ChinaWhys and wherefores – Illegal provision and obtaining of personal information under Chinese law

Scott Livingston and Graham Greenleaf

(2014) 131 *Privacy Laws & Business International Report* 1-5

In August 2014, Briton Peter Humphrey and his wife, naturalized American citizen Yu Yingzeng, were convicted by a Chinese court for violating the *PRC Criminal Law*'s prohibition on illegally obtaining the personal information of others. The couples' imprisonment provides a warning to companies operating in China on the dangers of falling afoul of the country's increasingly comprehensive personal information and data privacy laws. At the same time, the Humphrey case also points to the ongoing risk of political interference in legal processes in China, further underscoring the need for companies to develop internal policies and practices in full compliance with national laws.

In this article, we look at how the *PRC Criminal Law*'s personal information protection provision, Article 253(a), has been interpreted since its introduction in 2009. We begin with a brief account of the history of the Humphrey case, followed by an examination of Article 253(a) and its subsequent interpretation in the Humphrey and other cases.

The Humphrey Case – Background

The Humphreys ran a Shanghai-based investigation and advisory firm, ChinaWhys Co., that specialized in providing risk advisory services to multinational companies doing business in China. In July 2013, Chinese police detained the couple, and later charged them with violating the prohibition against illegal obtainment of personal information found in Article 253(a)2 of the *PRC Criminal Law*. On August 27, 2013, Peter Humphrey appeared in a taped confession on state-run China Central Television stating that he had used "illegal means" to obtain the personal information of Chinese citizens. At the couple's trial in August 2014, this information was alleged to have included 256 specific personal information records, including hukou (city residential permit) information, family information, and travel and phone records. ChinaWhys purchased this information for RMB 800 to RMB 2000 (about US $130 to $325) per record and used it in background investigation reports prepared for ChinaWhys' clients. Following trial, the couple were found guilty with Peter Humphrey sentenced to two and a half years in prison and fined RMB 200,000 (around USD $32,000). His wife, Yu Yingzeng, was sentenced to two years in prison and fined RMB 150,000 (USD $24,000).

Criminal Law Article (253(a)) – Scope and application

The addition of Article 253(a) to the Criminal Law by the Seventh Amendment, enacted in 2009 by the Standing Committee of the National People's Congress (SC-NPC, China's second-highest legislative

body[1]), was the first occurrence of direct protection of personal information by the criminal law in China.[2] Article 253(a) of the *PRC Criminal Law* prohibits companies or their staff members from "illegally" obtaining, selling, or providing citizens personal information to another, where such violations are "serious." In full, Article 253(a) provides:

> "Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, etc. in violation of the state provisions, sells or illegally provides citizen's personal information, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined.
>
> Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.
>
> Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph."

Article 253(a) contains two separate prohibitions. In 253(a)1, a prohibition on the sale or "illegal" provision of citizen's personal information collected by companies in certain enumerated industries. In 253(a)2, a prohibition on the illegal obtainment of the "aforementioned information" (i.e., information collected by the enumerated entities) by any party through theft or "other means." Each of these prohibitions is examined below.

Sale or 'Illegal' Provision

Article 253(a)1's prohibition on the sale or illegal provision of personal information is contained in its first paragraph and applies to staff members of "state organs" and certain enumerated industries. Generally, these listed industries provide services to the public (e.g., healthcare, telecommunications services, education) and so regularly collect large amounts of personal information in the course of performing their duties. However, the list of industries provided in paragraph one is capped off by an "etc." (等) catch-all, suggesting that the list is non-exclusive. (English language practitioners should be aware that this "etc." does not appear in most available translations of this provision.) As a result, there remains some uncertainty over how expansive this enumerated list should be read; that is, whether it should include only the listed industries, only the listed industries and similar industries that provide services to the public, or to all potential industries.

[1] Another law enacted by the SC-NPC, its Decision 'on Internet Information Protection' of 28 December 2012, provides that '[n]o organization or individual may steal or otherwise illegally acquire a citizen's personal electronic information, or sell or unlawfully provide a citizen's personal electronic information to others'. See Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), pgs 204-5.

