

# Tort liability for online privacy violations in China: The 2014 SPC Regulation

---

*Scott Livingston and Graham Greenleaf*

(2015) 136 *Privacy Laws & Business International Report*, 24-27.

*This article is the second of a two-part series examining the treatment of privacy under the Chinese civil law. In Part One, (Livingston, S and Greenleaf, G 'The emergence of tort liability for online privacy violations in China' (2015) 135 Privacy Laws & Business International Report, 22-24), we examined the historical development of the "right to privacy," and its application in the online setting. In Part Two, we examine the October 2014 promulgation entitled "The Supreme People's Court Regulations Concerning Some Questions of Applicable Law in Handling Civil Dispute Cases Involving the Use of Information Networks to Harm Personal Rights and Interests" (SPC Regulation), and its impact on the development of tort liability for online privacy violations in China.*

As discussed in Part One, China's *Tort Liability Law* (TLL) includes two articles protecting an individual's right to privacy. In Article 2, a civil right of action is provided for violation of certain individual "civil rights and interests" among which is an individual's "right to privacy."<sup>1</sup> In Article 36, these civil rights and interests are specifically protected from online infringement.

Yet despite the availability of this civil right of action, there have been few reported cases to date involving Article 36's protection of an individual's "right to privacy."<sup>2</sup> As discussed in Part One, it is believed that this is because Chinese courts may not have understood how to apply Article 36 to privacy matters, and so may have been unwilling to accept such cases.

In a bid to clarify this uncertainty, China's Supreme People's Court (SPC) promulgated the SPC Regulation on 23 June 23, 2014. The SPC Regulation, which became effective on 10 October, 2014, clarifies procedural questions relating to Article 36 while also taking the opportunity to add several new substantive provisions. It was accompanied by some illustrative cases.<sup>3</sup>

The release of the SPC Regulation comes as Chinese authorities are increasing their administrative supervision of the Internet, and amidst a high-profile crackdown on online 'rumours' and other content deemed harmful to the State. By issuing the SPC Regulation, China's highest court seems to be implicitly promoting what it considers to be a 'healthy' online ecosystem by providing another mechanism to ensure network service providers strictly monitor content transmitted or published on their networks.

---

<sup>1</sup> Although this article will emphasize the "right to privacy" aspect of Arts. 2 and 36, the "civil rights and interests" protected in these provisions are much broader than simply the "right to privacy," encompassing such additional rights as the "right to reputation," and "right to life," as well as various intellectual property rights such as copyright or patent ownership.

<sup>2</sup> To date, the bulk of Article 36 cases have involved claims of online IP violations.

<sup>3</sup> The SPC released with the Regulation a set of eight representative cases involving, inter alia, aspects of an individual's "right to privacy" or "right to reputation," to illustrate its major provisions. They do not add anything to its substantive content on privacy.

## Procedural Provisions of the SPC Regulation

Much of the SPC Regulation focuses on providing guidance for a number of procedural questions relating to civil suits brought under Article 36 of the TLL. This includes such issues as determining which court has jurisdiction (Art. 2), the joinder of network users to an action against a network service provider (or vice versa) (Art. 3), and, where necessary, the compelled discovery of the personal identity of network users (Art. 4).

Of these, the most noteworthy is likely to be Art. 4, which permits a People's Court to order a network service provider to turn over the personal information of an online user on the "basis of a request by the plaintiff and the concrete circumstances of the case." In an interview with Xinhua news, Yao Hui, Vice President of the First Civil Chamber of the SPC, eloquently stated that "when persons carrying out infringing acts online are hidden in the shadows, and publish posts without gods and ghosts knowing about it, it is often difficult to determine the defendant when persons suffering an infringement want to file a complaint."<sup>4</sup> Article 4 was therefore added to ensure that online tortfeasors<sup>5</sup> could not take refuge behind a mask of Internet anonymity to violate the rights of others.

PRC Internet laws have long required network service providers to notify authorities and turn over user information in circumstances where illegal content has been posted on their networks. To our knowledge, this is the first provision in Chinese law that permits a private citizen to request another's private information from a network service provider. The addition of Article 4 clarifies that when content appearing online damages the rights and interests of an individual, then the affected individual has the right to force the allegedly infringing party to face a court of law – and to face them.

## Substantive Provisions of the SPC Regulation

Unlike court rules or Practice Directions in common law jurisdictions, these SPC Regulations also provide detail to the substantive law of the legislation under which the Regulations are made. These details, which we discuss below, clarify that circumstances in which tort liability may be assessed for the illegal disclosure of personal information, and provide further guidance for certain other matters involving online privacy and reputation.

