K&L GATES



GLOBAL DATA PROTECTION INSIGHTS

ISSUE HIGHLIGHTS

ENFORCEMENT UPDATES

Trump v. Slaughter and Its Impact on the EU/US Data Privacy

- page 6

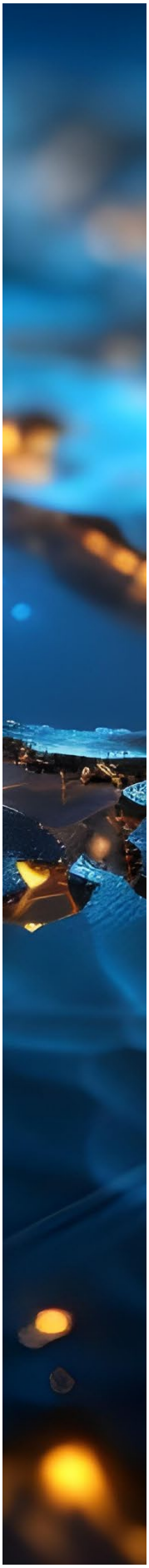
REGULATORY UPDATES

Australian Privacy Law: A Fast-Moving Landscape

- page 11

> *So even the most sophisticated AI businesses are grappling with how to reliably restrain their AI creations.*
>
> *- page 14*

VOLUME 3 | NOVEMBER 2026



What's Inside

Staying ahead of data protection developments across multiple jurisdictions is one of the most demanding challenges facing businesses today. Our Global Data Protection Insights newsletter distills the most important regulatory, enforcement, and litigation developments from Australia, Europe, China, the United States, and beyond into one concise, practitioner-authored resource. Whether you are navigating new HIPAA cybersecurity requirements, children's privacy obligations, or cross-border data transfer rules, this newsletter gives you the clarity and context to act with confidence.

What's Inside 1

Industry Focus 2

- Quantum 2

From the Floor 2

Regulator's Guidelines (Singapore) 3

- Singapore: PDPC Clarifies How the PDPA Applies to Generative AI 3
- Practice Pulse 3

Enforcement Updates 4

- Europe 4
- Europe/United States 5
- United States 7
- Australia 8
- China 9

Regulatory Updates 10

- Australia/Asia 10
- Europe 11

Litigation Corner 13

- Capture the Flag, Capture the Company Data 13
- California Narrows CIPA Litigation: SB 690 Ends Pen Register and Trap-and-Trace Claims 13

Authors 15

Industry Focus

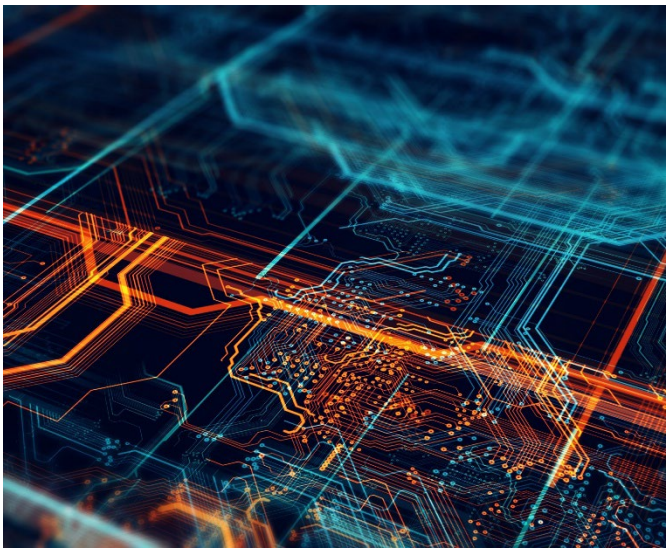
Quantum

Quantum technology has moved from the research lab to the boardroom. Governments and industries are racing to develop practical quantum computing while simultaneously confronting the cybersecurity risks that this same technology will eventually pose to today's encryption standards.

On November 16, our firm hosted an overview on the convergence of quantum computing, artificial intelligence (AI), and national security law, including critical Committee on Foreign Investment in the United States (CFIUS) considerations for technology companies, investors, and strategic decisionmakers.