[2] Amendment 7 to the Criminal Law of the People's Republic of China (VII), 2009

Based on our analysis of reported cases, we believe that Chinese courts have selected the second of these options and that Article 253(a)1 is likely to apply to the enumerated industries and similar industries that provide services to the public.

Our research examined twenty reported cases involving the illegal *sale* of personal information. Five involving the telecommunications industry, one from financial services, five involving a government authority (i.e., a "state organ"), five involving telecommunications, three involving air transportation, and two involving express delivery. Of these, only express delivery falls outside the enumerated list of industries although, as a proxy for the national mail service, it is arguably the type of public-facing industry targeted by the prohibition. These reported decisions suggest that PRC courts have not yet adopted an expansive view of the "etc." provided in paragraph one and have confined their application of Article 253(a)'s prohibition against sale or illegal provision to those companies operating in industries that serve a provide services to the public.

We caution, however, that the absence of further interpretative guidance and the potential for political influences in legal processes (see below) leaves open the possibility that a Chinese court may apply this provision more broadly in subsequent cases. The issue could be clarified if a court rejects a case because a defendant does not provide services to the public. From a policy perspective, it is not obvious why protection of personal data should be restricted to those industries which are public-facing, unless it is on the basis that it is in those industries that the most widespread harms are likely to occur and therefore where the need for criminal sanctions are greatest.

'Illegal' obtainment and its broad scope

Our view above is supported by two recent cases involving Article 253(a)2 in which the defendants were solely charged with "illegal obtainment" despite the fact that that the information purchased was later sold or otherwise provided to downstream parties (and therefore seemingly open to prosecution under Article 253(a)1).

In 2012, business information firm Dun & Bradstreet's local China operating subsidiary, D&B Marketing Services Co., Ltd., was found guilty of violating the "illegal obtainment" provision of Article 253(a)2 for purchasing the personal data of 150 million Chinese citizens. According to news reports, this information was later sold to company clients. The company was fined RMB $1 million (around USD $160,648 at the time) and four employees were sentenced to up to two years in jail.

In the Humphrey case, the couple purchased 256 personal information records, which information was later packaged in research reports provided to ChinaWhys clients. This information was originally provided to the Humphreys by certain individuals affiliated with business marketing companies.[3]

In these cases, it seems equally likely, and perhaps more reasonable, for a charge of "sale or illegal provision" to have been appended to the original charge of "illegal obtainment" given that the

[3] Notably, one of these individuals who sold information to ChinaWhys, Liu Yu, has also been charged with "illegal *obtainment*" of personal information, although it's unclear what, if any, part of his charge is in relation to the Humphreys case. (The other individuals involved in this case are reported to also have been "charged in other cases" (另案处理) but we have been unable to ascertain the basis of their specific charges.)

defendants later provided the illegally-gained information to third parties. The prosecutor's reluctance to do so suggests three possible reasons. First, that marketing and forensics companies fall outside the scope of industries covered by Article 253(a)1. Second, the prosecutor is unsure how Article 253(a)1 should be read and this uncertainty cautioned against application. Or, third, the prosecutor felt the "illegal obtainment" charge was sufficient to address the illegal conduct. In the Humphrey case, a possible fourth option may exist, insofar as what was sold to clients was technically a research report that also contained personal information, and was not intended to be a direct sale of personal info.

While we cannot know the reason behind the court's decision to focus solely on the "illegal obtainment" charge, this case history supports the notion that PRC courts have, to date, interpreted Article 253(a)1's prohibition on illegal sale or provision as restricted solely to state entities and other public facing industries, and not, as here, business information companies. Article 253(a)2, on the other hand, appears to be interpreted as a broad prohibition on illegal obtainment of personal information by any individual or entity, regardless of their particular industry.

