AN A.S. PRATT PUBLICATION
MAY 2023
VOL. 9 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 4** **May 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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.

Roundup of International Privacy Laws

By Pavel (Pasha) Sternberg and Christina Hernandez-Torres*

In this article, the authors provide an overview of upcoming privacy law changes around the world to better position companies to meet their compliance obligations.

Recent years have brought a dramatic increase in the number of countries that have comprehensive privacy and data security laws. As the world has become increasingly digital, privacy and data protection have become a greater concern for consumers and governments alike. A regulatory scheme that was – as recently as only a few years ago – found primarily only in Europe is now seen across the globe.

It is no surprise then that companies whose business spans the globe are finding international privacy laws confusing and burdensome. This is especially true this year when countries like China, Brazil, India and Canada are set to further complicate the global data privacy stage. This article is focused on providing an overview of these upcoming changes to better position companies to meet their compliance obligations.

CHINA'S NOTABLE CROSS-BORDER DATA TRANSFER RULES UPDATE

China's Personal Information Protection Law was passed in 2021 and requires companies to have a comprehensive privacy compliance framework. Included in that framework is a restriction on cross-border data transfers. In June and July 2022, two regulators – the Cyberspace Administration of China (CAC) and the National Information Security Standardization Technical Committee – issued regulations for transferring data out of China.

The PIPL provides that personal information can be transferred outside China only after the data subjects have given their informed consent, the company carries out an impact assessment and an appropriate transfer mechanism is used. The transfer mechanism that is required depends on the type of data being transferred, the volume of individuals whose personal information is being transferred and the role played by the company conducting the transfer in the Chinese economy.

In many cases, this analysis will result in a company having to get a security assessment approved by the CAC. This is the case if:

(1) The data being transferred is "important data";[1]

* Pavel (Pasha) A. Sternberg and Christina Hernandez-Torres, attorneys with Polsinelli PC, may be contacted at psternberg@polsinelli.com and chernandez-torres@polsinelli.com, respectively.

[1] The regulations define this as "data that, once tampered with, destroyed, leaked, illegally obtained[] or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc."

(2) The company is a "Critical Information Infrastructure Operator";

(3) The company processes the personal information of more than one million individuals and transfers any of it abroad; or

(4) In a calendar year it transfers either 100,000 individuals' personal information or 10,000 individuals' sensitive personal information abroad.

To get an approved security assessment, a company will have to submit an application containing a self-assessment to the provincial CAC office, which will conduct an initial check and then send it to the national CAC office for approval. The entire process is supposed to take approximately 60 days.

In situations where a security assessment is not required, a company can conduct a cross-border transfer after either obtaining a personal information protection certification from a professional institution designated by the CAC or entering into a regulator-approved standard format data transfer agreement with the overseas recipient of the data being transferred. These cases are primarily for internal cross-border transfers within one multinational company or one economic/business entity, as well as for cross-border transfers by non-Chinese entities that analyze and assess the behavior of the individuals located in China subject to the extraterritorial jurisdiction of the PIPL.

The Chinese government's focus on data localization is made evident by these regulations. At a minimum, all three transfer mechanisms require controls around data security and the further use or disclosure of data once it leaves China. In cases where it is appropriate, the standard format data transfer agreement is going to be the easiest and simplest approach for cross-border transfers, but it brings with it the burden of ensuring that the contract is held up. To that end, companies should be aware that noncompliance with the PIPL is subject to hefty fines and has already been used aggressively. Most prominently, in July 2022, the CAC fined the company Didi Global just over 8 billion yuan ($1.2 billion) for violating cybersecurity and data laws.

BRAZIL'S WEBSITE COOKIES AND PERSONAL DATA PROTECTION GUIDANCE

Brazil's National Data Protection Authority (ANPD) previously was charged with issuing regulations to clarify the statute's requirements. Since then, the ANPD has issued a few guidance documents related to the statute. First, in January 2022, the ANPD issued a resolution that reduced the compliance obligations for so-called small-sized processing agents, including removing the requirement to appoint a data protection officer, simplifying the policies that they must have and lengthening the statutory timelines to respond to customer inquiries and data incidents.

Additionally, in October 2022, the ANPD provided nonbinding guidance on cookies and other tracking technologies that process personal data. This guidance provides that:

- Personal data is broader than basic identifiers like names and phone numbers, and the definition includes behavioral profiles that can be cross-referenced to other data sets.
- The only two legal bases for use of cookies are consent and legitimate interest.
- Cookie collection subject to a legitimate interest basis is subject to opt outs only in some situations. The guidance also suggests that analytics tools are acceptable on a legitimate interest collection basis.
- Advertising and behavior tracking cookies are not "necessary" tools and are therefore subject to consent.
- Notice informing individuals about the categories of cookies, their purposes, third parties involved, retention period, data subjects' rights and other requirements under the LGPD should be provided.
- First-level banners (user-facing banners on landing pages) with basic information followed by second-level banners (opened through first-level banners) can be implemented to simplify users' viewing experience.

As in China, companies should be aware that noncompliance with the LGPD will result in fines of up to 2% of a business's annual revenue to a maximum of 50 million Brazilian reais per violation (approximately $9 million).

OTHER PENDING INTERNATIONAL PRIVACY UPDATES

Canada

Canada is a country that has had a prominent privacy law, the Personal Information Protection and Electronic Documents Act, for many years. In June 2022, new laws – the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act – were proposed to modernize the current federal privacy framework. Together, these new laws recognize individuals' privacy rights while acknowledging the benefits of data collection and use, and they create an enforcement mechanism to balance these sometimes competing interests.

The proposal has to go through the legislation process and many changes may result from this, but at a high level, the goals of the statutes are to:

(1) Give consumers more visibility into how personal information is collected and used, and the ability to exert more control over those activities;

(2) Provide minors with extra protections and impose more limitations on the collection and use of their personal information; and

(3) Allow for the safe and regulated use of artificial intelligence when it comes to data processing.

Canada has traditionally been at the forefront of privacy law regulation, so monitoring the progress of this legislation will be important to understanding how regulations in this space will evolve over the coming years.

India

In August 2022, India withdrew a 2019 privacy bill because of the negative feedback received from businesses and privacy advocates on its stringent cross-border requirements. Just three months later, in November 2022, a replacement bill – the Digital Personal Data Protection Bill 2022 – was proposed. The updated proposal would create more user-friendly cross-border data transfer requirements for certain countries and territories, and it removes the requirement to store critical personal data in India that was included in the 2019 bill. The 2022 bill would also narrow the scope of data protection afforded to consumers compared with what was in the previous version.

TAKEAWAYS

It is becoming increasingly important for businesses to assess the countries from which they collect data and how they are transferring that data internally if those transfers involve crossing international borders. As always, they must also review and understand what data they collect as well as how that data is processed, used, shared and sold. The places where these activities occur and what those activities are will determine the rules that companies will have to abide by as compliance increasingly becomes a complicated and burdensome endeavor.