

Update

Electronic growing pains

Cyber security and data protection in the People's Republic of China

Introduction

The protection of data, whether it be personal information or trade secrets, and the vulnerability of that data to misuse for commercial gain are issues that Governments all around the world grapple with. China is no exception, and with good reason. At the close of 2015, China had over 680 million active internet users and online retail transactions of over RMB 3877.3 billion. By 2020, China's e-commerce market is predicted to be larger than those of the U.S., the UK, Japan, Germany, and France combined.

With the huge growth in internet subscribers and e-commerce in China, data protection and cyber security have become increasingly important. In February of this year it was reported that Taobao, China's largest online retailer, was the victim of a cyber-attack in which hackers successfully compromised more than 20 million user accounts linked with the site. This is just one high profile example of the many data protection and cyber security issues that have arisen in China in recent years.

In this article we look at the current state of the law in China in relation to data protection and cyber security. We also look at the future of data protection and cyber security law and discuss proposed new laws. We then set out ten key questions companies operating in China should ask when considering their data storage and e-commerce policies.

does not currently have a stand-alone data protection or cyber security law. Instead, the rules around data protection and cyber security are fragmented across multiple laws and regulations, with oversight typically left to industry-specific regulators.

General law requirements

At the broadest level, data protection in China is afforded to all citizens through the Constitution of China which contains a general principle on protecting the freedom and privacy of correspondence. While the Constitution does not provide a cause of action in and of itself, the Tort Law of China gives individuals whose civil rights and interests have been infringed the right to make a claim against the infringing party. Such civil rights and interests include, among other things, the right to privacy.

The State may also bring an action under the Criminal Law, whereby there are various offences that relate to purchasing, selling or otherwise acquiring personal information of citizens.

The State also imposes privacy of information through the Resident ID Card Law, which requires businesses that collect identifying information of citizens contained on identity cards to keep such information confidential.

The Decision on Strengthening Network Information Protection (the "Act") provides more specific regulations on the collection and use of the personal data of citizens with companies subject to a range of penalties for failing to comply. In addition, the Act gives citizens a right to request their information to



¹ SOURCE - Dezan Shira & Associates China Briefing "Logging In: Understanding e-Commerce in China" March 24, 2016, Editors: Jake Liddle and Qian Zhou.

Data protection laws in China

China, unlike other Asia Pacific states such as Singapore and Hong Kong,

be deleted and provides a private cause of action for an infringement of their rights pursuant to the Act.

Industry specific requirements

China has enacted a number of industry specific regulations that provide additional rules. The most relevant of these regulations is the Consumer Rights Law, which imposes obligations on businesses in the collection and handling of consumers' personal information, the key requirement being that consumers' personal information cannot be collected without their consent. There also exists a significant range of industry-specific regulations within the telecommunication, banking, and healthcare sectors.

The guidelines

In 2013, in response to rapid growth in the use of data and the Internet, the government enacted the Information Security Information Guidance on Protection of Personal Information of Public and Commercial Service Information ("the Guidelines"). The Guidelines are a set of non-binding guidelines that apply to all private entities and are designed to protect the personal information of individuals. The Guidelines provide guidance on the collection, processing, transferring and deletion of personal information; how computer networks that handle personal information should be maintained; and the appropriate responses to take when information has been mishandled.

While the Guidelines are non-binding they are significant in that they are an amalgamation of current regulations and represent best practice within China.

Cyber security laws In China

In enacting regulations, China has tended to treat cyber security as a distinct issue to that of data protection. Current laws that do address cyber security tend to do so in an indirect manner. The first of these, the State Secrets Law, makes it an offence to improperly handle information designated a state secret. In January 2016 China also enacted the Anti-terrorism Law which is intended to identify people and activities, including those discussed online that threaten public and government security. Significantly, the Act requires that telecom operators and Internet service providers give technical support and assistance, including decryption solutions to police and national security authorities.

The future of data protection and cyber security law in China

The most significant development in cyber security is expected to come with the introduction of a law modeled after the Cyber Security Law of the People's Republic of China (Draft). The main objective of the Draft Law is to preserve national security by enabling the government to have more control over networks and data security. If enacted in its present form, the Draft Cyber Security Law will codify currently scattered Internet censorship rules, provide a comprehensive regulatory regime for cyber security and impose legal obligations on network operators and network service providers.

In addition, it is expected the insurance sector will also see the introduction of specific regulations with the recent release of the Draft Regulation of Information of Insurance Institutions in October 2015.