Before turning to the question of when a violation is deemed "serious," there remains one additional question with respect to the "illegal obtainment" clause of Article 253(a)2. As noted above, this clause seeks to prohibit the "illegal obtainment of the aforesaid information (上述信息)," where such "aforesaid information" apparently refers to the type of information specified in the first paragraph, i.e., citizen's personal information collected by staff members of state organs or entities in certain listed industries. Under this interpretation, a defendant would only be guilty of violating Article 253(a)2 if the illegally obtained personal information originated from an Article 253(a)1 covered entity. However, this interpretation does not seem to have been adopted by PRC courts in practice.

Our research indicates that PRC courts seem to have interpreted "aforesaid information" to refer solely to the "citizen's personal information" language found in Article 253(a)1 and not to its attached industry qualifiers. In nine of the last ten reported cases involving Article 253(a)2, such personal information was purchased online or from various individuals, and did not originate from a state entity or the type of public-facing industry found in Article 253(a)1. It therefore seems that Article 253(a)2 is substantially broader than its plain text suggests, permitting prosecution of industries and entities in all sectors, regardless of where such personal information originated.

'Serious violation' or possible political factors?

As noted above, Art. 253(a) is only intended to apply to illegal transfers of personal information when such matters are "serious." However, there has been very little guidance given to date to determine what makes a matter "serious." According to court transcripts, the Humphrey actions were deemed "serious" because of the "great benefit" (i.e., income) they received when selling ChinaWhy's research reports to their domestic and foreign clients. In other cases, "serious" seems to have been met based on the large amounts of data purchased or sold by defendants.

In a recent review of the Humphrey case written by Professor Donald Clarke,[4] the author suggested that the Humphrey sentence may represent an "outlier" when compared to other Article 253(a) illegal obtainment actions. In a sample of the 20 most recent Article 253(a)2 cases involving illegal obtainment, Professor Clarke found that 19 involved at least 1000 pieces of information, 6 involved over 100,000, and 2 involved several million.[5] In all cases, no defendant received a fine higher than RMB 30,000 or jail time longer than 18 months. This contrasts sharply with the treatment afforded Mr. Humphrey and his wife, in which only 256 records were involved but where the couple received jail time of more than two years, and collective fines of RMB 300,000.

Part of the reason behind this disparity in sentencing, and finding of "seriousness," may have to do with a reported connection between ChinaWhys and the China subsidiary of GlaxoSmithKline ("GSK China"). GSK China is currently ensnared in an ongoing anti-corruption investigation that has resulted in corruption charges against its former chief manager and other employees.

According to news reports, GSK hired ChinaWhys to investigate and identify an anonymous whistleblower who had alleged in a letter to senior management that the company had bribed Chinese doctors in order to secure business. The suspected whistleblower is said to be a person with significant political influence in China, and many believe that such relationships played a significant role in the Chinese government's decision to prosecute the couple.

While court-provided transcripts of the hearing made no mention of GSK, these political factors may have influenced a finding of "serious" in this case, but that can only be speculation.

Some of many prosecutions under Article 253(a)

Article 253(a) has become the most-used provision to enforce data privacy protections in China, has now been used in an estimated minimum of 260 prosecutions. It is worth reviewing examples of the variety of contexts in which it has been used, to help avoid wrong assumptions being made.

The first prosecution under the "illegal obtainment" provision of Article 253(a), in 2009, involved a defendant from Zhuhai who "illegally purchased a detailed log of telephone calls made by high-ranking local government officials, then sold it to fraudsters who used it to impersonate the officials over the telephone", obtaining transfers of money from their friends or relatives because of an alleged emergency situation. He was sentenced to 18 months in prison and fined.[6]

---

[4] Donald C. Clarke, *The Peter Humphrey Case: My (Preliminary) Take*, Chinese Law Prof Blog, August 12, 2014, http://lawprofessors.typepad.com/china_law_prof_blog/2014/08/the-peter-humphrey-case-my-preliminary-take.html

[5] The sole remaining case -- which we have not been able to independently verify -- is said to have involved six pieces of personal information, which Professor Clarke suggests probably represents an "usual" fact pattern.