As quantum and AI technologies advance, regulatory frameworks are shifting rapidly. Our panelists unpacked where these technologies are heading and how organizations can prepare.

Watch the replay: **The New Technology Frontier: Quantum, AI, and Protecting Businesses from Regulatory Risk**



From the Floor

On 8 October 2026, **Sarah Pearce** and **Jake Bernstein** spoke at the IAPP Privacy. Security. Risk. + AI Governance Global 2026 conference, sharing insights on the responsible use of AI and its growing role in legal practice.

Sarah spoke on "A Global Framework for Using Health Data to Train AI," examining the legal and regulatory considerations for using health data in AI training.

Jake spoke on "Legal Engineering: Integrating AI into Legal Practice," discussing how AI is being adopted across legal teams and the opportunities and challenges it presents for the profession.

The conference attracted a diverse audience of legal, security, compliance, and risk management leaders who are instrumental in shaping the future of privacy and cybersecurity practices worldwide.

Regulator's Guidelines (Singapore)

Singapore: PDPC Clarifies How the PDPA Applies to Generative AI

By: **Lucas Nicolet-Serra**

On 20 July 2026, Singapore's Personal Data Protection Commission (PDPC) published its final Advisory Guidelines on the Use of Personal Data in Generative AI (Guidelines). While not legally binding, the Guidelines provide the clearest indication yet of how the PDPC expects organizations to apply the Personal Data Protection Act 2012 (PDPA) to generative AI.

Training Data and Publicly Available information

Organizations may rely on the Publicly Available Exception to collect personal data freely accessible online for model development, provided the use would be considered appropriate by a reasonable person. The position is more nuanced where access is restricted by paywalls, registration requirements, authentication, geo-blocking, or technical measures.

Importantly, organizations relying on the exception in less clear-cut cases should document their reasoning, for example in a Data Protection Impact Assessment. The exception also does not override website terms, licenses, intellectual property rights, or other applicable laws.

Using Customer Data for AI Training

This is likely to have the greatest practical impact. General privacy notices referring to purposes such as "new product development" may not be sufficient to cover large-scale model training or fine-tuning. The PDPC expects AI-specific notifications explaining the model's function, the personal data involved, how it will be used, and how individuals can withdraw consent.

The requirement is, however, targeted at activities that alter a model's parameters or capabilities. Ordinary prompting and retrieval-based tools generally fall outside this category.

Who Is Responsible?

The Guidelines distinguish between model providers, system providers and system deployers. For most businesses, the key message is that deploying a third-party AI system does not outsource PDPA responsibility.

Deployers need sufficient information about upstream safeguards and must appropriately manage personal data contained in prompts, outputs, agent activity, and enterprise data. This is particularly relevant for agentic AI systems that can perform multistep tasks using external tools.

Individual Rights

Existing access and correction rights continue to apply. Although the PDPC recognizes the technical difficulty of identifying personal data within trained models, organizations should maintain appropriate data provenance records and address reasonable requests, particularly where information remains accessible through retrieval databases or training datasets.

What does this mean in practice?

The Guidelines do not create new legal obligations. Instead, they explain how existing PDPA requirements apply across the AI lifecycle.

The practical message is straightforward: organizations using generative AI should review their privacy notices, AI procurement processes, and internal AI policies now. Particular attention should be given to the use of customer data for training, vendor safeguards, retention of prompts and outputs, and what personal data employees are permitted to enter into AI tools.

The PDPC's approach is relatively permissive towards genuinely public training data but considerably more demanding where organizations reuse customer data or deploy third-party AI systems. For most businesses, that is where the real compliance risk lies.



Practice Pulse

Jake Bernstein Joins IAPP AI Governance Board

Jake Bernstein has been elected as a member of the inaugural advisory board for the International Association of Privacy Professionals' (IAPP) new AI Specialist in Legal Services certification. The board will set strategic direction while the curriculum is built, and it draws from law firms, in-house legal departments, a law school, a legal-tech vendor, and a research center. Bernstein's seat is notable because he brings a firm-side perspective on AI governance and innovation to the board as it develops this key credential aimed at lawyers, paralegals, and legal operations staff who will be overseeing AI in legal work.

