AN A.S. PRATT PUBLICATION
FEBRUARY 2025
VOL. 11 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 2** **February 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Clarifications of Legal Bases for Cross-Border Data Transfers in Landmark Judgment by the Guangzhou Internet Court in China

By Sarah Kwong, Dan Wu and Amigo L. Xie

In this article, the authors discuss a Chinese court's judgment shedding light on the judicial perspective regarding cross-border personal information transfers, offering valuable insights for companies to consider.

The Guangzhou Internet Court in China (Court) recently released its judgment under the Personal Information Protection Law (PIPL),[1] Case No.: (2022) Yue 0192 Min Chu No. 6486) (Judgment),[2] setting a crucial reference in cross-border data transfers of personal information from China. It is said that this is the first court judgment in China on cross-border data transfer.

The Judgment sheds light on the judicial perspective regarding cross-border personal information transfers, offering valuable insights for companies to consider. Multinational companies must give significance to adapting their worldwide compliance strategies locally, especially through the revision of privacy policies and consent mechanisms, to align with Chinese regulatory requirements.

LOCALIZATION OF GLOBAL DATA PROTECTION POLICIES BASED ON DISTINCT LEGAL BASES

The Court's focuses on the defendants' "Customer Personal Data Protection Charter" and scrutinizes the information provided to users about data collection, processing, and transfer. The Judgment highlights the necessity for companies to localize their global data protection policies to align with PIPL requirements, as reliance on other jurisdictions' data privacy practices alone, for example the General Data Protection Regulation,[3] might not be considered to be sufficient. It is also important to adopt transparent and well-defined policies that outline specific purposes and scope of data processing to accurately lay out the legal bases for data processing, including cross-border data transfers.

---

* The authors, lawyers with K&L Gates, may be contacted at sarah.kwong@klgates.com, dan.wu@klgates.com and amigo.xie@klgates.com, respectively.

1 http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

2 https://mp.weixin.qq.com/s/iAgo-W6qe2-VO-ZpEbLKdg.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

COMPLIANCE REQUIREMENTS OF INFORMED CONSENT

The Judgment highlighted the importance of clear and comprehensive notifications to data subjects and proper separate informed consent, especially for cross-border data transfers where consent is the chosen legal basis. This is evident in the Court's examination as to whether the defendants adequately informed the plaintiff of the overseas recipients of the plaintiff's personal information.

COMPLIANCE WITH LEGAL MECHANISMS FOR CROSS-BORDER DATA TRANSFERS

The plaintiff initially demanded examination of the legal mechanism used by the defendants in their cross-border data transfers, including whether they had obtained necessary security assessments and certifications. Because the plaintiff later withdrew this demand and replaced it with a new demand during the proceedings, the Court did not opine on the legal mechanism. However, it is a good reminder that a legal mechanism and other key compliance points, such as records of processing activities and data protection impact assessments, in the context of cross-border data transfers are essential for demonstrating compliance with PIPL requirements and could be challenged by data subjects when there is a dispute.

PENALTY AND DAMAGES

In this case, the damages have been awarded to the plaintiff for the direct losses suffered (i.e., legal fee, translation fee and evidence collection cost in this case), but companies should also be aware of the potential administrative penalties imposed on them and personal liabilities imposed on their officers.

For general violations, companies can be subject to penalties including correction orders, warnings, and confiscation of illegal gains. The fines for violations are guided by ranges for companies who are data controllers and for any person in charge or any other individual of companies directly liable for the violation.

As for severe violations, the fines imposed on companies could be up to RMB50 million (around €6.5 million) or 5% of their last year's annual revenue, and companies can be ordered to suspend business activities or face license revocation; any person in charge or any other individual of the companies directly liable for the violation can be fined and may also be banned for a certain period of time from serving in leadership roles of the companies involved in the violation.

BACKGROUND

The Judgment was first delivered on 8 September 2023. In this case, the plaintiff, Zuo (Plaintiff), raised concerns about the Plaintiff's personal information being transferred out of China and shared globally without the Plaintiff's knowledge and separate consent

after he purchased a membership card from a Shanghai company (First Defendant) for discounted services of a French multinational hotel group (Second Defendant, collectively with First Defendant, Defendants) and used the Second Defendant's app to book a hotel in Myanmar, providing personal information and agreeing to the "Customer Personal Data Protection Charter" published by Second Defendant. However, the Defendants argued the personal information processing was necessary for contract performance and aligned with industry practices for global hotel services.

As mentioned above, the Judgment offers insights into the complexities of PIPL and the balancing of individual privacy rights with multinational companies' global operational needs. It also reflects a trend of increasing data protection regulations and enforcement in the China landscape. The Judgment serves as a reminder for multinational companies operating in China, as it stresses the need for a careful balance between global business operations and compliance with local data protection laws.

KEY ISSUES ADDRESSED BY THE COURT

In the Judgment, the Court addressed several key issues under the PIPL, particularly in areas such as cross-border data transfers, data subject's consent, and localization of data privacy protection policies.

These key issues are summarized below.

Actionability of the Case

One of the key issues addressed by the Court was the question of whether Plaintiff's case was actionable in the first place. Despite the Defendants' argument that Plaintiff had not directly approached them and exercised the Plaintiff's rights first before taking legal action, the Court took a broader view, distinguishing differences between an infringement of basic rights of a data subject and that of a data subject's right to access, enabling Plaintiff's case to proceed based on its merits. This clarified in what circumstances a data subject is required to exercise his rights against a data controller before he can seek judicial remedies and in what circumstances it is not.

The Legal Bases for the Defendants' Processing of Personal Information; the Requirement of Informed Consent

The Court highlighted that PIPL provides multiple legal bases for processing personal information, with consent being one of the several bases. The Court recognized that the Defendants' collection and processing of Plaintiff's personal information was primarily for the purpose of concluding and performing service contracts (for membership and hotel reservation services) and further clarified that contractual necessity, as one of the legal bases for processing personal information under the PIPL, stands on equal footing with consent. In other words, a data subject's consent is not required when there is the necessity for the conclusion and performance of a contract to which the data subject is a party.

However, the Court did not accept the Defendants' argument that this contractual necessity basis eliminated the need for separate consent of a data subject. This is because besides using the data subject's personal information for booking the hotel, the Defendants also collected and onward transferred the relevant personal information to data recipients in other jurisdictions for marketing purposes, which was not necessary for contract performance. The Court also rejected the Defendants' claim that their privacy policy disclosures were adequate to inform users and obtain consent. Instead, it emphasized the need for more detailed information about overseas recipients and onward transfers, and explicit consent for these specific cross-border data flows beyond general privacy policy acceptances in this context, prior to collecting and transferring the data internationally.

CRITERIA FOR DETERMINING DAMAGES

Regarding award of damages to the Plaintiff, the Court is of the view that under the PIPL, the assessment places emphasis on the expenses incurred to prohibit the infringement behavior. In particular, the Court determines what constitutes financial losses, e.g., reasonable expenses incurred by the infringed party to stop the infringement, such as the reasonable expenses incurred in the investigation or collection of evidence. The Court may also consider legal fees incurred.

In the present case, taking into account the reasonableness and necessity of expenses, the extent of fault committed by the Defendants, and the impacts on the Plaintiff's personal information (including how the personal information has been handled and the volume and extent of the personal information involved), the Court awarded damages in the sum of RMB20,000 (around €2,600) to the Plaintiff (inclusive of reasonable expenses).

CONCLUSION

As China continues to enforce its data protection regime, businesses should expect increased scrutiny of their data practices. Proactive compliance measures and a user-centric approach to data management will be crucial for navigating this evolving regulatory landscape.