[6] *Zhou Jianping Case*: First Instance Criminal Judgment No. 612 of 2009, People's Court of Xiangzhou District of Guangzhou Province, Zhuhai City; see Hunton and Williams LLP, 'New Chinese Tort Liability Law Contains Provisions Affecting Personal Data' (Hunton and Williams LLP Client Alert, January 2010).

The most significant previous prosecution under Article 253(a) was where Dun & Bradstreet's Chinese subsidiary, Shanghai Roadway D&B Marketing Services Co. Ltd., was fined one million yuan (US$160,640) and four former executives were sentenced to up to two years each in prison, and also fined, for illegally buying information on Chinese consumers.[7] The personal information purchased from insurance companies, banks and other marketers allegedly involved 150 million Chinese consumers. Dun & Bradstreet subsequently sold the company.

The following examples of court decisions under Article 253(a) are a small sample of the more typical prosecutions involving sale and purchase of personal information in commercial quantities, with both prison sentences and suspended sentences resulting.

- Twenty-three defendants, employees of a telecommunications company, illegally sold personal information including personal phone numbers of the company's subscribers. The court found that the sale infringed the legitimate rights and interests of the subscribers and caused serious damages and imposed jail terms ranging from 6 to 30 months.[8]
- Defendant Xu spent 500 yuan (US$80) to purchase over one million items of customer purchase information concerning a particular store from Zhang, who was prosecuted separately. Xu was convicted under article 253(a)2 for illegally obtaining personal information, and given a suspended one year sentence and a fine of 1,000 yuan (US$160).[9]
- In a similar case, Bai, in charge of personnel at a technology company, authorized the marketing manager (prosecuted separately) to purchase more than one million items of customer information for marketing purposes for 900 yuan (US$146). Bai later made a voluntary confession. The company was fined 30,000 yuan (US$5,000) and Bai was fined 10,000 yuan (US$1,600) and given a six-month suspended sentence.[10]

Implications of ChinaWhys and other cases for doing business in China

The principal conclusion of this article is that PRC courts have, to date, interpreted narrowly Article 253(a)1's prohibition on illegal sale or provision, restricting its application solely to state entities and other public facing industries. However, they have given Article 253(a)2 a broad interpretation,

---

[7] Shanghai Zhabei District Court, 28 December 2012; Kathy Chu, 'Dun & Bradstreet Fined, Four Sentenced in China' (*Wall Street Journal*, 9 January 2013) <http://online.wsj.com/news/articles/SB10001424127887323482504578230781008932240>.

[8] Beijing Second Intermediate People's Court, 5 August 2011; see McKenzie and Fang 'China's Online Data Privacy Rules Coming into Effect'.

[9] People's Court, Shanghai Pudong New District, Case Number (2013) PU Criminal First 1087 (2013); information provided by George Tian.

[10] People's Court, Shanghai Pudong New District, Case Number (2013) PU Criminal First 86(4) (2013); information provided by George Tian.

applying it to illegal obtainment of personal information by any individual or entity, regardless of their particular industry, and apparently without the need for a preceding prosecution under Article 253(a)1 or for the information to have originated from an Article 253(a)1 listed-entity.

It is important to note that irrespective of what role political factors may or may not have played in the ChinaWhys prosecution, the information purchased by the Humphreys was personal information of others and entitled to protection under PRC law. Closer scrutiny of ChinaWhys existing business practices in light of Chinese legal requirements should have raised a red flag with respect to these purchases. The many previous prosecutions under Article 253(a), and the diversity of circumstances under which they may occur, should also have been well known. To prevent such occurrences from affecting their operations in China, companies should review their internal privacy policy and practices to ensure their data collection and use policies and practices operate in full compliance with Chinese law.

Authors: Scott Livingston, Covington & Burling LLP, Beijing and Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia. *The authors would like to thank Steven Zhu and Susan Shao of Covington & Burling LLP for their research assistance in preparing this article.*