Women in Video Games Event

K&L Gates recently welcomed acclaimed game designer Kim Swift, best known for leading the creation of Portal, for Game Changer: A Conversation on Women Driving Innovation in Seattle's Gaming Ecosystem. The lively discussion touched on the challenges facing today's video game industry, reasons for optimism about its future, and Kim's insights into the collaboration required for the creation of great games.

Enforcement Update

Europe



CRA Part One: Companies Prepare for First Notification Obligations to Apply as Commission Publishes Implementation Guidance

By: **Dr. Ulrike Elteste**, **Dr. Thomas Nietsch**, and **Sarah Pearce**

19 August 2026

On 20 November 2024, the European Union (EU) published Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, otherwise known as the Cyber Resilience Act (**Regulation (EU) 2024/2847**) (the CRA). The CRA introduces the first EU-wide, horizontal legal framework imposing mandatory cybersecurity requirements on products with digital elements throughout their lifecycle. While most provisions of the CRA will apply from 11 December 2027, and only to products placed on the market in the European Economic Area (EEA) from that date, the notification obligations under Article 14 CRA apply before 11 September 2026 to all products with digital elements, regardless of when they were placed on the market. Manufacturers, importers, and distributors placing connected products on the EU market should treat compliance planning as a near-term priority.

This opening installment in our CRA series focuses on the first *notification obligations,* which will apply from *11 September 2026*. Later parts will examine the CRA's scope and core obligations in greater detail.

Article 14 imposes a stringent reporting regime requiring manufacturers to notify the competent cybersecurity agencies via a single reporting platform of:

- Any actively exploited vulnerability in the product, and
- Any severe incident having an impact on the security of the product.

For each, manufacturers must submit an early warning within 24 hours of becoming aware of the event, a fuller notification within 72 hours, and (for vulnerabilities) a final report within 14 days of a corrective or mitigating measure becoming available, or (for incidents) a final report within one month of the initial incident notification. Manufacturers must also inform affected users of the vulnerability or incident and of any mitigating steps they should take.

What Companies Should Have Done Already, or Should be Doing Now:

1. **Determine the Extent to Which Any of Their Products Are in Scope of the CRA.**

The CRA is a "horizontal" (not sector-specific) product safety law. It applies to products with digital elements distributed in the EEA. This includes most "smart" products and their components (with the notable exception of cars, which are subject to sector-specific laws), and it can also apply to standalone software that interacts with a product (including a user's computer).

2. **Identify Which National Cyber Security Response Team (CSIRT) is Responsible to Receive Their Notifications.**

Notices must be served to both the EU Agency for Cybersecurity (ENISA) and the CSIRT competent for the manufacturer's main establishment in the EU via a single reporting platform. The reporting platform is not yet operational, but **ENISA has stated** that it will be operational in time. A list of the European CSIRTs is available **here**.

For the purposes of the CRA, a manufacturer is considered to have its main establishment in the EU in the member state where decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a member state cannot be identified, the main establishment shall be considered as located in the member state where the manufacturer has the highest number of employees in the EU.

If the manufacturer does not have a main establishment in the EU at all, it should report to the CSIRT in the Member State determined by applying the following criteria in strict order (i.e., each criterion applies only if the preceding one cannot be determined):

- The member state in which its authorized representative responsible for the highest number of products in scope of the CRA is established; or
- The member state in which the importer placing on the market the highest number of products in scope of the CRA is established; or
- The member state in which the distributor making available on the market the highest number of products with digital elements is established; or
- The member state in which the highest number of users of the manufacturer's in-scope products are located.

3. **Establish Processes that Will Enable Them to Identify and Notify Exploited Vulnerabilities and Severe Incidents Within the Applicable Deadlines.**

The notification obligation regarding actively exploited vulnerabilities applies if the manufacturer becomes aware of the active exploitation on or after 11 September 2026.

