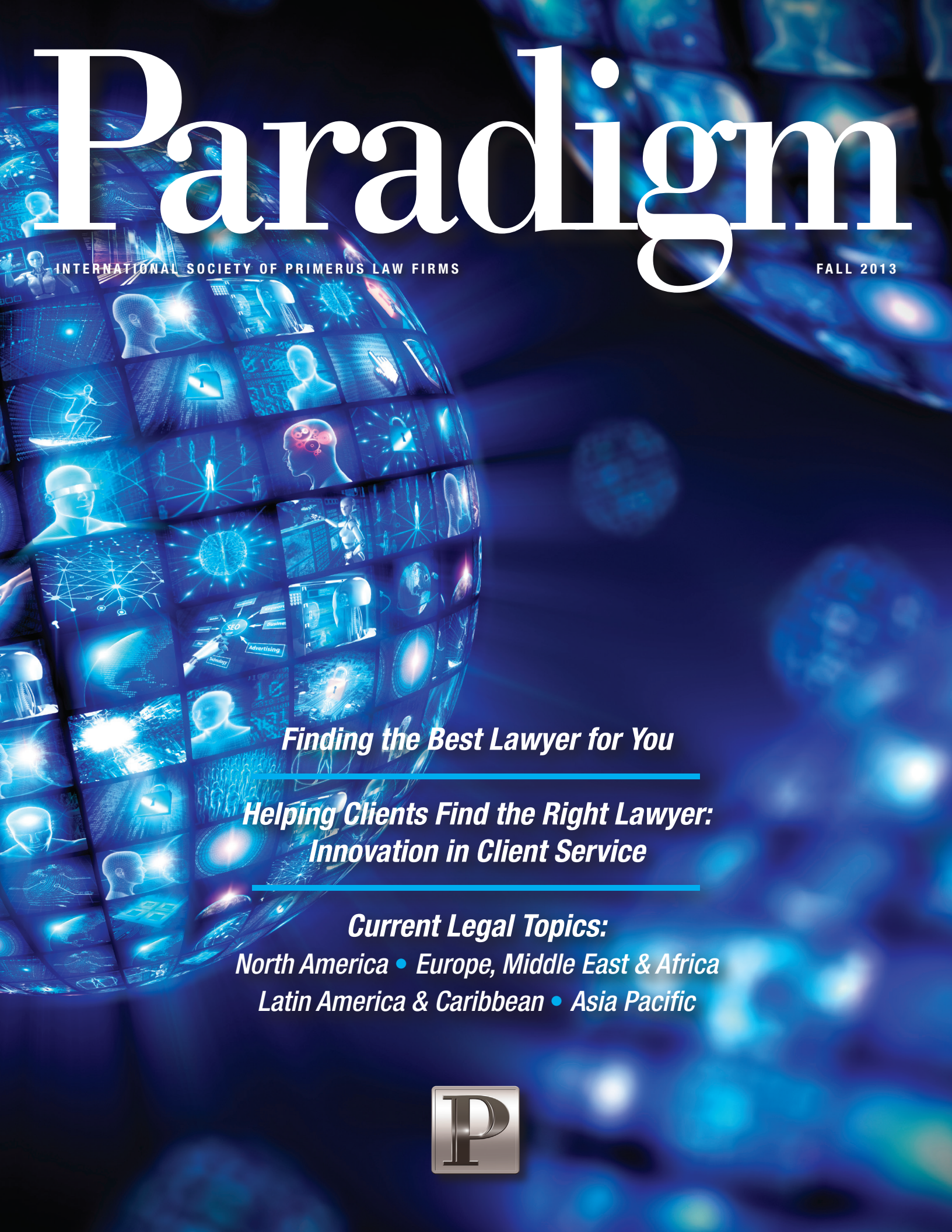
Paradigm

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

FALL 2013



Finding the Best Lawyer for You

Helping Clients Find the Right Lawyer: Innovation in Client Service

Current Legal Topics:

North America • Europe, Middle East & Africa

Latin America & Caribbean • Asia Pacific

Caroline Berube

The Development of Data Protection in China

Introduction

China recently increased its focus on data protection issues, in particular, those regarding personal information submitted electronically. Although China does not yet have a comprehensive national data protection plan, the Government has published a number of administrative regulations and related advisory rules over the past year that have significantly advanced data protection issues in China.

These regulations, some of which are binding and some of which are merely advisory, will likely become the foundation on which China's data privacy laws are built. Therefore, foreign companies will benefit from familiarizing themselves with these policies, even those which are not binding, as the principles will likely be incorporated into subsequent regulations.

History of Data Protection in China

Until recently, data protection was only addressed at a national level in certain provisions of general Chinese regulations. This section summarizes the scope of data protection under these regulations. While the scope of data protection has been extended by subsequent legislation, these regulations still remain valid.

Chinese Criminal Law

The most explicit data protection provisions are set forth in the Criminal Law of the People's Republic of China (the "Criminal Law") which prohibits any person from obtaining the personal information of any Chinese citizen by theft or other illegal means.

Additionally, the Criminal Law prohibits private organizations and their employees from selling or otherwise illegally providing personal information of any Chinese citizen they obtain during the course of performing their services. This provision had originally only applied to government agencies, but was extended in 2009 to apply to private organizations involved in the financial, telecommunication, transportation, education and medical sectors.

