Privacy by Design in China's Digital Privacy Laws and its Application in Smart Cities

Hongyu Fu

Chong Liu
BEIJING, China

Abstract
The rapid development of internet and data technological tools gravely endangers people's privacy in China, triggering legislative response to provide more protection. Private by Design is embodied in recent Chinese digital privacy laws and applied in Chinese smart cities. It provides a balance between digital privacy protection and the need of utilization of personal private information to make cities more intelligent, efficient and environment friendly.

Keywords:
Private by Design, digital privacy law, smart cities

1. Privacy by Design: Principles and Its Application in EU and U.S.

1.1 Introduction of Privacy by Design and Its Foundational Principles

"Privacy by Design" is a paradigm developed by Dr. Ann Cavoukian, in the 1990s, to address the emerging and growing threats to online privacy. The main idea is to inscribe the privacy protection into the design of information technologies from the very start. This paradigm represents a significant innovation with respect to the traditional approaches of privacy protection because it requires a significant shift from a "reactive model to proactive one."[1]

1 See Anna Monreale, Salvatore Rinzivillo, Francesca Pratesi, Fosca Giannotti and Dino Pedreschi, Privacy-by-design in big data analytics and social mining (EPJ Data Science 2014) 3.

According to Dr. Ann Cavoukian, "Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."[2] The Private by Design paradigm consists of seven foundational principles: (1) Proactive not Reactive; (2) Privacy as the Default Setting; (3) Privacy Embedded into Design; (4) Full Functionality; (5) Full Lifecycle Protection; (6) Visibility and Transparency; (7) Keep it User-Centric.[3] Therefore, Private by Design highlights the proactive protection of privacy, the end-to-end and full lifecycle protection by using the protection system embedded into design. Besides, user-friendly characteristics, the increased data transparency, and a "win-win" result are critical elements, based on the seven principles of Private by Design.

1.2 An Overview of the Application of Private by Design in EU and U.S.

EU and U.S. have incorporated Privacy by Design in their digital privacy protections laws, though in different manners. EU insisted to enact an comprehensive and far-reaching digital privacy law, and adopted Data Protection Directive in 1995 to protect individuals' personal data and the free movement of such data.[4] In 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online rights of privacy and boost Europe's digital economy.[5] After more than four years' legislation efforts, the EU passed the General Data Protection Regulation (GDPR) in 2016, which superseded the Data Protection Directive and became enforceable in 2018.

The GDPR reflects the seven basic principles of Private by Design in many parts. Firstly, GDPR protects natural persons' fundamental rights to protect their personal data and shows the respect for their privacy. Secondly, GDPR reflects the transparent, full-life cycle protection on individuals'

2 See Anne Cavoukian, 'Private by Design. The 7 Foundational Principles. Originally' <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> accessed on April 25 2021.

3 *Ibid*.

4 European Parliament, Regulation (EU) 2016/679 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 [2016] OJ L199/1 (General Data Protection Regulation).

5 Full text available at https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

personal data. Thirdly, Article 25 specifies on "Data protection by design and by default" explicitly, making it a settled legal principle.

In U.S., legal protection of privacy is based on a combination of the Constitutional protection, federal legislation, industry self-regulations and the state laws. The Fair Information Practice Principles (FIPPs) published by the U.S. Department of Health, Education and Welfare in 1973 has been the foundation of the U.S. legislation on personal data protection. In recent years, with a rising tide of privacy blunders on social networking sites and platforms, U.S. is also searching for a new regulatory approach, i.e., private by design.[6]

The Federal Trade Commission first rolled out Private by Design as an official policy in its 2010 privacy report, as one of three components of a proposed framework for data security. The other two components are "simplified choice" and "greater transparency."[7] And in its 2012 Report, FTC proposed the final FTC privacy framework and implementation recommendations, incorporating "Privacy by Design"; "Simplified Consumer Choice" and "Transparency" principles.[8] According to the 2012 FTC report, Privacy by Design requires companies to promote consumer privacy throughout their organizations, and at every stage of the development of their products and services. The FTC report further requires the companies to assure data security, take reasonable collection limits, make sound retention practices, and keep data accuracy by adopting appropriate procedural measures.[9]

