereafter the *Decision*; 全国人大常委会关于加强网络信息保护的决定 quánguó réndà chángwêihuì guānyú jiāqiáng wângluò xìnxī bāohù de juédìng) implemented in 2012, the *Decision on Amending the Law of the People's Republic of China on the Protection of Consumer Rights and Interests* (hereafter *2013 Amendment*; 中华人民共和国消费者权益保护法 [2013 修正] zhōnghuá rénmín gōnghéguō xiāofèizhê quányì bâohùfâ [2013 xiūzhèng]) released on April 28, 2013, and the *Notice Regarding Strengthening the Management of Network Access for Mobile Smart Terminals* (hereafter the *Notice*; 工业和信息化部关于加强移动智能终端进网管理的通知 gōngyè hé xìnxīhuàbù guānyú jiāqiáng yídòng zhìnéng zhōngduān jìnwâng guânli de tōngzhī) released in 2012.

The *Decision* states that it is the responsibility of the Internet service provider to protect users' online information, specifically limiting collection only to when "necessary," and requiring users' consent. Additionally, Internet service providers must not sell or divulge information to third parties nor destroy data without consent (Committee of the National People's Congress, 2012). The *2013 Amendment* requires that e-business operators not collect data unrelated to business operations, use improper gathering techniques, or divulge consumers' personal data (Committee of the National People's Congress, 2013a, 2013b). The *Notice* further prohibits smart devices from preinstalling applications or features that make privacy issues a concern. As with the Decision, the Notice requires user consent for data collection and requires smartphone manufacturers to build in data protections into their devices (Committee of the National People's Congress, 2013a, 2013b).

The *Decision*, the *2013 Amendment*, and the *Notice* make clear statements about who should take care of users' data privacy by assigning responsibilities to three major subjects: Internet service providers, e-commerce operators, and smart device manufacturers. However, in the context of the smart city campaign, digital platforms are increasingly overlapping and precise responsibility for data flows is unclear. It is difficult to distinguish who should take care of what data and take relevant responsibilities. In order to protect the legal interests of citizens, promote a healthy development of social and economic information, and strengthen China's cyber sovereignty and national security, the Cybersecurity Law was officially implemented on June 1, 2017 (Xinhua, 2016). This official proclamation signifies the protection of online users' personal information entering a new stage.

The Cybersecurity Law innovatively separates personal information rights from privacy rights. It includes the protection of personal online information as a fundamental civil right and leverages its legal status quo. The Cybersecurity Law highlights "personal information of natural persons is legally protected by Cybersecurity Law. No organizations or individuals can abuse or misuse personal online information." These protections are established in the "Network Information Security," section, especially by Articles 40–49, which assign obligations to service providers around the responsible accumulation and management of personal data (Committee of the National People's Congress, 2016).

The Cybersecurity Law stipulates requirements for the protection of personal information, especially for avoiding disclosure, damage, and loss of personal information. It seeks to establish the paradigm that Internet service providers, either individuals or organisations, must undertake the responsibility for data protection. In this sense, approaches and methods of data collection and storage must be regulated and standardised for Internet service providers and related organisations. It is also noteworthy that compared with the *Decision*, *2013 Amendment*, and the *Notice*, the Cybersecurity Law expands the scope of personal information protection from "users" to "individuals," illustrating the extensiveness of Cybersecurity Law.

As stipulated, network operators providing business and service activities are subject to the requirements of the Cybersecurity Law regime, despite this, the government's role in protecting citizens is not explicit. Kitchin (2014) identifies the role of "politics of city data" and the governance of data generated from interconnected digital devices, which is also lacking from this framework. The policy problem of media convergence also complicate things, so while Article 40 establishes a need for data management, the question as to who, precisely, is responsible remains unclear. At an individual level, the problem of reidentification and general data transparency are also not represented. Therefore, we suggest that the Cybersecurity Law will need to be updated to better fit the complexities of the city data landscape by referring to the experience of other countries with regard to data protection.