Tort Liability Law

The Tort Liability Law of the People's Republic of China (the "Tort Law") also contains provisions regarding data protection. Article 2 of the Tort Law includes a right to privacy in the definition of civil rights. Accordingly, any person whose personal information is improperly obtained and/or disclosed may be entitled to file a claim under the Tort Law.

It should be noted that, although both the Criminal Law and Tort Law contain provisions addressing data protection, there have not been any detailed guidelines or interpretations regarding the enforcement of such provisions. Therefore, these have had only a limited impact on the enforcement of data protection in China.

Development of Data Protection Regulations

In 2012, the Chinese authorities issued a number of rules, regulations, and advisory guidelines regarding data protection. This section summarizes the two primary national regulations issued by the Chinese authorities and discusses their impact on

Caroline Berube's practice focuses on Chinese corporate law and commercial practice. She is especially well-regarded for advising clients on the Asian legal structure of their companies, based on her sound understanding of the pitfalls and advantages of most Asian jurisdictions. She has advised clients in various industries such as manufacturing, energy (oil, gas and mining), technology and services.

HJM Asia Law & Co LLC
B-1002, R&F Full Square Plaza No. 16,
Ma Chang Road
ZhuJiang New City Tianhe District
Guangzhou, China 510623
+8620 8121 6605 Phone
+8620 8121 6505 Fax
cberube@hjmasialaw.com
www.hjmasialaw.com

the development of data protection in China.

Decision on Strengthening the Protection of Internet Data

On December 28, 2012, the Standing Committee of the National People's Congress published the Decision on Strengthening the Protection of Internet Data (the "Decision"). The Decision sets forth requirements for certain internet service providers ("ISPs"), telephone companies, and other organizations, including government agencies, that collect personal information in digital form in the course of providing services (collectively "Data Collectors").

In particular, the Decision requires that Data Collectors:

i. Inform individuals of the purpose, manner and scope of their collection of electronic personal information;

ii. Obtain consent from users before collecting electronic personal information;

iii. Strictly maintain the confidentiality of all electronic personal information collected during the course of their business;

iv. Develop and publish policies for the collection and use of electronic personal information; and

v. Take immediate remedial measures and notify the competent authorities in the event of a discovered or suspected disclosure or leak of the stored electronic personal information.

Data Collectors that fail to comply with the above-listed requirements may be subject to fines, confiscation of any illicit gains, revocation of licenses and registrations, termination of websites, as well as potential civil liability to the affected users.

The Decision contains one provision that may be counterproductive to the protection of personal information. This provision, often referred to as the "Real Name Provision," requires that users provide their real names when entering into an agreement for the provision of services.

While the Decision is the first national, binding regulation regarding data protection, it contains only 12 broadly worded articles. Therefore, Data Collectors will probably have to wait for an official guideline or interpretation regarding the implementation impact of these requirements, including the Real Name Provision.

Guideline for Personal Information Protection Within Information Systems for Public and Commercial Services

On November 15, 2012, the Ministry of Industry and Information Technology (the "MIIT") issued the Information Technology Security – Guideline for Personal Information Protection Within Information Systems for Public and Commercial Services (the "Guideline"). Although the Guideline is not legally binding, it is relevant insofar as it provides the basic principles on which further regulations will likely be based.

The Guideline provides the first national definition of "personal information," which it defines as "information that can identify users independently or in combination with other information." The Guideline also identifies two categories of personal information: sensitive personal information," which is information that, if disclosed, could have adverse effects on the individual, and "general personal information," which includes all other personal information.

Additionally, the Guideline provides eight principles that should be followed in the handling of personal information:

i. Organizations should have a clear and justifiable purpose for collecting personal information;

ii. Organizations should collect the minimum amount of data required for such purpose;

iii. Organizations should publish the purpose, manner, and scope of their personal information collection;

iv. Organizations must obtain express consent before collecting sensitive personal information;

v. Organizations must ensure that all information collected is complete and up-to-date;

vi. Organizations shall strictly maintain the confidentiality of personal information and take appropriate measures to ensure that such personal information is kept secure;

vii. Organizations shall no longer use personal information once the original purpose for which it was collected has been completed; and

viii. Organizations must establish and implement appropriate internal policies for the maintenance of personal information.

It is worth noting that many of the above-listed principles mirror some of the requirements established in the Decision.

While the Guideline came into effect on February 1, 2013, no official text has been released. Also, it is important to remember that the Guideline is not legally binding. Nevertheless, the Guideline is the first national standard for data protection that applies to all industries, and therefore should be reviewed by all companies in the development of their data protection policies and procedures in China.

Conclusion

China recently increased its focus on data protection issues, in particular, those regarding personal information submitted electronically. Although China does not yet have a comprehensive national data protection plan, the Government has published a number of administrative regulations and related advisory rules over the past year that have significantly advanced data protection issues in China.

These regulations, some of which are binding and some of which are merely advisory, will likely become the foundation on which China's data privacy laws are built. Therefore, foreign companies will benefit from familiarizing themselves with these policies, even those which are not binding, as the principles will likely be incorporated into subsequent regulations. P