2. *Private by Design in China*

2.1 The Chinese Legal Regime of Digital Privacy Protection

Unlike EU and U.S., digital privacy protection legal regime in China can be characterized as (1) coordinated from multiple areas of law, (2) comprehensive in enacting an integrated legislation, and (3) supplemented by lower-level legal documents. China in recent years have enacted several legislations, the provisions of which provide criminal, civil, and adminis-

6 Deirdre K. Mulligan and Jennifer King, 'Bridging the gap between privacy and design' (2012) 14 U. Pa. J. Const. L. 989.
7 FTC, Protecting Consumer Privacy in an Era of Rapid Change (FTC 2010) 9.
8 FTC, Protecting Consumer Privacy in an Era of Rapid Change (FTC 2012) 7-8.
9 See *ibid.*, 22-34.

trative sanctions or remedies for breach of privacy and personal information in digital era. The criminal, civil and administrative law provisions provide a full-scale legal network addressing digital privacy protection issues, though the relationship among them is not well delineated. In 2020 a major legislation was proposed, named Personal Information Protection Law. The draft law marks an attempt by China's legislators to enact an encompassing, comprehensive law covering most aspect in this matter, changing the landscape of digital privacy protection from the coordinated approach to a unified approach. Besides such specific legislative provisions, departments in charge of privacy protection and digital society administration published lower-level legal documents supplementing the legislation, which, together with privacy protection provision in other areas of laws, provided clearer guidance for different participants to fulfill their legal responsibilities.

2.1.1 China's Coordinated Legislative Approach to Digital Privacy Protection

The Criminal Code provides sanctions against intentional infringement on a person's personal information and privacy since 2009, making it punishable by imprisonment and fine. The scope of criminal punishment has been gradually expanded, and severity extended in recent years as of some personal infringement cases leading to severe harm to the victim. For example, since the case of Xu Yuyu, the Supreme People's Court and the Supreme People's Procuratorate published the judicial interpretation of "crime of infringing on citizens' personal information" (the Interpretation)[10]. The Interpretation shows the determination of the highest Chinese Judicial Institutions, which is to put emphasis on protecting citizens' important private personal information and exert the punishment in severe and lenient manner depending on different circumstances.

With respect to the civil law, the Civil Code of the People's Republic of China (the Civil Code), which is a foundational, systematic, and comprehensive code in the area of private law. Firstly, the Civil Code's protection on digital privacy is manifested in Article 111: "The personal information of a natural person shall be protected by law." Neither the illegal collec-

10 Xu Yuyu case involves a telephone fraud against Ms. Xu, a high school graduate student from a less wealthy family, who was going to college. Ms. Xu's personal information was hacked and was defrauded to wire out several thousand RMB prepared for her college study. She committed suicide, and the case generated an outcry in China for criminal punishment of personal information invasions.

tion, use, process and transmission, nor the illegal deal, provision, and publishment of the personal information of other persons are allowed. Secondly, the Civil Code made specific stipulations to protect the right of privacy and personal information in Book Four, Personality Rights. According to Articles 1032 and 1034, a natural person enjoys the right of privacy, and the Civil Code protects a natural person's personal information. Remarkably, the Civil Code keeps balance between protection and processing. For example, an actor shall not assume any civil liability if the processing is for protecting the public interest or the lawful rights and interests of the natural person. Thirdly, although the Civil Code is a private law, it can also prevent the administrative decision, management, and supervision from violating a natural person's private right. In other words, the Civil Code can impose certain restrictions on the administrative power.

Concerning the administrative law, the Cybersecurity Law of the People's Republic of China (the Cybersecurity Law) provides the foundational legal protection on cybersecurity and the lawful rights and interests of citizens, legal persons and other organizations. Firstly, the Cybersecurity Law emphasizes on constructing a comprehensive state governance system on the cyber area. According to Articles 6, 9, 10, 11 and 12, the system needs the state's legal measures. However, the cyber security cannot be realized with the mere efforts from the state. The participation of the entire society, the intensify industry self-discipline by network-related industry organizations and any individual or organization's legal usage of the internet are also essential. Secondly, the Cybersecurity Law completes cyber security obligations and responsibilities of network operators, who are the owners and administrators of the network as well as network service providers. Thirdly, in Chapter VI, Legal Liability, the penalties for illegal acts have been raised, which is conducive to ensure the implementation of the Cybersecurity Law.