6 | SUGGESTIONS FOR FUTURE LEGAL UPDATE

6.1 | Preconsent policy upgrade

Edwards (2015, p. 32) suggests that video tutorials may guide users through privacy settings of mobile device applications so that they better understand the settings they accept. The traditional agreement to "Notice and Choice" is considered a preconsent policy through which users and service providers reach consent for their mutual benefit of online service and user data collection. Boardman (2006) argued that using preticked boxes fails to fulfil the preposition that user consent must be clear and unambiguous. Existing research identifies that users either reject

or fail to read terms and conditions (Morrison, 2015), or lack proper conceptual understanding of what, exactly, is being given up in user data agreements (Keith, Babb, Lowry, Furner, & Abdullat, 2013). Therefore, following Edwards (2015), we suggest upgrading the current preconsent policy to include user education, such as video tutorials, as a requirement in the Cybersecurity Law. We would specify that any educational materials be as user-friendly and unambiguous as feasible, identify data gathering techniques and consequent risks. Materials should include information on privacy settings, data selection process, data analysis process, and the potential outcomes from citizen-generated information, as well as information regarding parties responsible for data management.

6.2 | Encryption of citizen data

By implementing adequate data encryption, individual user data may be protected against deidentification. Encryption is widely used in sensitive and ethical data management, including medical, genetic, and insurance data. In these contexts, transmitted data are encrypted or decontextualised to protect individual identities (Milieu Ltd & Time.lex, 2014). Service providers should encrypt data by default in order to prevent users from being reidentified.

6.3 | The right to be forgotten

The right to be forgotten originates from the issue that media affects private life by publicising events that should remain private, and thus violating citizens' right to privacy (Mantelero, 2013). In 2012, the European Union expanded the right to be forgotten to the Internet data. This right requires search engines to erase online documents of certain personal data (The European Parliament and of the Council of the European Union, 2016). Although the right to be forgotten has not been officially introduced in China, some media scholars (Zhang & Zhou, 2018) have presented it as an important tool for protecting user privacy, arguing that China's Cybersecurity Law provides a legal base for the right to be forgotten. By making this right explicit, better protections could be extended to users.

7 | CONCLUSION

China's smart city campaign has put personal data security at the forefront of public concerns. As discussed, existing legislation lags far behind the growing personal data risks emerging in the smart city campaign and beyond and thus does not effectively address these problems. Given the limitations of the Cybersecurity Law, we have proposed three possible directions to improve the law to better protect people's online personal data. It would be mistaken to read our suggestions as indicating that the smart city framework is merely a cover for an intensification of surveillance (Yu, 2017). Instead, we hope that both government and corporate sectors will work together to protect user data from exploitation (van Dijk, 2014, p. 204). Without this faith in government and corporate organisations, any suggestions to improve personal data protection would not only be impossible but redundant.

Yet personal data protection in China is a complicated problem that cannot be easily solved in the short term. The negotiation, competition, and interaction between the three leading forces of governmental, commercial, and citizen powers will make personal data protection a contested process with bumps and turns. The smart city campaign, in which the three parties

are intertwined, thus provides a good context to examine the politics of personal data as well as to explore possible ways to solve personal data risks to mitigate contentions among the three powers. We hope this article helps start to open up investigation in the area. Empirical research is needed to comprehensively examine China's ongoing smart city campaign and the data policy, politics, and ethics in the national plan.

ACKNOWLEDGEMENT

This article would not be possible without the guidance of Robbie Fordyce, who helped shape the initial direction of the article and also gave valuable feedback on the final draft.

ORCID

Fan Yang http://orcid.org/0000-0001-6707-4344

REFERENCES

Boardman, R. (2006). Use of consent in data protection, viewed 29th January 2018, https://www.twobirds.com/en/news/articles/2006/use-of-consent-in-data-protection

Cartier, C. (2015). Territorial urbanisation and the party-state in China. *Territory, Politics, Governance*, *3*(3), 294–320.

China Academy of Information and Communications Technology & EU-China Policy Dialogues Support Facility II. (2014). Comparative study of smart cities in Europe and China 2014 (Current Chinese Economic Report Series), *The Commercial Press China and Springer*: Beijing, Berlin.