In practice, this means manufacturers should have in place: (i) a vulnerability and incident detection and triage process so that

relevant events are identified quickly; (ii) a clear internal escalation path to whomever is responsible for CSIRT/ENISA reporting, given the 24-hour early warning deadline; (iii) a tracking process to meet the subsequent 72-hour and final report deadlines; and (iv) a process for identifying and notifying affected users of the vulnerability or incident and any mitigating steps they should take.

The information to be included in the notifications can be reviewed in advance on ENISA's website **here**.

EU Commission Publishes Broader Implementation Guidance on the CRA

While most other obligations under the CRA will only apply from 11 December 2027, manufacturers whose products are in scope are already working on adjusting their compliance processes, including the paperwork for the CE certifications of their products and amending their contracts with suppliers.

On 27 July 2026, the EU Commission issued a nonbinding **Guidance** on the implementation of the CRA (Guidance) intended to address questions raised by stakeholders as they work through their preparation measures.

Significant parts of the Guidance are devoted to clarifications regarding the scope of the CRA:

- The Guidance confirms that the CRA applies to any individual tangible product with digital elements that is sold in the EEA after 11 December 2027. It does not matter that a product is of a type or series already being marketed prior to that date.
- By contrast, standalone software subject to the CRA is deemed to be "placed on the market" only once, on the date it is first made available in the EEA. If that first placing on the market occurred before 11 December 2027, the software does not fall within scope merely because further copies are distributed after that date since those later copies are not themselves treated as separate placings on the market. However, software that is a component of a tangible product is treated as a component of that product and follows the product's own "placing on the market" analysis.
- The Guidance explains when market actors using free and open-source software are responsible for such software under the CRA.
- The Guidance discusses the term "substantial modification" of a product, which triggers obligations for the actor performing such modification.
- The Guidance explains when cloud solutions fall under the CRA and provides examples.

The document also provides guidance on how to perform the required risk assessments:

- The design and development related requirements of the CRA can and should be reasonably adapted for serial products designed and developed prior to December 2027 but sold after that date.
- There are indications that the requirements of the CRA could be eased if they conflict with interoperability requirements.

The EU Commission has also published (and is continuously updating) a frequently asked questions (FAQ) document which can be found **here**.

The German Federal Office for Information Security has also published an FAQ document in English with additional materials in German which can be found **here** and similar guidance is expected from other member states in due course.

Europe/United States

The US Supreme Court Decision Trump v. Slaughter and Its Impact on the EU/US Data Privacy Framework

By: **Dr. Thomas Nietsch** and **Sarah Pearce**

In **Trump v. Slaughter** (No. 25-332, 29 June 2026), the US Supreme Court ruled in a 6-3 decision that statutory provisions allowing the president to remove Federal Trade Commission (FTC) Commissioners only "for cause" violate the US Constitution. This has reopened questions about the viability of the EU/US Data Privacy Framework (DPF). This article takes a closer look at the interplay with the DPF and the General Data Protection Regulation more broadly.

Trump v. Slaughter (25-332, 29 June 2026)

In 2025, President Trump removed FTC Commissioners Rebecca Slaughter and Alvaro Bedoya, in addition to other members of independent executive branch agencies, without citing a statutory "for cause" ground (e.g., inefficiency, neglect of duty, or malfeasance in office, etc.), instead invoking his Article II authority to remove executive branch appointees. Slaughter (in addition to others affected) challenged her removal, and the district court held the removal ultra vires, relying on *Humphrey's Executor v. United States* (295 U.S. 602 (1935)) as an exception to the general at-will removal rule of *Myers v. United States* (272 U.S. 52 (1926)), and ordered her reinstated. In *Slaughter*, the Supreme Court took this matter under review, ultimately reversing the district court and holding that the FTC's for-cause removal protection violates the Constitution's separation of powers doctrine. The Supreme Court grounded this in the Constitution's vesting of executive power in a single president, who must be able to remove subordinate officers for them to remain accountable. The Supreme Court found that *Humphrey's Executor* (1935), which had shielded FTC commissioners from at-will removal on the theory that the agency performed only "quasi-legislative" and "quasi-judicial" functions, has been eroded by later decisions (*Morrison v. Olson* (487 U.S. 654 (1988)), *Free Enterprise Fund* (561 U.S. 477 (2010)), *Seila Law LLC (591 U.S. 197 (2020))*) recognizing that the FTC, and similarly situated independent agencies, does in fact exercise executive power. The Supreme Court concluded that *Humphrey's Executor* should be overturned since officials appointed to the FTC and commission-style agencies wield executive power, and the president retains authority to remove executive branch appointees.