2.1.2 China's Recent Endeavor to a Unified Digital Privacy Protection Law

The draft of Personal Information Protection Law was issued on October 21, 2020 for public comment. The draft assimilates the relevant laws and regulations of the Cybersecurity Law, Law on the Protection of Rights and Interests of Consumers, the Civil Code, the E-Commerce Law and so on. Besides, the draft also assimilates some good rules of foreign legislation, for example GDPR. In conclusion, there are five main highlights of the draft:

(1) The expansion of the applicable territorial scope. According to Article 3, the draft law shall not only be applied within the territory of the People's Republic of China, but also be applied to the processing outside the territory of the People's Republic of China, under certain circumstances. Article 3 is similar to the stipulations in Article 3 of GDPR.
(2) The emphasis on the preliminary explication and the consent of a natural person. Most of the rules on personal information processing are stipulated in Chapter II. In Article 14, the draft law clearly clarifies the definition of "consent to the processing of personal information", i.e., an individual shall express his consent voluntarily and explicitly on the premise of being fully informed. However, being excessive with the explication on premise and the consent of a natural person can sometimes be the enemy of the good. According to Article 13, the lawmakers have decreased the limitation on information processing, which is beneficial for the balance between personal information protection and usage. In the era of big data and cloud technology, this new balance can promote the economy vitality.
(3) The emphasis on the obligation of the personal information processors. The draft law has increased the personal information processors' freedom on processing personal information. Thus, comparatively, it is necessary for the processors to bear more responsibilities on protecting individuals' personal information. The specific stipulations are in Chapter V, Obligations of Personal Information Processors.
(4) The explicit statement of individuals' rights in personal information processing activities. According to Articles 44 to 48, individuals shall have the following five main rights, i.e. the right to know and the right to decide on the processing of their personal information; the right to consult and duplicate their personal information; the right to request personal information processors to correct or supplement relevant information; the right to delete his or her personal information; the right to request personal information processors to interpret the personal information processing rules they develop.
(5) The strengthening on monitoring of the states' departments. "Personal information protection is different from industry to industry." Therefore, Article 56 stipulates on three kinds of states' departments performing the function of protecting personal information, which have

formed a system, in order to make sure every individual can receive the legal protection on their personal information.[11]

2.1.3 Supplementing Rules to Digital Privacy Legislation

In addition to the four main legislations hereinberfore, there are various separate rules on personal information in different departmental laws and regulations. For example, Article 12 in Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases; Article 16 in Regulation on the Handling of Medical Accidents; Article 4 in Provisions on the Technical Measures for the Protection of the Security of the Internet, and so on.

2.2 The Application of Private by Design under Current China's Digital Privacy Protection Laws

Although there is no explicit term "Private by Design" appearing in the Chinese legislations, the seven foundational principles of Private by Design have been embodied in the Chinese digital privacy laws.

2.2.1 The "Proactive not Reactive" Principle Is Embodied in the Chinese Criminal and Administrative Legislations

First of all, the criminal law naturally has a deterrent effect, with the legal power to impose fine, limit individuals' person freedom and even take one's life. To protect citizens' data privacy, the Amendment IX to the criminal law revised the criminal law from two aspects.

In the first place, the Amendment added a new crime called "crime of infringing on citizens' personal information", which expanded the scope of the criminal subjects. Before the Amendment IX became effective, according to the Amendment VII, the criminal subjects of crimes on personal information were enumerated as "the staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment". While in the Amendment IX, all citizens

11 Full text available at <https://m.mpaypass.com.cn/news/202010/22144504.html> accessed on April 25 2021.

could be the criminal subjects. The Amendment also expanded the scope of "personal information". The "personal information" is no longer limited within the scope of personal information that is obtained during the organ's or entity's performance of duties or provision of services. According to the Amendment VII, any act of infringing on citizens' personal information, if with serious circumstances, is under the criminal law's jurisdiction; In the next place, the criminal law also clarifies that the network service provider has the obligation to perform the information network security management.