Committee of the National People's Congress. (2012). Decision on strengthening protection of online information(全国人大常委会关于加强网络信息保护的决定 quánguó réndà chángwêihuì guānyú jiāqiáng wângluò xìnxī bâohù de juédìng, viewed 28th February 2018, http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm

Committee of the National People's Congress. (2013a). Notice regarding strengthening the management of network access for mobile smart terminals (工业和信息化部关于加强移动智能终端进网管理的通知 (工信部电管〔2013〕120号 gōngyè hé xìnxīhuàbù guānyú jiāqiáng yídòng zhìnéng zhōngduān de tōngzhī) , viewed 26th February 2018, http://www.gov.cn/zwgk/2013-10/31/content_2518541.htm

Committee of the National People's Congress. (2013b). Decion on amending the law of the People's Republic of China on the protection of consumer rights and interests (2013 Amendment(中华人民共和国消费者权益保护法 修改 zhōnghuá rénmín gònghéguó xiāofèizhê quányì bâohùfâ xiūgāi), viewed 27th February 2018, http://www.gov.cn/jrzg/2013-10/25/content_2515455.htm

Committee of the National People's Congress. (2016). Cybersecurity Law (中华人民共和国网络安全法 zhōnghuá rénmín gònghéguó wângluò ānquán fâ), viewed 28th June 2017, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

Cui, P. (2018). Alipay leaked users' privacy in the their annual report? Sesame Credit responded “wrong” (支付宝年度账单泄露用户隐私?芝麻信用回应称“错了” zhīfùbâo niándù zhàngdān xièlù yònghù yîsī), viewed 22nd February 2018, http://www.sohu.com/a/214491628_115565

Dahad, N. (2016). Smart cities can deliver better public service, but need secure Internet of things (IoT), viewed 5th March 2018, http://www.thenextsiliconvalley.com/2016/02/14/4540-smart-cities-can-deliver-better-public-service-but-needs-secure-internet-of-things-iot/

Edwards, L. (2015). Privacy, security and data protection in smart cities: A critical EU law perspective, *CREATe Working Paper Series (2015/11)* https://doi.org/10.5281/zenodo.34501

EUSME Centre. (2015). Sector report: Smart cities in China, Report: Smart Cities in China.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovie, N., & Meijers, E. (2007). Smart cities: Ranking of European medium-sized cities, Vienna, Austria: Centre of REGIONAL science (SRF), VIENNA University of Technology, http://www.smart-cities.eu/download/smart_cities_final_report.pdf

Greenwald, G. (2013). NSA collecting phone records of millions of verizon customers daily, viewed 22nd February 2018, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Hu, M., & Li, C. (2012). Design smart city based on 3S, Internet of things, grid computing and cloud computing technology. *IOT Workshop, CCIS*, *312*, 466–472.

IBM 100. (2013). Smarter planet, viewed 25th February 2018, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/smarterplanet/doi://www-03.ibm.com/ibm/history/ibm100/us/en/icons/smarterplanet/

Keith, M. J., Babb, J., Lowry, P. B., Furner, C., & Abdullat, A. (2013). The roles of privacy assurance, network effects, and information cascades in the adoption of and willingness to pay for location-based services with mobile applications, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2287446

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*, 1–14.

Li, Y. L., Lin, Y. L., & Geertman, S. (2015). The development of smart cities in China, *CUPUM 2015*, 291-Paper.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, July–December, 1–13.

Mantelero, A. (2013). The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Martinez-Balleste, A., Perez-Martinez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6). http://ieeexplore.ieee.org.ezp.lib.unimelb.edu.au/document/6525606/?part=1

McQuire, S. (2008). *The media city: Media, architecture and urban space*. London: SAGE Publications Ltd.

Milieu Ltd & Time.lex. (2014). Overview of the national laws on electronic health records in the EU member states and their interaction with the provision of cross-border eHealth services: Final report and recommendations (contract 2013 63 02), viewed 18th March 2018, https://ec.europa.eu/health//sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*, 1497–1516.