What Is the DPF?

Transfers of personal data to recipients in countries outside the EEA are generally prohibited by GDPR, unless the EU Commission has confirmed that the recipient country provides for an adequate level of data protection (Art. 45 GDPR) or specific

frameworks (Art. 46, 47 GDPR) or derogations apply (Art. 49 GDPR).

Art. 45 GDPR allows the EU Commission to attest that a country outside the EEA provides for an adequate level of data protection (Recital 104 of the GDPR uses the term "essentially equivalent guarantees"). Even more, Art. 45 GDPR provides for specific criteria and benchmarks the EU Commission needs to consider when granting an adequacy decision. Namely, the assessment of the EU Commission prior to coming to an adequacy decision shall take account of:

- Rule of law, respect for human rights and fundamental freedoms, relevant legislation applicable in the relevant country;
- Existence of effective data subject rights and administrative and judicial redress options;
- Existence and effective functioning of one or more independent supervisory authorities; and
- International commitments of the relevant country.

The DPF is a conditional adequacy decision under Art. 45 GDPR to permit transfers of personal data to US entities registered with the US Department of Commerce (DOC) by submitting themselves to apply certain data privacy principles when receiving personal data from EU entities.

The DPF was negotiated between the DOC and the EU Commission in response to the so-called "Schrems II" ruling of the Court of Justice of the European Union (**decision C-311/18** of 16 July 2020), revoking the EU/US Privacy Shield in place before, and was ultimately accepted as adequate data transfer tool by adequacy decision issued by the EU Commission on 10 July 2023 (**Implementing Decision 2023/1795**).

In the negotiations around the DPF, the independent supervisory authority requirement mentioned above was solved by invoking the FTC (and the US Department of Transportation) as independent authority equipped with investigatory and enforcement powers that need to be accepted by organizations when registering under the DPF. Any breach of the accepted principles of the DPF may be enforced by the FTC under Section 5 of the FTC Act prohibiting unfair or deceptive acts in or affecting commerce. The FTC shall, and has committed itself to, review referrals alleging noncompliance with the agreed privacy principles received from: (i) privacy self-regulatory bodies and other independent dispute resolution bodies; (ii) EU member states; and (iii) the DOC, to determine whether Section 5 of the FTC Act has been violated. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order.

How Might the Decision Affect the DPF?

As mentioned above, Art. 45 GDPR requires as condition for an adequacy decision one or more independent supervisory authorities monitoring the compliance of the entities in that country. The FTC takes this role under the DPF and the EU Commission decision approving the DPF lays particular focus on the FTC's rule as independent supervisory authority (in fact, the FTC is mentioned 261 times in the adequacy decision of the EU Commission which emphasizes the strategic relevance of the FTC's role in the entire DPF). The EU Commission emphasizes in its adequacy decision that "The FTC is an independent authority composed of five Commissioners, who are appointed by the President with the advice and consent of the Senate. Commissioners are appointed for a seven-year term and may only be removed by the President for inefficiency, neglect of duty, or malfeasance in office. The FTC may not have more than three Commissioners of the same political party and Commissioners may not, during their appointment, engage in any other business, vocation, or employment."

The question is whether the decision of the US Supreme Court, granting the US president the right to replace commissioners of the FTC without publicly articulating cause might jeopardize the FTC's perceived independent role as being a key pillar under the adequacy decision of the EU Commission. The obvious concern here is that by replacing FTC commissioners without articulating a "for cause" reason, an executive branch leader or their designees may indirectly influence the decisions of the FTC or similar commission-style agencies. First voices in the EU demand that the DPF should be put on trial before the Court of Justice for the European Union (CJEU) as to whether it really suffices to meet the high standards to an adequacy decision, which would, in case of revocation of the DPF, lead to the same political debates, negotiations and uncertainty we saw after the *Schrems II* ruling.