Secondly, the judicial interpretation in 2017 made explicit interpretation on "serious circumstance". The Interpretation set different standards for different kinds of personal information. According to Article 5, paragraph 3, the crime standard is 50 pieces for "the citizen's whereabouts, communication contents, credit investigation information and property information"; while for "accommodation information, communication records, health and physiological information, transaction information and other personal information", the crime standard is 500 pieces. Also, the Interpretation adopts the fair principle. For example, with respect to the punishment, Article 12 stipulates that the punishment will be considered based on the hazards caused by the crime, the amount of illegal income involved in the crime, and criminal record and confession and repentance attitudes of the defendant.

In conclusion, the criminal code and the interpretation expanded the scope of the criminal subjects and the criminal acts on personal information, which can protect the personal information and prevent crimes before-the -fact. In addition to the criminal code, the Cybersecurity Law also shows the preventative measures on protecting personal information. The Cybersecurity Law stipulates on the regular conduction of data protection reviews. According to Article 21, it is important for the network operators to establish safe and effective protection system; to choose a appropriate technical solution; to strengthen the data protection capacity according to the Cybersecurity Law. In addition, according to Article 25, the Cybersecurity Law also focuses on making emergency response plans for cybersecurity incidents.

2.2.2 The "Privacy as the Default Setting" Principle Is Embodied in the Relevant Stipulations on Mobile Internet Application Program (APP).

"Privacy as the Default Setting" means that the protection on citizens' privacy has been built into the system with the default setting. Being

applied to the apps operation, it means that the privacy policy and other collection and usage rules showed to the users have adopted the strictest protection on personal privacy as a default setting, being built into IT systems, technology infrastructure or business practices by default.[12] In other words, it is similar to the "opt-out" regime on personal privacy protection. Only if a user chooses not to consent the policy or the rules, will their privacy lose protection. In fact, this automate protection on users' privacy is also embodied in the Chinese legislation. Taking Provisions on the Administration of Mobile Internet Applications Information Services (the Provisions) as an example, the Provisions not only stipulates on a mobile internet apps provider's obligation, but also emphasizes on an internet apps service provider's obligation.

According to Article 7, a mobile internet apps provider shall establish and improve the users' information security protection mechanism. For example, encrypting and protecting the users' data; preventing unrelated people from obtaining the data; preventing the data from being downloaded and stolen and recording the operation on important documents and so on.[13] Article 8 stipulates that an internet apps service provider shall perform management and supervision responsibilities for apps providers. For example, urging apps providers to establish and improve the security examination mechanism to protect users' information; to provide complete explanations on the obtaining of apps and users' information, and to present them to users. If apps providers violate the Provisions, the internet apps service providers shall adopt measures, such as warning, suspension of launching, and removal of apps, keep relevant records, and report to the competent department.

2.2.3 *The Principles of "Privacy Embedded into Design" and "Full Lifecycle Protection" are Applied in The Civil Code and The Cybersecurity Law*

The principles of Privacy Embedded into Design and End-to-End Security have connections on personal information protection. These two principles both focus on a comprehensive security mechanism to protect personal information. However, the former one focuses on the preventative

12 Full text available at <https://www.pwc.com/us/en/services/consulting/library/gdpr-embedding-data-protection.html> accessed on April 25 2021.

13 Full text available at <http://www.ip-guard.net/blog/?p=1818> accessed on April 25 2021.

measures, while the latter one puts emphasis on the later-stage management. Therefore, these two principles will be introduced together.

Firstly, the Civil Code provides a basic "End-to-End Security" system for personal information and privacy protection. According to Book Four, Personality Rights, Chapter VI, Right of Privacy and Protection of Personal Information, the Civil Code protects a natural person's personal information and privacy from six aspects, i.e. (1) the definition of privacy and personal information; (2) the principles of processing the personal information; (3) the obligations of a information processors; (4) the strict restrictions on exemption excuses for processing a natural person's information; (5) the three main rights of a natural person; (6) the confidentiality of the state organs, statutory institutions and their staff members. These stipulations have established a comprehensive firewall for a natural person's privacy and personal information. [14]

Secondly, the Cybersecurity Law mainly protects network users' personal information from two aspects, i.e., network operation security and network information security. According to Articles 15 and 40, the state shall establish and improve the system of cybersecurity standards and the system for the protection of users' information.[15] The network operation security is the premise of the network information security, just like the relationship between Privacy Embedded into Design and End-to-End Security.