Morrison, K. (2015). Survey: Many users never read social networking terms of service agreements, viewed 21st February 2018, http://www.adweek.com/digital/survey-many-users-never-read-social-networking-terms-of-service-agreements/

Nakagawa, R. (2013). The rapid growth of the smartphone market in China and the "business ecosystem". 立命館国際研究, *25(3), 219–229*.

Nam, T., & Pardo, T. A. (2011). Conceptualising smart city with dimensions of technology, people, and institutions, The Proceedings of the 12th Annual International Conference on Digital Government Research, June 12–15, 282–291.

Nellis, S., & Cadell, C. (2018). Apple moves to store iCloud keys in China, raising human rights fears, viewed 3rd March 2018, https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060

QuestMobile. (2018). QuestMobile: 2017 China mobile Internet report, viewed 2nd March 2018, https://www.questmobile.com.cn/blog/en/blog_130.html

Sassen, S. (1991). *The global city: New York, London, Tokyo*. New Jersey: Princeton University Press.

Statista. (2018). Market share of mobile operating systems in China from January 2013 to December 2017, viewed 11th March 2018, https://www.statista.com/statistics/262176/market-share-held-by-mobile-operating-systems-in-china/

Tech. (2016). Sesame Credits Hu Tao: Technology + Credits, The Future of Smart City (芝麻信用 胡涛:科技+信用,智慧城市的未来 zhīma xìnyòng Hú Tāo: kējì + xìnyòng, zhìhuìchéngshì de wèilái), viewed 11th March 2018, https://kknews.cc/tech/ljj949.html

The Central People's Government of the People's Republic of China. (2012). 12th Five-Year Plan (whole passage) ("十二五"规划纲要(全文)shíèrwû guīhuà gāngyào (quánwén)), viewed 22nd February, http://www.china.com.cn/policy/txt/2011-03/16/content_22156007.htm

The European Parliament and of the Council of the European Union. (2016). Regulation (EU) 2016/579 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, viewed 17th March 2018, http%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FTXT%2FPDF%2F%3Furi%3DCELEX%3A32016R0679%26amp%3Bfrom%3DEN

Tomba, L. (2017). Gentrifying China's urbanisation? Why culture and capital aren't enough. *International Journal of Urban and Regional Research*, *41*(3), 508–517.

van Dijk, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Wang, S. L. (2011). Spatial data mining under Smart Earth, 2011 IEEE International Conference on Granualr Computing (GrC), 2011 IEEE international conference on: 717–722 Nov, 2011.

Xiaobai. (2018). I tried to protect my information security when sexting others (我试了试如何在聊骚时保护自己的信息安全 wÔ shìleshì rúheé zài liáotiān shí bâohù zìjî de ānquán), viewed 31st January 2018, http://www.vice.cn/read/how-to-sext-securely-safely-what-apps-to-use-sexting-chinese-version

Xinhua. (2016). Xinhua insight: China adopts Cybersecurity Law to protect national security, Citizens' Rights, viewed 12th December 2017, http://www.xinhuanet.com/english/2016-11/07/c_135812209.htm

Xinhua. (2018). China outnumbers other countries in smart city pilots: Report, viewed 26th February 2018, http://www.xinhuanet.com/english/2018-02/20/c_136987058.htm

Yang, F. (2017). *Faked in China: Nation branding, counterfeit culture, and globalisation*. Bloomington: Indiana University Press.

Yu, K. (2017). China's smart city plan to boost surveillance, viewed 28th March 2018, https://www.sbs.com.au/news/china-s-smart-city-plan-to-boost-surveillance

Zhang, K., Ni, J. B., Yang, K., Liang, X. H., Ren, J., & Shen, X. M. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, *55*(1), 122–129.

Zhang, Z. A., & Zhou, Y. T. (2018), The introduction of the right of being forgotten in the era of big data (论大数据时代 "被遗忘权" 的中国引入 lùn dàshùjù shídaì bèiyíwàngquán de zhōngguó yînrù), viewed 17th March 2018, http://mp.weixin.qq.com/s/EfrYeO3ZvykEq0xEqiunrg

How to cite this article: Yang F, Xu J. Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia Pac Policy Stud*. 2018;5:533–543. https://doi.org/10.1002/app5.246