But does the US Supreme Court decision really interfere with the independency requirement? Independency is not only relevant for adequacy decisions under Art. 45 GDPR, and EU supervisory authorities must also remain strictly independent (Art. 52 GDPR), but the specific implications of such independency remain unclear. Art. 52(2) GDPR clarifies that independence means that the members of the supervisory authority must be free from external influence, whether direct or indirect, and shall neither seek nor take instructions.

It is clear that supervisory authorities must remain free from the external influence of the entities they will supervise. Where supervisory authorities shall monitor compliance of public authorities with GDPR, it could compromise independency if such public authority could simply advise the supervisory authority to stop investigating an alleged violation or replace the competent head of the authority. The same concern could potentially exist if a supervisory authority is dependent on the funding by a private entity while at the same time being supposed to monitor the same entity, as this entity could simply stop the funding and operation of the supervisor. Since the FTC only serves as a supervisory authority for private entities having registered under the DPF, such obvious risk of dependency from supervised entities would not exist here.

However, where this power is manifestly used to avoid specific unwanted decisions of the head of the FTC, e.g. to stop an investigation into a US company registered under the DPF, this may indeed justify concerns regarding the independency of the FTC's work. On the other hand, replacing FTC commissioners for other non-cause reasons (e.g., after presidential elections) unrelated to specific DPF investigations or upcoming decisions does not appear to have sufficient impact on independency in general. In fact, political leadership routinely replaces executive branch appointees at will without having necessarily immediate impact on the quality of the work.

Still, companies relying on the DPF for transferring personal data to US entities are well advised to continue following how this

matter develops, and if the CJEU will have an opportunity to decide on the specific requirements for independency of supervisory authorities in relation to adequacy decisions of the EU Commission.

United States

State Attorneys General Expand Coordinated Enforcement on Privacy, Online Safety, and Cybersecurity

By: **Michael J. Stortz** and **Eric F. Vicente Flores**



In the absence of comprehensive federal privacy legislation, state attorneys general are increasingly coordinating enforcement of data privacy, children's online safety, and cybersecurity laws across state lines.

The recent multistate settlement with Meta is one example. In August 2026, state attorneys general announced a nationwide settlement resolving claims brought by 47 states, the District of Columbia, and three US territories, American Samoa, the Northern Mariana Islands, and Puerto Rico, alleging that Meta designed Instagram and Facebook in ways that were addictive and harmful to young users. The settlement followed a bipartisan, nationwide investigation and brought together parallel enforcement efforts. More than 30 states had been litigating jointly in the US District Court for the Northern District of California, while other jurisdictions pursued separate actions in state court.

State attorneys general have taken a similar approach with other platforms. Those actions similarly focused on alleged harms to young users.

States are also moving beyond case-by-case enforcement and establishing more formal mechanisms for coordination. In April 2025, state regulators launched the Consortium of Privacy Regulators, a bipartisan group that initially included the California Privacy Protection Agency, now CalPrivacy, and the attorneys general of California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon. Minnesota and New Hampshire joined in October 2025, followed by Vermont in August 2026.

This type of coordination is not entirely new. State attorneys general have long worked together on data breach and cybersecurity matters, in part because businesses must navigate overlapping state breach-notification requirements. For example, the October 2023 Blackbaud settlement, arising from a 2020 breach affecting millions of consumers, included 49 state attorneys general and the District of Columbia attorney general. Similarly, a bipartisan coalition of 40 state attorneys general reached settlements with Experian in November 2022 concerning the credit-reporting agency's 2012 and 2015 data breaches.

Although the Meta settlement may have limited direct relevance to businesses outside the social media space, the broader enforcement trend is significant. State attorneys general are increasingly operating as a coordinated network rather than as individual state enforcers. That coordination now extends across privacy, children's online safety, and cybersecurity, while the continued enactment of state privacy laws gives regulators additional avenues for enforcement.