2.2.4 The Full Functionality Principle Is Applied in The Civil Code and The Personal Information Protection Law.

Full Functionality principle means that Private by Design seeks to accommodate a "win-win" manner rather than a dated, zero-sum approach. In other words, this principle is seeking for a balance. This principle is embodied in many legislations by increasing the legitimacy for operators to process the personal information.

Firstly, according to Article 1036 in the Civil Code, there are three circumstances under which an actor does not need to obtain the natural person's consent. The three circumstances are (1) under the consent by the natural person or his or her guardian; (2) with the initiative publishment

14 Full text available at <https://m.mpaypass.com.cn/news/202006/11113115.html> accessed on April 25 2021.

15 The Cybersecurity Law of China.

of the natural person or the legal publishment; (3) for protecting the public interest or the lawful rights and interests of the natural person.

Secondly, according to the Personal Information Protection Law, Article 13, there are six circumstances under which a personal information processor to process personal information without the preliminary consent.[16] The draft law decreases the limitation on the personal information processing, which is beneficial for the balance between personal information protection and usage.

2.2.5 *The Visibility and Transparency Principle Is Embodied in Preliminary Informing and Later-stage Processing.*

The principle of Visibility and Transparency is embodied in two aspects, namely, to inform users clearly before collecting their information and to process personal information transparently. The first aspect is always explicitly indicated as the principles of openness and transparency in laws and regulations. For example, in Article 7 of the Personal Information Protection Law; Article 1035 of the Civil Code; Article 7 of the Cybersecurity Law; Article 17 of the E-commerce Law; Article 29 of Law of the People's Republic of China on the Protection of Consumer Rights and Interests and so on. Besides, after receiving individuals' personal information, the transparency of processing and retention on personal information shall also be guaranteed.

2.2.6 *The Keep It User-Centric Principle Is Applied in Confirming Users' Right by Laws and Regulations.*

Most of the Chinese laws and regulations explicitly stipulate on an individual's right to protect his or her personal information. For example, the Personal Information Protection Law makes a conclusion on individuals' rights in personal information processing activities in Articles 44-48, which shows the priority to users' privacy.

Also, the Chinese legislative institution enacts laws and regulations in key areas concerning citizens' personal information protection. For example, the E-commerce Law was enacted to safeguard the lawful rights and interests of all parties to e-commerce. According to Article 18 and 19,

16 See the specific stipulations in the Personal Information Protection Law.

the E-commerce Law adopts the "opt-in" regime, stipulating that an e-commerce business shall provide the consumer with options not targeting his or her identifiable traits; and shall not set the said tie-in sale as a default option, which show respect and equally protection for the lawful rights and interests of consumers. Besides, the E-commerce Law also increases e-commerce businesses' burden of proof in order to help the consumer defend his or her lawful rights and interests. According to Article 62, over the course of handling an e-commerce dispute, an e-commerce business shall provide the original contract and transaction records to ascertain the facts. Otherwise, the e-commerce business shall assume corresponding legal liability.

In conclusion, the Chinese legislations on personal information, from the public laws to the private laws, have contained the spirit of the seven principles of Private by Design. In the future, with the Personal Information Protection Law becoming effective and more and more departmental laws being enacted in key areas, the Chinese legal protection on personal information will become more complete.

3. *Application of Privacy by Design in China's Smart Cities, with A Case Study of Face Recognition Technology*

3.1 China's Smart City Building and the Entailed Privacy Concerns

The overarching concept of smart city rests on internet that connects various end users and their appliances, as well as the vast amount of data that are being generated and processed for system control and decision making. China has been building up internet and data infrastructure which facilitate the construction of smart cities, especially with the rollout of 5G and gigabit network. The application of internet over things (IoT) has increased significantly in China, not only in first tier cities like Beijing, Shanghai, and Shenzhen, but also in so-called New First Tier cities including Hangzhou and Chengdu, as well as cities in lower tiers. The fast pace in smart city building reflects China's momentum in all three layers of IoT logical architecture, including application layer, transport layer and sensing layer.[17]

17 For the discussion about the layers of IoT, see Li Ling, Li Shancang, Zhao Shanshan, 'QoS-aware scheduling of service-oriented Internet of things' (2014) 10 2 IEEE Trans on Industial Informatics 1497-1505[12]; Wu Chunkun. Security Fundamentals for Internet of Things (Science Press 2013).