### Civil action for disclosure of personal information online, with exceptions

Article 12 of the SPC Regulation states that disclosure of an individual's "personal information" or disclosure of certain sensitive information<sup>6</sup> such as health, medical history, or criminal records, will be actionable under the TLL if it causes a harm to a natural person, unless it meets one or more of the following exceptions:

---

<sup>4</sup> Luo Sha, Xu Wei, "Standardizing Case Trials of Online Torts, The Supreme People's Court Issues a Judicial Interpretation," Xinhua News, October 10, 2014, available at: <https://chinacopyrightandmedia.wordpress.com/2014/10/10/xinhua-standardizing-case-trials-of-online-torts-the-supreme-peoples-court-issues-a-judicial-interpretation/>

<sup>5</sup> An individual who commits a wrongful act that injures another and for which the law provides a legal right to seek relief.

<sup>6</sup> The first paragraph of Art. 12 reads in full: "Where network users of network service providers use the network to publicize genetic information, medical history materials, health inspection materials, criminal records, household addresses, private activities and other personal information or personal privacy of natural persons, resulting in harm to the other person, and the person suffering infringement demands they bear tort liability, the People's Court shall support this."

1. The relevant individual has agreed to the publication in writing and the publication takes place within the scope of this agreement;
2. The publication is intended to spur the social public interest, and is within the scope of necessity;
3. The publication is made by schools, scientific institutions, etc., for the purposes of scientific research for the public interest, or for statistical purposes, with the written agreement of the natural person, and the method of publication does not allow the identification of a specific natural person;
4. Where the personal information has already been published online by the relevant individual, or has been lawfully published by other means;
5. Where the publication involves personal information that is obtained through lawful channels; or
6. The publication is excused by other laws or administrative regulations.

As noted in Part One, China's main action to date against the illegal disclosure of personal information has been through enforcement of the illicit sale and purchase provisions of Article 253(a) of the PRC Criminal Law.<sup>7</sup> Civil actions under the TLL's Article 2 or Article 36, by contrast, have been fairly limited. The addition of Article 12 to the SPC Regulation clarifies that a tort remedy exists for individuals to proceed against network service providers or network users for unlawful disclosure of personal information, and brings China's civil law jurisprudence in line with similar personal information protections provided by China's administrative and criminal laws.

### **Content requirements for valid removal or blocking notices**

Article 36 of the TLL provides that a tort victim may notify a network service provider of an alleged privacy violation in order to request the removal or blockage of that offending information. However, the type of notice required to effect such action is not addressed in the law and it is unclear what form such user notice should take. Article 5 of the SPC Regulation clarifies the issue by stating that a notice will be deemed valid by a People's Court if it contains:

- a.) the name and contact method of the notifier;
- b.) the network address where it is demanded that necessary measures are taken, or related information sufficient to pinpoint the infringing content; and
- c.) the reason the notifier demands deletion of the corresponding information.

If a notice received by the network service provider does not meet these requirements, then the network service provider may be exempted from liability by a People's Court.

Crucially, the SPC Regulation does not address how a network service provider is to assess the validity of a received notice. After all, one can easily imagine a situation where a large network service provider, Google for instance, receives hundreds of requests for removal or blockage, not all of which will be valid. In such a situation, how should the network service

---

<sup>7</sup> Livingston, S and Greenleaf, G "ChinaWhys and wherefores: Illegal provision of personal data under Chinese law" (2014) Privacy Laws & Business International Report, Oct 2014, p. 1-5. (Examining China's use of Article 253(a) of the PRC Criminal Law to prosecute instances of illegal purchase or sale of a citizen's personal information).

provider respond? The SPC Regulation provides no answer and it remains to be seen how liability will be determined in circumstances where a network service provider has received an Article 5 notice but has independently determined that the covered content is non-violative of another's civil rights. Since Chinese law lacks a concrete definition of the "right to privacy," network service providers will have few guideposts by which to review and judge these potential privacy removal and blockage claims.

Finally, it is worth noting that Article 5 of the SPC Regulation has the potential to allow a Chinese equivalent of the European Union's so-called 'right to be forgotten' to develop, if it is used in relation to TLL Article 2. This bears watching over time.