Ten key questions

Taking into account the regulatory regime in China, we set out below ten key questions companies operating in China should ask themselves when considering data protection and cyber security issues:

1. Are you responsible for the protection of personal information?

Chinese regulators have chosen to place the responsibility for data protection on the businesses that collect this data. Under the Guidelines, businesses that collect, process and retain the personal information of individuals have a positive duty to provide proper safeguards and protection for this information. This includes auditing internal security systems and having emergency plans in place in the event that data is leaked, lost, damaged, tampered or improperly used.

2. What type of information do you handle?

Not all information is equal and a central tenant of the Guidelines is the type of information that is handled. Information is categorized as either Personal Sensitive Information or Personal General Information. This categorization of information is significant because if the information is Personal General Information, the subject of that information may be deemed to give tacit consent to its collection and use (subject to a number of exceptions). If the information is Personal Sensitive Information express consent is required. The Guidelines provide a number of criteria to assess whether information is sensitive which broadly turns on the degree to which the information may identify or harm an individual if leaked. All other information that is not sensitive information is considered general information.

3. How do you collect information?

The Guidelines make it a point to note, repeatedly, that information should not be arbitrarily collected. The collection of information should be done with an informed purpose which is clearly and specifically stated. In collecting information there should be a clear method and process and only the minimum amount of information required to achieve the informed purpose should be collected.

4. Do you tell the user what you are doing?

Some things are best kept secret, but according to the Guidelines the fact that you are collecting personal information and what you are doing with that information is not one of them. The Guidelines require businesses to be transparent in their collection of information, such that information is not collected in a concealed or undisclosed manner, and relevant matters, as outlined in the Guidelines, are disclosed to the person whose information is being collected.

5. Do you ask permission first?

It is a primary requirement of the Guidelines that businesses receive consent to the collection and use of an individual's personal information.

Express consent must be received where:

- the information is considered personal sensitive information;
- the information is to be transferred to a third-party;
- the information is to be transferred overseas, even if that transfer is to a related entity;
- the information is personal sensitive information and it is to be retained after it has been processed;
- the information is to be retained for a period longer than disclosed to the subject of the information.

For general information the subject may be deemed to give tacit consent,

Further information

If you would like further information on any issue raised in this update please contact:

Richard Bell

Partner

E: richard.bell@clydeco.com

Clyde & Co

Level 23 - Shanghai Two IFC

8 Century Avenue

Shanghai, 200120, China

T: +86 21 6035 6188

F: +86 21 6035 6199

Further advice should be taken before relying on the contents of this summary.

Clyde & Co accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary. No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co.

© Clyde & Co 2016

except where the information falls under one of the above exceptions.

6. How do you process and manage information?

Although the Guidelines' rules for the processing of information are not as detailed as other sections they nevertheless stipulate a number of requirements. Primarily, there must be an established system for the processing of personal information and the information should only be processed for the purposes disclosed and consented to by the subject of that information. In addition, while the information is retained, it must not be assessed by anyone that does not have a connection with the purpose for which the information is being processed.

7. Do you allow the user to check their own information?

An aspect of the Guidelines which may be considered more related to cyber security, is the requirement that a business must keep a record of the personal information they possess and the status of that information. Correspondingly, the Guidelines also allow a person whose information has been collected the right to request whether the business retains any of their personal information, the contents of the information, and the status of processing that information. Where a person's personal information is incorrect the Guidelines provide that they have a right to request the correction of that information.

8. Do you transfer information to a third party or an associated entity?

It is common for companies to transfer information internally, to a related entity overseas, or to a third party. However, the Guidelines put some limitations on this. The Guidelines require that the subject of the information be informed of and consent to the transfer to a third-party or overseas, even if that transfer is to a related entity.

9. Do you delete information?

The Guidelines include provisions which provide that where a subject of information requests the deletion of their personal information with just reasons, businesses are required to delete such information. Moreover, businesses are also required to delete information once the informed purpose of collecting that information has been achieved or the disclosed time-limit has elapsed. Where it is necessary to retain the information beyond this period any identifying details of the information must be removed.

10. Have you got a user agreement?

Risks posed by cyber security issues can be mitigated through a correctly drafted user agreement. While that may involve some expense, having a user agreement that is up to date with the law and complies with best practice will often be the best defense against an action by the regulator or user.

Conclusion

China is a huge market for all things related to the internet and e-commerce. That market is growing, but with that growth comes the pain of potential security breaches and cybercrime.

With increasing requirements for data protection and cyber security, and increasing industry specific regulation, there is now a strong basis for companies to review their data protection and cyber security practices and policies. Companies, particularly those operating in multiple jurisdictions, must ensure they comply with Chinese specific regulations and not simply adopt practices and policies formulated for other markets. In addition, companies should be aware that data protection and cyber security are no longer issues to address on a one off basis, but rather are ongoing matters that should be continually audited and updated to ensure compliance.