The sensing layer, which includes the sources of data like RFID, GPS, environment detectors, cameras, etc., has infiltrated not only into industrial settings, but also to average offices and households. Intelligent device manufactures compete fiercely on this level, producing cutting edge end user devices that fit into different scenes. Thanks to the fast pace of urbanization and booming in real estate market, newly built home and offices are generally equipped with such data collecting devices providing basic input for the community and city IoT infrastructure. The utilization of wireless technologies over WiFi, Bluetooth and other energy-signal transforming mechanisms also enables intelligent innovation for older buildings. In the transport layer, the bandwidth of mobile communication networks and computer networks increases significantly in the 5G era, expanding the transmittable data into more applicable scenes and enabling new technologies including autonomous driving. In the application layer, major platform providers provide services to various users including governments and public entities, allowing the latter to engage in smart decision based on big data and AI. The public sector also pushes for the utilization of new technologies, under the requirements of Fang, Guan, Fu reform.[18] Big data and AI are also used for managing traffic and most importantly, in recent COVID-19 pandemic prevention and control.[19] To give more room to the private sector and to positively engage with new technologies, municipal governments in China are weighing themselves in transforming mega cities into smart cities.

The fast expansion of the utilization of IoT and AI technologies has generated concerns over the breach of privacy in various settings. In smart homes, the intelligent devices make privacy exposure more easily, where leaking of private information could happen over the internet by means of security breach or inadvertent maneuvers by residents. Hacking into home cameras has been prevalent in China because of weak security protocols.[20] The inter-connected nature of smart devices further exacerbates the problem. In addition, the face recognition technology has been developed to an extent that customer's face information could be captured far a certain

18 *Fang, Guan, Fu* in Chinese means government agency shall return power to market, to provide better management and to serve well the needs of market participants.

19 For a summary of the application, see "What are the roles of Big Data in Pandemic Control and Management", available at <https://www.thepaper.cn/newsDetail_forward_9806802> accessed on April 25 2021.

20 See media report, available at <https://www.sohu.com/a/150861985_182299> accessed on April 25 2021.

distance, creating concerns over her privacy as well as financial security. It also raises a contract law issue, where the customer may dispute whether she gives actual and voluntary consent to the payment request, thus finalizes the transaction. In another instance where smart utility devices are applied, a user's real time electricity, water and other utility usage are constantly monitored and processed. The big data generated from these smart utility devices assists the utility providers to adjust their services to better meet users' demand, reduce unnecessary production and make energy consumption greener. Yet utility consumption data may reveal users' personal lifestyle. Improper use of such information may create social inequality among groups with different income, as household income level in general positively correlates with its utility consumption. The data may also reveal information regarding personal habits and recreational activities which is private. On a broader level, the inter-connectivity of numerous IoT devices make the smart cities more susceptible to data breaches, and the invasion in end user device may cause large scale privacy incidents to ensure utility data being anonymous and identified. It is crucial to secure privacy. Therefore, a more comprehensive legal framework covering each layer and every participant is needed, to address privacy concerns from using smart utility devices to the technologies used in smart cities.

3.2 The General Application of Privacy by Design in China's Smart Cities

The Private by Design principles, when actively applied, can provide illustrative solutions to above challenges against privacy protection in smart city building in China.

Firstly, Private by Design requires privacy protection to be incorporated throughout the life cycle of smart city planning, building, operation, and management. Privacy protection therefore is considered as part of the major functions of a smart city, which is a requirement must be met not a cost to be ignored. The incorporation of privacy protection can mitigate the risk of privacy invasion, especially considering that the remedies provided by privacy laws apply ex post to privacy infringement and may not be sufficient to prevent large scale privacy invasion in city level.

