Privacy Law
Bulletin

Preventing COVID-19 and protecting personal information in China

Dr Jie (Jeanne) Huang *THE UNIVERSITY OF SYDNEY LAW SCHOOL*

The recent COVID-19 outbreak has pushed the tension of protecting personal information in a transnational context to an apex. Using a real case where the personal information of an international traveller is illegally released by Chinese media, the article analyses Chinese law for personal information protection in the context of the COVID-19 pandemic.

Facts

In late March 2020, Chinese media widely reported an Australian lady with Chinese origin who breached the home quarantine requirement by jogging without wearing a mask in the residential complex she temporarily lived in, in Beijing.[1] A Chinese policeman required this lady to stay at home. This lady refused and alleged she was abused by the policeman. Chinese media released this lady's photo,[2] her age, her flight information, her name,[3] her nationality, her temporary home address in Beijing, the Chinese and Australian universities she graduated from and the years of her graduation, her employment history and positions, her current employer and her salary, etc. Her employer was the Chinese subsidiary of German pharmaceutical giant Bayer. Bayer China quickly made an announcement and fired this lady for breaching Chinese quarantine requirement. Because her Chinese visa was sponsored by Bayer in China, the Chinese Government revoked her visa and deported her after Bayer terminated her employment contract. Clearly, this lady violated the COVID-19 mandatory self-quarantine regulation in China. Her conduct threatened the public health and was not justifiable. However, does her offence justify releasing her detailed personal information online under Chinese law?

Personal information right distinguished from privacy

The Chinese Constitution provides very limited protection for an individual's right to personal information. The Constitution provides that the residence of Chinese citizens is inviolable and that freedom and privacy of correspondence of Chinese citizens are protected by law.[4] These provisions have limited implications on personal information protection in China. Literally speaking, these constitutional provisions are for residence and correspondence. Personal information protection concerns information far more than an individual's address and other contact information. It is unclear whether these constitutional provisions can cover all other personal information. More importantly, these constitutional provisions are about protecting privacy; however, in China, protecting personal information is not the same as protecting privacy.

The General Provisions of the Civil Law of the People's Republic of China, a fundamental law for civil rights and obligations in China, was enacted in 2017. It prescribes privacy and personal information protection in different articles. Article 110 provides that "natural person[s] [have] the right to life ...[,] body, health, name, portrait, reputation, honor, privacy, and marriage [autonomy]." Article 111 indicates:

> The personal information of a natural person shall be protected by law. Any organization or individual [who] needs to acquire the personal information of an individual shall obtain such information in accordance with law and quarantee the safety of such information … [and] shall [not] illegally collect, use, process, transmit, trade, provide or publicize the personal information of others.

There are two opinions regarding the relationship between Art 110 and Art 111. The first is Art 110 is *lex generalis* while Art 111 is *lex specialis*: protecting personal information (Art 111) is to enhance the protection of privacy (Art 110) in the digital economy. The second opinion is that Art 111 is not *lex specialis* as opposed to Art 110, because personal information is different from privacy. The second opinion is endorsed by the Proposed Chinese Civil Code (third draft) (the Proposed Chinese Civil Code).[5] If enacted, the Proposed Chinese Civil Code will replace all existing laws concerning civil law issues.[6] Article 811 of the Proposed Chinese Civil Code defines privacy and Art 812 provides that the right to privacy should be protected as *erga omnes*.[7] Articles 813–817 address personal information, however focusing on collection and processing

of personal information according to principles of legality, proportionality and necessity — namely, provisions for privacy focuses on non-intrusion of privacy while those for personal information highlight how to legally use personal information. Therefore, the right to privacy and the right to personal information are distinguishable. Distinguishing personal information from privacy can also find support from other Chinese legislation. For example, the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Trial Cases involving Civil Disputes over Infringements on Personal Rights and Interests through Information Networks also suggest that not all personal information can be considered part of privacy.[8] Article 12.1 provides that internet users or network service providers shall not use the internet to disclose personal privacy *and other personal information*. Article 87 of the E-Commerce Law of the People's Republic of China also provides that if a state functionary sells or illegally provides others with the *personal information*, privacy or trade secrets that come to their knowledge in the performance of their duties, they shall be subject to legal liability according to law. If personal information were to be equal to privacy, the italicised part would be redundant. In conclusion, in China the right to personal information protection is not an absolute right like privacy or property ownership, and its protection is comparatively weaker.[9]

The mandatory nature of personal information protection law

Data protection law may be considered as mandatory law and directly applicable to foreign-related civil relations without guidance from the conflict rules in China. In 2012, the Chinese Supreme People's Court issued a judicial interpretation which defines mandatory law as:

> … provisions of the laws and administrative regulations [that involve] the social public interests of [China], … [that] the parties [concerned] cannot [exclude their application through an agreement, or] that [are] directly applicable to foreign-related civil relationship without [guidance from the] conflict rules.[10]

The judicial interpretation provides the following situations under which a law may be determined as mandatory law:

- involving the protection of the interests of labourers
- involving food or public health safety
- involving environmental safety
- involving financial safety such as foreign exchange administration
- involving anti-monopoly or anti-dumping or
- other situations

In the context of COVID-19, if a law for public health safety requires releasing of personal information, this law should be applied because it is a mandatory law, and consequently foreign laws should be excluded. Applying this to the COVID-19 case, although that lady's habitual residence is in Australia, Australian privacy law would not be applied by Chinese courts. This is because Chinese law for COVID-19 is a mandatory law. On 4 February 2020, China's Central Cyberspace Affairs Commission issued a Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control of Disease (Notification).[11] Therefore, this Notification should be applied to international travellers whose habitual residences are not in China.

This Notification provides that all localities and departments should attach great importance to the protection of personal information. Except for those agencies authorised by the State Council's sanitary and health department in accordance with China's Cybersecurity Law, the Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases and Regulations on Public Health Emergencies, no other unit or individual may use personal information on the grounds of epidemic prevention and control or disease prevention without the consent of the person whose data is being collected.[12] Where laws and administrative regulations provide otherwise, they shall be implemented accordingly. The collection of personal information necessary for joint prevention and control should refer to the national standard of Personal Information Security Specification 2017 and adhere to the principle of minimum collection.[13] The collection object in principle is limited to key groups such as diagnosed persons, suspects, and close contacts, and is generally not targeted at specific areas to prevent de facto discrimination against specific geographic groups. Personal information collected for epidemic prevention and control and disease prevention shall not be used for other purposes.[14] No entity or individual may disclose personal information such as name, age, identity card number, phone number, home address, etc without the consent of the person whose information is being collected, except for the joint disease defence and control work. All personal information used should be desensitised and anonymised.

Therefore, by releasing the Australian lady's personal information such as employment and education details without her consent, the relevant Chinese media have likely violated this Notification. The collection and release of her information did not comply with the

minimum principle because her employment information, the university she graduated from, and the year of her graduation have nothing to do with disease prevention and control.

Practical implications

- On 4 February 2020, China's Central Cyberspace Affairs Commission issued a Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control of Disease. The Notification aims to protect personal information while combating the COVID-19 pandemic.
- In China, the right to personal information is considered a personality right. However, the right to personal information is not the same as the right to privacy.
- Data protection laws may be considered mandatory laws and directly apply to foreign-related civil relations without guidance from the conflict rules.

Dr Jie (Jeanne) Huang
Associate Professor
The University of Sydney Law School
Jeanne.huang@sydney.edu.au
www.sydney.edu.au

Footnotes

1. N Gan "A Chinese Australian woman breached coronavirus quarantine in Beijing to go for a jog—and lost her job" *CNN* (20 March 2020) https://edition.cnn.com/2020/03/20/asia/beijing-coronavirus-woman-fired-intl-hnk/index.html.
2. Some Chinese media mosaicked her face, but some did not.
3. Her name has three Chinese characters and the media released the first Chinese character — being the surname — and the last Chinese character. Some Chinese media released her full English name.
4. Constitution of the People's Republic of China, Arts 39 and 40.
5. The Proposed Chinese Civil Code (third draft) was submitted for review at the 15th Meeting of the 13th Standing Committee of the National People's Congress on 23 December 2019. The official draft of the Proposed Chinese Civil Code can be found at www.npc.gov.cn/npc/c35174/mfdgfbca.shtml.
6. Above, Art 1260.
7. Above n 5, Art 812 provides limited exceptions (ie, circumstances prescribed by law and consented by a right holder) to intrusion of privacy.
8. Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Trial Case involving Civil Disputes over Infringements on Personal Rights and Interests through Information Networks (promulgated on 21 August 2014 and effective on 10 October 2014, Fa Shi [2014] No 10).
9. C Xiao "Personal Data Rights in the Era of Big Data [Da Shuju Shidai de Geren Xingxi Quan Baofu]" (2018) 3 *Soc Sci China* [*Zhongguo Shehui Kexue*] 102 at 115–16.
10. Interpretation of the Supreme People's Court on Several Issues Concerning the Application of the "Law of the People's Republic of China on the Law Applicable to Foreign-Related Civil Relationships" (promulgated on 28 December 2012 and effective on 7 January 2013, Fa Shi [2012] No 24), Art 10.
11. Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control of Disease (promulgated and effective on 4 February 2020).
12. Above, Art 1.
13. Above n 11, Art 2.
14. Above n 11, Art 3.