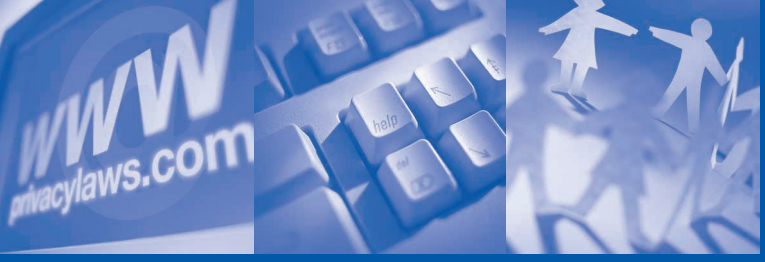

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

PIPEDA reform 3.0: Radical changes to Canadian privacy protection policy in new Bill

Canada's sweeping privacy reform strips the OPC of oversight of private sector. By **Colin J. Bennett**, Professor Emeritus at the University of Victoria, Canada.

On 15 June , the Government of Canada tabled Bill C36, establishing a new Protecting Privacy and Consumer Data Act (PPCDA), the latest attempt to reform the Personal Information Protection and Electronic Documents Act (PIPEDA) and establish a

Continued on p.3

China intensifies its enforcement of data protection

Yan Luo of Covington reports on China's enforcement of existing data laws in 2026.

In 2026, Chinese regulators have continued to enforce existing data laws in a more targeted and fact-specific manner. Recent cases and enforcement actions show three clear enforcement priorities: cross-border transfers of personal information; data collection and use by mobile applications (apps) and embedded Software Development Kits (SDKs); and data security incidents.

These developments indicate a focus on operational accountability. Regulators are increasingly examining

Continued on p.5

Issue 202 **AUGUST 2026**

See the publisher's blog at privacylaws.com/blog2026aug

INTERNATIONAL report

ISSUE NO 202 AUGUST 2026

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Colin J. Bennett
University of Victoria, Canada
Yan Luo
Covington, US
Sam Meijer and Rosalie Brand
Kennedy Van der Laan, the Netherlands
Joanna Mazur
University of Warsaw, Poland
Maisie Robinson
PL&B
Pablo Palazzi
Allende & Brea, Argentina
Graham Greenleaf
Macquarie University, Australia
Saket Bisani
Bisani Legal, India
Oladoyin Olanrewaju and Danielle Dobrusin
Hunton Andrews Kurth LLP, US
Elena Testa
Independent Consultant, Italy

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative + 44 (0)7507 658880.
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Changes ahead in the regulator line-up

While we still have no news about the appointment of a new term for the European Data Protection Supervisor, the current EDPS Wojciech Wiewiórowski (seeking reappointment) has commented on the EU's attempts to streamline the GDPR and the AI Act by means of the Digital Omnibus. At the CPDP conference in May (p.30), he said that simplification does not mean – and should not be understood to mean – deregulation. He also highlighted enforcement of the digital rulebook, and the need for a harmonised and coherent application of the EU legislative framework. This relates to the DPA cooperation which he says should be strengthened not only among EU Data Protection Authorities but should also take place at a cross-regulatory level across several legal fields (p.29).

The AI Act's enforcement is shared across various authorities. Read on p.8 how the EU DPAs are currently enforcing the EU AI Act. The EDPS wears two hats here – it is the AI regulator for EU institutions as well as supervises their data protection compliance under the GDPR. No process exists about this as far as I know. Which law will take precedence in a conflict situation?

The regulator has changed in the Netherlands, and a more business-friendly environment is to be expected (p.7). In the UK, the government department responsible for sponsoring the ICO is currently seeking to appoint a new Chair to the Information Commission, a governance structure created by the 2025 Data (Use and Access) Act.

In the US, President Donald Trump managed to remove a Federal Trade Commissioner, and this has been approved by the Court of Appeal (p.12) regardless of the obvious threat to the EU-US data transfer arrangement. In Canada, the legislator plans to strip the DPA of oversight of the private sector, and to establish one body to regulate online harms, social media, AI chatbots, as well as private sector privacy (p.1).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

China enforcement... from p.1

whether companies' actual cross-border data flows remain within approved scopes, whether App and SDK practices fully implement privacy requirements, and whether companies have employed effective data security controls to prevent security incidents.

Intensified enforcement of cross-border data transfers

Cross-border data transfers have become one of the most visible enforcement priorities in China. Under the current data export regime, a data exporter may need to adopt one of the prescribed transfer mechanisms depending on the volume and nature of the data to be transferred.[1] These mechanisms include a security assessment administered by the Cyberspace Administration of China (CAC), the filing of a standard contract (SCC) with the local CAC, or certification by an approved third-party institution.

Regulators have stepped up enforcement against unlawful cross-border transfers. On 13 June 2026, the Shanghai Cyberspace Administration announced administrative penalties against a leading online travel service platform under the Personal Information Protection Law (PIPL) for failing to fully comply with the CAC's approval obtained for the security assessment and unlawfully transferring personal information overseas.[2] The company was fined RMB 10 million (around US $1.47 million) and ordered to make rectifications.

The key enforcement message is that obtaining CAC approval is not the end of the compliance exercise. Companies must ensure that their actual transfers remain within the approved scope. If regulators approve only certain transfer scenarios or data fields, the exporter should not treat the approval as a general license for all related data transfers.