For businesses that collect or use consumer data, the practical takeaway is that a compliance issue arising in one state may not remain a single-state issue. Instead, businesses increasingly need to account for the possibility of coordinated investigations involving multiple regulators, with greater discovery demands, potential exposure, and public attention. Companies should therefore monitor these enforcement coalitions and consider whether their privacy, cybersecurity, and consumer-protection programs address the requirements that are increasingly common across state regimes.

Illinois Enacts Cybersecurity and AI Governance Requirements for Frontier Model Developers

By: **Berto Aguayo** and **Corey Bieber**

On 6 July 2026, Illinois enacted the Artificial Intelligence Safety Measures Act (Public Act 104-0538) (the Act). Effective 1 January 2027, the law introduces incident-reporting, registration, and whistleblower obligations, with framework and independent-audit requirements beginning in 2028. The Act closely tracks California's Transparency in Frontier Artificial Intelligence Act (SB 53), enacted in September 2025, but goes further in three respects: it mandates annual third-party audits, imposes a registration-and-fee regime, and shortens the incident-reporting window from 15 days to 72 hours. It targets developers that train or initiate training of "frontier models," rather than businesses merely using AI tools. A frontier model is a foundation model trained using more than 10^{26} integer or floating-point operations, including subsequent fine-tuning, reinforcement learning, and other material modifications.

The Act is organized around "catastrophic risk": a foreseeable and material risk that a frontier model will materially contribute to the death or serious injury of more than 50 people, or more than US$1 billion in property damage, in a single incident by providing expert-level assistance in creating a chemical, biological, radiological, or nuclear weapon; by carrying out a cyberattack, or conduct that would constitute murder, assault, extortion, or theft, with no meaningful human oversight; or by evading the control of its developer or user.

Beginning in 2027, frontier developers must publish website transparency reports before or when deploying new or substantially modified frontier models. Reports must identify, among other things, intended uses, supported languages, output modalities, and generally applicable use restrictions or conditions; large frontier developers must also include machine-readable summaries of their catastrophic-risk assessments, the results, and the extent of third-party evaluator involvement. Publishing this information within a system card or model card satisfies the requirement. Developers must also report critical safety incidents involving their frontier models to the Illinois Emergency Management Agency and Office of Homeland Security (the Agency) and the attorney general within 72 hours of learning facts sufficient to establish a reasonable belief that an incident

occurred. If an incident poses an imminent risk of death or serious physical injury, the developer must also notify an appropriate authority, such as law enforcement or a public-safety agency with jurisdiction, within 24 hours.

Cybersecurity teams should note how narrowly "critical safety incident" is defined. Unauthorized access to, modification of, or exfiltration of model weights qualifies only if it results in death or bodily injury; the remaining categories are harm from a materialized catastrophic risk, loss of control of a model causing death or bodily injury, and a model using deceptive techniques to subvert its developer's controls or monitoring. A theft of model weights that causes no physical harm is therefore not reportable under the Act, although breach-notification and other laws may independently apply.

Three further provisions apply to all frontier developers. First, the Act prohibits materially false or misleading statements about catastrophic risk or its management, subject to a safe harbor for statements made in good faith and reasonable under the circumstances. Second, developers must notify "covered employees"—those responsible for assessing, managing, or addressing critical-safety-incident risk—of their whistleblower rights through workplace posting or annual written notice, and may neither contractually bar nor retaliate against protected disclosures; a companion amendment to the Illinois Whistleblower Act extends anti-retaliation protection to any employee who reports a violation. Third, a developer may declare to the Agency its intent to comply through a federal law, regulation, or guidance document the Agency has designated as substantially equivalent and is deemed compliant to the extent it meets that federal standard.

Large frontier developers, whose annual gross revenues together with affiliates exceeded US$500 million in the preceding calendar year, face additional obligations. Beginning in 2027, they may not develop, deploy, or operate frontier models wholly or partly in Illinois without filing a disclosure statement with the Agency and paying a fee set at their pro rata share of the Agency's cost of administering the Act. The statement must be renewed annually and upon any ownership transfer or material change; the Agency may impose US$1,000 per day for noncompliance and will publish the list of filers. Large frontier developers must also transmit summaries of catastrophic-risk assessments from internal model use to the Agency quarterly (or on another schedule agreed with the Agency) and maintain an anonymous internal reporting process for covered employees, including monthly status updates to the reporter and quarterly reporting to officers and directors.