Secondly, the concept of Privacy by Default makes residents and users more confident about the privacy protection. Currently privacy protection legal regime premises on the notion of self-determination, where a user gives informed consent to the collection and use of her personal information and private data. The proliferation of IoT devices in smart cities brings convenience and efficiency to its residents, but it makes users more

difficult to make meaningful decisions on whether to allow the collection or use of their private information. Privacy by Design requires each participant in smart cities, when collecting and using users' private information, must respect users' right of privacy and personal information, must by default protect users' relevant rights without users' further or additional action. Thus, users are not required to go through voluminous amounts of informed consent documents, as they can expect every informed consent document by default provides sufficient protection for their privacy. This will also in turn facilitate the collection and use of private data, as more users are willing to voluntarily allow data access.

Thirdly, Private by Design can generate positive results in smart city planning, building and management, creating win-win for various participants. In the past decades, China has been developing fast in internet and data technologies, at the cost of users' personal information and privacy. Recently the legislation made it clear that privacy and personal information are strictly protected by civil law, administrative law and criminal law, overcoming the concerns that stringent legal protection on privacy may choke technology development and innovation process. The application of Private by Design principles provides good illustration that the need of privacy protection and the interest of technology innovation can both be met. In smart cities where Private by Design principles are applied, privacy can be attained together with efficiency, cleanliness, and convenience. The positive sum result will in turn attract more residents and more capital, creating more competitiveness for the city.

3.3 Case Study: Applying Privacy by Design in Face Recognition Technology

Face recognition technology serves as the nexus between human and machine, where a person who intends to access and control the machine is identified and authorized. Comparing to the other biometric identification technologies, it is more accurate with recent development in image capture and analysis technologies. In addition, it doesn't require the cooperation of the users, and can identify an user remotely without his or her actual knowledge of being identified. Thus it enables quick and mass surveillance, especially for security purposes. Smart cities in China have vastly used face recognition technologies to provide identification in public places, especially where security is of concern, including transportation hubs and major gatherings. Privately, face recognition has been used in mobile apps when a user intends to get access to his or her private information, always to his or her financial information, where mobile bank is used.

Recently, the application of face recognition technology later goes into different urban areas, including public spaces where security is of less concern like parks and zoos, workplaces; where the working hours of the employees are monitored; and vending machines where the identity of a purchaser is verified and an automatic charge against her account is made. The wide application of face recognition technology by government and businesses in cities in China reflects the need of a more accurate, efficient, and convenient mechanism, which can be used to verify the identity of a user intending to have access to the city's services, public or private. Some municipalities used the face recognition technology to identify people who violated traffic rules.[21] In some parks, people must scan their faces to get toilet paper.[22] And in some universities, students were required to make face recognition before they engaged in sports activities. However, the necessity of such pervasive use and negative implication to user's personal information and privacy are not properly and adequately addressed.

In the vast and fast process of urbanization, commercial pragmatism, few concern went over the need for protection of personal rights, leading to outcries in society where people object the proliferation of unnecessary use of face recognition technology. In 2019, a case was brought by Professor Guo Bing who intended to enter Wide Life Park in the City of Hangzhou but required to go through face recognition. Professor Guo considered his facial information as extremely sensitive and private, and sued the zoo in the city's Fuyang district court.[23] The district court decided that the zoo violated its contract with Professor Guo and ordered nominal compensation. The intermediate court of Hangzhou upon appeal (where court sessions were streamed online) made a landmark decision, which emphasized on the nature of personal facial information as sensitive information protected under the then applicable civil laws, and the misuse of personal facial information might cause substantial personal and financial

21 "A man in the City of Zhengzhou declined to provide ID number, and the Police used Face recognition to identify", available at <https://new.qq.com/omn/20191108/20191108A0NP7R00.html> accessed on April 25 2021.

22 "One uses face recognition to get toilet paper in public restrooms", available at <https://baijiahao.baidu.com/s?id=1637066496072386885&wfr=spider&for=pc> accessed on April 25 2021.