This point is illustrated by two other enforcement cases announced by the Shanghai Cyberspace Administration earlier this year.[3] In one case, a hotel management company had applied for a security assessment for data transfers arising from online reservations. The CAC approved the overall transfer but rejected certain data fields due to lack of necessity. The company nevertheless transferred the rejected fields, and was later ordered to make rectifications and fined. In the other case, a property management company exported user accommodation information and financial account information without adopting any required transfer mechanism. The Shanghai Cyberspace Administration ordered rectification and issued a warning, but did not impose a fine.

The contrast between these cases indicates that failure to adopt any transfer mechanism may trigger enforcement, but a deliberate or continued transfer of data fields that have been expressly rejected by the regulator may be viewed as more serious. Companies that have completed security assessments or SCC filings should therefore monitor and assess their actual cross-border data flows against the approved scenarios, data categories, recipients and purposes.

Continued scrutiny of apps and SDKs

Data collection and use by apps (including mini programs) and SDKs remain a core enforcement theme, with regulators also identifying priority sectors for closer scrutiny. On 2 April 2026, the CAC, the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security (MPS) jointly launched the 2026 special enforcement actions on personal information protection.[4] One of the main targets is the unlawful collection and use of personal information by apps and SDKs.

In China, App privacy compliance requirements are set out across a range of legal authorities, including the PIPL, the Cybersecurity Law, sectoral rules for telecommunications and consumer protection, national standards and regulator-issued guidance. Multiple regulators may be involved in supervision and enforcement. Central and local branches of the CAC, MIIT and MPS may also engage third-party institutions to conduct technical testing and publish lists of non-compliant apps and SDKs.

The 2026 special enforcement actions focus on recurring compliance issues involving apps and SDKs. These include:

1. failure to publish privacy policies, enable account deletion or provide effective complaint channels;
2. incomplete or inaccurate notice of the purposes, methods and scope of personal information collection and use;
3. collection without consent, or forced consent to unnecessary data collection; and
4. excessive collection of personal information or excessive calling for device permissions beyond the necessary frequency.

In addition, the 2026 special enforcement actions also identify key sectors for enforcement, including internet advertising, education, transport, healthcare and finance. In practice, regulatory announcements in 2026 have already covered apps in several of these sectors. For example, on 27 April 2026, the CAC announced a list of 33 non-compliant apps, including many in the education, transport and healthcare sectors.[5] Operators in priority sectors may expect further batches of regulatory announcements during 2026.

Data breach as an enforcement trigger

Data breaches and breach risks continue to give regulators a concrete basis for enforcement. Article 27 of the Data Security Law (DSL) requires data processing entities to establish and improve data security management systems, conduct data security education and training, and adopt technical and other necessary measures to ensure data security. Where a breach or breach risk exposes weak access controls, inadequate vulnerability management or other security deficiencies, regulators may rely on the incident as evidence of a failure to perform statutory data security obligations.

For instance, in April 2026, the Zhejiang Cyberspace Administration announced administrative penalties against a local technology company for violating Article 27 of the DSL.[6] The investigation found that a database operated by the company was suspected of having been compromised. The company's server port had a weak password vulnerability, which was exploited by hackers and resulted in data being stolen overseas. The company was ordered to make rectifications and was given a warning and a fine of RMB 50,000 (around US $7,360).

In another enforcement case announced by the Xi'an Cyberspace Administration in March 2026, a local technology company was penalized for failing to fulfill its data security protection obligations under the DSL as well.[7] The company had not taken necessary measures to ensure the security of its relevant systems. As a result, an unauthorized access vulnerability was exploited by malicious foreign IP addresses, creating a risk of data leakage. The company was ordered to make rectifications, and was given a warning and a fine.

These cases show that regulators continue to use data breaches and breach risks as enforcement triggers. Basic security failures, such as weak passwords, exposed ports and insufficient access controls, may be treated as failures to implement statutory data security protection obligations.

Key takeaways

The 2026 enforcement developments point to a practical compliance agenda centered on operational accountability. First, companies should revisit their cross-border data transfer approvals and confirm that live data flows remain within the approved scope. Second, app and SDK compliance should be treated as an ongoing product governance exercise. Third, data security protection should be supported by both governance policies and appropriate technical controls. Companies should be prepared to demonstrate that these controls were implemented in practice, not merely documented on paper.

AUTHOR

Yan Luo is a Partner at Covington's California office in the US.
The author wishes to express her gratitude to Mingxin Liu for his contributions to the article.
Email: yluo@cov.com

REFERENCES

1 Article 38, Personal Information Protection Law; Provisions on Facilitating and Regulating Cross-Border Data Flows.
2 See: mp.weixin.qq.com/s/f1-b4qGK7sDNO7YErl8Low
3 See: mp.weixin.qq.com/s/W_EDyn0NIltRWO72L7dVyA
4 See: www.cac.gov.cn/2026-04/02/c_1776867645836849.htm
5 See: www.cac.gov.cn/2026-04/27/c_1779028107561553.htm
6 See: www.zjwx.gov.cn/col/col1694583/art/2026/art_525f2e44cd849977d51bb824eff8e304.html
7 See: www.shaanxijubao.cn/20260313/2b1b1117f90eb7800b93cf77dee3de75.html

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> *PL&B International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner.
>
> **Mark Keddie, Chief Privacy Officer, SITA, Switzerland**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data (Use and Access) Act 2025, the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.