### **Network Service Providers: "Timely" responses and "knowledge"**

Under Article 36 of the TLL, a network service provider may be held liable for infringement of an individual's civil rights by a network user of its services under two circumstances. First, under Article 36(2), where the network service provider has received notice from the tort victim, but failed to "timely" remedy the alleged violation. Second, where no notice has been received, but where the network service provider "knew" that a network user was infringing the rights of another person through its network.

The SPC Regulation provides additional clarity for both of these terms, addressing when a response to a request for removal or blockage is "timely" and under what circumstances a network service provider shall be deemed to have "known" of a rights violation occurring on their platform.

Under Article 6, courts are instructed to determine the "timeliness" of a network service provider's response to a request for removal or blockage based on a comprehensive appraisal of the existing circumstances, including "the nature of the network service, the form of valid notification and its degree of accuracy, the type and extent of the infringement of rights and interest through online information, etc." The lack of quantitative guideposts found in this interpretation suggests that People's Courts will have a great deal of discretion to determine "timeliness" based on the specific facts of each individual case.

In the absence of notice from the victim, the time at which a network service provider is deemed to have "known" of a rights violation, is to be determined based on a comprehensive consideration of several factors relating to the content, accessibility and management of the offending information (Article 9). These factors mainly involve assessing the online reach of the offending information (e.g., the number of unique visits or whether the network service provider ranked, recommended, or otherwise processed the offending information) and the internal processes of the network service provider for managing content available on its networks.

The emphasis on self-monitoring found in the SPC Regulation follows renewed attention from China's internet regulators to the self-monitoring practices of network service providers. In August 2013, for example, six major Chinese websites launched a joint site dedicated to eradicating "online rumours," under which users could submit or forward potentially harmful content for review and verification.<sup>8</sup> This move came amidst a larger government anti-rumour campaign targeting potential channels of unhealthy or illegal content.

---

<sup>8</sup> See e.g., Tim Hume, "Chinese Web Giants Join Forces in Crackdown on Online Rumors," CNN, August 2, 2013, available at: <http://www.cnn.com/2013/08/02/world/asia/china-online-rumor-crackdown/>

As China's network service providers are already tasked with scanning their networks for content harmful to the State, the addition of a requirement to monitor content potentially infringing another's civil rights is likely to further increase their operational costs and burden.

### **Prohibition on commercial slander**

Over the last few years, China has seen a number of high-profile cases involving claims of media extortion. In April 2015, a leading Chinese business newspaper, 21st Century Herald, was shut down by authorities following allegations of extortion. Under the alleged scheme, 21st Century Herald would publish negative reports about Chinese companies, which would be removed only after the targeted company paid off the newspaper by purchasing advertising. Using this approach, the paper is said to have netted tens of millions of dollars from targeted companies.<sup>9</sup> China's own state-run television channel, China Central Television (CCTV) has also been the target of several investigations over various bribery and graft allegations, including claims that the station would provide positive coverage in exchange for cash bribes.<sup>10</sup>

To combat such acts, the SPC Regulation inserts a new substantive provision in Article 11 stating that the People's Court should accept any cases where a network user or network service provider has libelled or slandered a commercial entity, "lowering the social valuation of their products or services." Although this provision is not related directly to individual privacy, it is likely to increase use of the Regulation, and thus its familiarity to Chinese courts and practitioners.

### **Prohibition on payments to remove privacy infringements or commercial slander**

In support of Article 11, Article 14 provides that where a network user or network service provider has committed an infringement of privacy (or of another right), then any agreements they may have entered into with the person suffering the infringement, by which content would be taken down in exchange for remuneration, will be found unenforceable. This provision covers both agreements with natural persons as well as businesses.<sup>11</sup>

### **Publications by State organs as privacy breaches**

Although various criminal and administrative laws have protected information submitted to government officials,<sup>12</sup> China's civil law has not previously clarified whether (or when) publication of personal data created by State organs might constitute an actionable privacy breach. In some jurisdictions outside China, this matter is dealt with through provisions in

---

<sup>9</sup> Te-Ping Chen, "China Closes 21st Century Business Herald's Website," Wall Street Journal, April 30, 2015, available at: <http://www.wsj.com/articles/china-closes-21st-century-business-heralds-website-1430402223>

<sup>10</sup> Edward Wong, "CCTV, China's Propaganda Tool, Finds Itself at Center of Antigraft Drive," New York Times, Feb. 13, 2015, available at: <http://www.nytimes.com/2015/02/14/world/asia/cctv-china-central-television-corruption.html>