23 Guo Bing v. Hangzhou Wildlife Park Co., Ltd, Zhe0111MinChu No.6971(2019).

injuries. The court asked the zoo to delete the face photo taken from Professor Guo, as well as his fingerprint information.[24]

The decisions were rendered before the application of the Civil Code, but the judicial recognition marked a fundamental step towards the balance between the proliferation of facial recognition technology and the urgent need of personal information protection. On one hand, the two courts' decline to decide whether the compulsory use of face recognition technology, without informed consent from the user, violates the statutory protection of personal information, leaving the uncertainty on the legality of such use intact. On the other hand, the decisions do confirm that if there is a legal basis for the protection of personal information (in this case, a breach of consumer's contract), the grieved party can sue for damages as well as specific performance including requesting the deletion of any unauthorized personal information obtained and retained by a commercial party. It can be argued that the case was not decided under the Civil Code, therefore it lacks the authority as a precedent for subsequent disputes on face recognition technology. Nevertheless, the development of this case generates great public attention to the abuse of face technology in current Chinese cities. It also calls for a better legal framework to address the need for privacy and personal information protection.

Compared with similar cases, for example, the Swedish Data Inspection Authority imposed fines on the Swedish Data Inspection Authority, because this school uses face recognition technology to monitor its student attendance, which is against the GDPR. However, the decisions from the courts in China did not invoke a tort theory, thus not giving a direct answer to whether a person in China has the priority to use his or her facial information over any authorized commercial use; and whether he or she can claim any remedies in case his or her right is infringed. And what is more important is, since facial recognition technology is widely used by public entities, which also retains most accurate and full-scale facial information, how to restrict the use of the technology by public entities for ill-defined public purposes is far from being raised and contested in courts.

Privacy by Design can be used in the application of face recognition technology in building smart cities in China. The policy goal is to make a proper balance between the need of swift and accurate identification

24 The decision was officially announced, but the full opinion is not currently available. The abstract can be accessed at <https://www.chinacourt.org/article/detail/2021/04/id/5956124.shtml> accessed on April 25 2021.

in certain situations, to enhance security and efficiency, to reduce congestion and prevent identify fraud, and the need to protect people's privacy and personal information as basic civil rights, against unintended and unauthorized use either by commercial entities or by public entities. The principle on preventing abuse has been acknowledged in practice. City of Hangzhou, in response to the Wild Life Park case, proposed a municipal regulation to forbid compulsory use of face recognition technologies in commercial and residential properties.[25] One of the new national standards requires more secured systems involving remote face recognition.[26] The principles of Privacy Embedded into Design and Full Lifecycle Protection are also critical to strengthening privacy protection when face recognition technology is applied. Face information is considered sensitive and pertains not only to privacy but also to user's financial and other security. Another national standard requires full assessment and risk prevention before handling sensitive information, providing comprehensive and reliable protective mechanism above data minimization and necessity principles.[27] It can be argued that although the fast urbanization and wide application of face technologies in China bring privacy concerns, recent judicial cases and technology standards incorporated Privacy by Design principles while attempting to reconcile the competing interests of efficiency and privacy protection. The decisions and soft rules supplement China's legislative regime on privacy protection, making face recognition technology more privacy-friendly and less invasive to user's rights.

4. Conclusion

China in recent years is advancing in its digital privacy protection laws, learning from EU and U.S., and more importantly reacting to domestic pressure as of the proliferation of internet technologies which have gravely threatened people's privacy. It has incorporated Privacy by Design in its legal provisions and applied in its smart city planning and building. Priva-

25 Draft City Regulation on Property Management (2020) Full text available at <http://sf.hangzhou.gov.cn/art/2020/9/10/art_1659435_57186813.html> accessed on April 25 2021.

26 Information security technology—Technical requirements for remote face recognition system (2020), available at <http://std.samr.gov.cn/gb/search/gbDetailed?id=A47A713B767814ABE05397BE0A0ABB25> accessed on April 25 2021.

27 'GB/T39335-2020 Information Security Technology Personal Information Security Assessment Guidelines', China Standard Press, 2020 (in Chinese).

cy by Design provides meaningful guidance and solutions to the balance of privacy protection and better utilization, especially considering the interconnectivity of IoT devices in smart cities. The application of Privacy by Design, like digital privacy laws, remain to be tested in court. However, it can be argued that China's recent legislative response to provide a better and more comprehensive digital privacy protection framework, applying Privacy by Design principles in smart cities and other situations, could be illustrative in regime and constructive in experience.