

Legal Updates & News

Bulletins

Data Privacy in China: Civil and Criminal Law Developments

January 2010

by [Arthur Dicker](#), [Paul D. McKenzie](#), [Gordon Milner](#)

Related Practices:

- [Privacy and Data Security](#)

Data Privacy in China: Civil and Criminal Law Developments

Legal assistant Fang Jingxiao in the firm's Beijing office provided valuable assistance on this article.

China, like many jurisdictions, has been grappling with the issue of how to protect personal information and data at a time when information tools are becoming increasingly pervasive and sophisticated. People's Republic of China ("PRC") law has not traditionally included robust rights of privacy that can be built upon to take account of modern information technology, although certain notions of an individual right to privacy can be derived from the *PRC Constitution* and other legislation.

China does not have comprehensive national law focusing exclusively upon the regulation of data privacy. In 2003, the Chinese government began considering the need for such legislation by commissioning a group of legal scholars to prepare what became in 2005 the draft Personal Information Protection Measures (the "Measures"). The Measures have not been adopted to date, and various local governments and courts have taken steps in the interim. Please refer to our earlier client alert for a more detailed discussion of the Measures as well as local regulations and judicial interpretations at:

http://www.mofo.com/international/CN_en/news/15332.html.

Significant changes occurred in 2009 with the promulgation of amendments to the *Criminal Law* (the "Criminal Law Amendments"), which included sanctions for the unlawful disclosure or acquisition of certain kinds of personal data. Over the past seven years, China circulated multiple drafts of a new *Tort Liability Law* (the "Tort Law") with relatively far-reaching provisions governing data protection and privacy rights. The Criminal Law Amendments and the last draft of the Tort Law are also discussed in the client alert referred to above.

On December 26, 2009, the Standing Committee of the National People's Congress adopted the Tort Law, which will come into effect on July 1, 2010. On the criminal law front, prosecutors have already started to pursue prosecutions under the data privacy provisions of the Criminal Law Amendments, with one case in particular drawing media attention.

This client alert outlines the significance of promulgation of the Tort Law and discusses the import of the recent criminal case.

Tort Liability Law

The final Tort Law promulgated on December 26 confirms the material provisions cited in our previous client alert:

- The right of privacy is a unique type of right separate from other civil rights and interests, although the definition of privacy and the scope of the right are not described in detail.
- Infringement of the right of privacy can give rise to a private right of action for civil damages (*i.e.*, a tort claim).
- A party whose right to privacy is infringed is entitled to claim from the tortfeasor the profits arising from

the breach as well as damages for emotional harm.

- A website operator who either recognizes that a party's privacy or other rights are being infringed through content posted on the operator's website or who is warned of such infringement by an affected party and fails to remove the content or adopt other corrective measures, is jointly and severally liable with the party having posted the content.
- If an affected party requests registered information about the party having posted infringing content and the website operator refuses to divulge such information, the website operator itself becomes liable for the infringement.

One additional subject matter related to privacy protection addressed in the final version of the Tort Law that was not included in the draft discussed in our prior alert concerns protection of the data privacy of medical patients. The Tort Law requires medical institutions to establish and keep various types of medical records and hold such records private and confidential. A patient has the right to bring a tort claim against a medical institution or its personnel for damages resulting from the unauthorized disclosure of the patient's medical records by the medical institution or such personnel.

On balance, the most significant development from the privacy provisions of the Tort Law is the creation of a new private right of action of an individual to claim damages for breach of his or her privacy right. Whereas past attempts to address misappropriation of personal data had to invoke attenuated references to the *General Principles of the PRC Civil Law* (the "General Principles"), these General Principles, along with the *PRC Constitution* and other PRC Civil Code measures, never recognized a private right of action for a breach of one's relatively amorphous "right of privacy."

We expect that future judicial and legislative interpretation of the Tort Law and new legislation will further clarify the nature of this private right of action, presumably in line with the General Principles which are applied to other private rights of action. In particular, we note that the Tort Law explicitly reaffirms one of the general precepts of Chinese law that an employer is responsible for the actions of its employees in the course of performing their work-related tasks, and thus if those actions result in the infringement of an individual's privacy right, the employer may be held liable.

Criminal Conviction in Southern China

On January 3, 2010, a court in the southern Chinese city of Zhuhai reportedly convicted a Chinese citizen of the illegal acquisition of someone else's personal information. The individual was sentenced to one and a half years in prison with a fine of 2,000 Renminbi. The case has been described as the first conviction in China under the Criminal Law Amendments.

The case involved a Chinese private citizen who purchased a detailed log of telephone calls made and received by high-ranking local government officials and sold the information to fraudsters who used it to impersonate the officials and convince their friends and relatives that they needed money due to emergency circumstances. Several individuals then transferred money to a bank account under the control of the fraudsters. The fraudsters were convicted of fraud and the individual who purchased and resold the telephone log to the fraudsters was convicted for the illegal acquisition of the personal information of those government officials.

The case is important for its interpretation of the term "severe circumstances" as used in the Criminal Law Amendments. Under Article 7 of the Criminal Law Amendments, a wrongdoer is to be convicted only when, among other things, the circumstances of the case are severe. The language leaves room for interpretation as to how the courts should consider the relevant circumstances to be severe, but presumably the factors could include both the manner in which the information is obtained and the harm which results from misuse of the information.

The case at hand demonstrates the court's belief that one possible set of severe circumstances could be when stolen personal information is later used to commit another crime. This interpretation may soon be reaffirmed in another case in the city of Hangzhou, where a person has been arrested (though not yet convicted) under the same provisions for the sale of personal information of automobile owners to a third party. Purportedly, the information was later used by the third party to engage in blackmail. Another factor which could have led the court in Zhuhai to consider the circumstances to be severe is the target of the stolen information, which were high-ranking local government officials. It will be interesting to see whether a court would consider a different set of facts to be severe, for example where the information was not used to

commit a crime but an individual or company nevertheless suffered large monetary losses as a result.

Companies doing business in China should carefully evaluate their business strategies and internal control procedures in light of the potential risks presented by the data privacy provisions of the newly enacted Tort Law and recent judicial interpretations such as the case in Zhuhai. We will continue to monitor developments in this field and update our clients on what those developments could mean for operations in China.

© 1996-2008 Morrison & Foerster LLP. All rights reserved.