<sup>11</sup> In January 2015, China's Cyberspace Administration of China, Ministry of Industry and Information Technology, and other ministries launched a campaign to end the quid-pro-quo practice of deleting online posts for money. See e.g., [http://www.thepaper.cn/newsDetail\\_forward\\_1296314](http://www.thepaper.cn/newsDetail_forward_1296314)

<sup>12</sup> The previous laws include the Supreme People's Court *Provisions on Several Issues regarding the Hearing of Administrative Cases Involving Public Government Information* (2011), providing that citizens can take administrative actions against State agencies which publish information interfering with their privacy, and the National People's Congress Standing Committee 2012 Decision which prohibits State agencies or their employees from disclosing, selling or illegally providing to others citizens' personal electronic information. For details see G Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pgs 221-23 'Public sector personal information in China'.

data privacy laws on when ‘publicly available information’ can also constitute ‘personal information’.

Article 13 of the SPC Regulation provides that where a network user or network service provider “publishes information from sources such as documentation created by State organs according to their duties and openly carried out official acts, etc.” then they may still be liable for privacy infringement if one of four factors is present in the information published: (i) it does not ‘conform to’ the source; (ii) it will ‘cause misunderstanding’ because of added content or comments, or how it is presented; (iii) it has been publicly corrected, but “the network user refuses to correct it, or the network service provider does not correct it”; or (iv) the information has been publicly corrected but the network user or network service provider “continue to publish the pre-correction information”. The conditions are broad and overlapping, but they make it clear that republication of official information may carry risks of privacy infringements for both individuals and network service providers. These are in addition to existing risks of publishing State secrets.

## Remedies

Articles 16-18 deal with the remedies available against both network users and network service providers. They included requirements to make apologies and restore reputation, with the Court able to publish its own ‘online declaration’ concerning a matter, or publish court documents, if this becomes necessary (Art. 16). Where infringements result in “asset losses or grave spiritual harm”, compensation may be required (Art. 17), and may include reasonable expenses and lawyer’s fees of victims (Art. 18). Where it is not possible to assess asset losses or an account of profits, the Court may make its assessment up to 500,000 yuan (US\$80,000).

## Understanding who is a Network Service Provider

As no set definition exists for the term “network service provider,” its scope can only be determined with reference to other usage in PRC law. In addition to appearing in the TLL and SPC Regulation, the term “network service provider” is also used in the 2012 Decision of the Standing Committee of the National People’s Congress on Strengthening Online Information Protection (“Online Information Decision”), China’s highest-level data privacy promulgation.<sup>13</sup> There, Article 6 refers to both “[network service providers] providing website access service,” as well as “[network service providers] providing Internet publication services.” This context suggest that the term “network service provider” is meant to encompass, at the least, both Internet content providers such as websites, as well as network access providers such as China Mobile. Other usage of the term in Chinese laws and regulations, and in related court decisions, confirm this understanding.<sup>14</sup>

---

<sup>13</sup> For further discussion of this law see “China Enacts New Data Privacy Legislation,” *Covington E-Alert* January 11, 2013 (Covington & Burling, available online); G Greenleaf *Asian Data Privacy Laws* (OUP, 2014), Chapter 7.

<sup>14</sup> See e.g., “Five Model Cases Published by the Supreme People’s Court,” June 2014. (“作为专业视频分享网站的土豆网是影响力较大的专业网络服务提供者,” (“Tudou, as a professional video sharing website, is a professional network service provider with particularly large influence.”))

## Conclusions

In privacy disputes, use of the Criminal Law article 253(a) by authorities<sup>15</sup> is still more common in China than civil litigation between private parties. Although civil law privacy rights have had not yet had a major commercial impact, and have been used mainly in inter-personal conflicts, the SPC Regulation have the potential to change this, and to place civil actions far more in the centre of the resolution of privacy disputes in China. The regulation leaves many key terms undefined, which will cause difficulties for businesses, particularly network service providers. Nevertheless, it give explicit guidance on many key points to all of China's courts in how to deal with such cases, which will both encourage potential litigants and their lawyers to commence cases, and encourage the courts to deal with them. The Regulation's specific reference to compensation up to 500,000 yuan (US\$80,000), where financial harm or undue profits cannot be ascertained, may encourage courts to be more generous with compensation than they have been as yet.

---

<sup>15</sup> S Livingston and G Greenleaf 'China Whys and Wherefores – Illegal Provision and Obtaining of Personal Information Under Chinese Law' (2014) 131 *Privacy Laws & Business International Report* 1-5