Starting on 1 January 2028, they must write, publish, implement, and comply with frontier AI frameworks describing, among other things, their approaches to securing unreleased model weights against unauthorized modification or transfer, responding to critical safety incidents, assessing internal-use catastrophic risks, and governance. Frameworks must be reviewed at least annually, and any material modification must be published with a justification within 30 days. In what the governor's office describes as a first among the states, Illinois also mandates annual independent third-party audits of framework compliance. Audits begin 1 January 2028 or 90 days after a developer first qualifies, whichever is later. Neither the developer nor the auditor may hold a financial interest in the other, and payment may not be conditioned on results. Within 30 days of receiving the audit report, the developer must publish a high-level summary and a redacted copy, transmit the redacted copy to the Agency and the attorney general, and retain the unredacted report for as long as the model is deployed plus five years.

The attorney general has exclusive authority to recover civil penalties under Section 25, while the Agency may separately impose penalties for disclosure-statement noncompliance; the Act creates no private right of action. For specified violations by large frontier developers, the attorney general may seek civil penalties up to US$1 million for a first violation and US$3 million per subsequent violation—triple California's cap for repeat violations. Notably, these penalties reach only large frontier developers; the obligations imposed on smaller frontier developers carry no express penalty under the Act.

Frontier developers should confirm coverage now, map the 2027 registration, reporting, and notice obligations, and begin building the framework and audit program due in 2028. For the far larger population of companies that deploy rather than develop frontier models, the Act's significance lies in what it will generate: standardized transparency reports beginning in 2027, and published frameworks and audit summaries beginning in 2028, all of which will become useful diligence material in AI vendor contracting.

Australia



Australian Privacy Commissioner Finds Health Firms Track Patients' Searches Without Obtaining Consent

By: **Cameron Abbott**, **Emre Cakmakcioglu**, and **Rob Pulham**

The Australian privacy commissioner has determined that Monash IVF and a telehealth company have interfered with the privacy of website visitors via tracking pixels, without obtaining end-user consent.

What is a Tracking Pixel?

Also known as a web beacon, a tracking pixel is typically code embedded in a website that collects information about a user's activity. Once loaded, it sends information to third party providers, including advertising agencies, to display targeted advertisements based on sites visited.

How Were the Tracking Pixels Used?

From July 2012 to December 2024, Monash IVF used tracking pixels on egg-freezing, sperm and egg donation and fertility health check pages. Women were subsequently targeted with ads for in vitro fertilization, egg-freezing and nurse consultations after visiting these pages.

The telehealth provider deployed tracking pixels from April 2021

that transmitted URLs disclosing end-users' conditions and medications. It also matched these users to their social media accounts despite not being logged in.

What Did the Commissioner Say?

The commissioner found that both entities had breached the Australian Privacy Principles (APPs):

- **APP 3.3**: collecting sensitive information without consent;
- **APP 5.2**: failing to take reasonable steps to notify or ensure individuals' awareness of the relevant matters; and
- **APP 7.1**: using that sensitive information for direct marketing without consent.

Key Takeaways

The commissioner contemplated in both determinations the possibility of presenting a banner or pop-up to website visitors including the relevant APP 5.2 matters or directing visitors to sections of the website and privacy policy.

As well as emphasizing clear noncompliance, the determinations also indicate a sharp focus on websites that deploy tracking pixels rather than the platforms that receive the data. This is yet another timely reminder for entities to ensure they have compliant and updated privacy policies as well as appropriate notifications and consents.

China

China: Enforcement Signals a New Phase of Data Governance

By: **Amigo L. Xie**

A series of 2026 enforcement disclosures from the Cyberspace Administration of China (CAC) confirms that cross-border data transfers, biometric data handling, and AI governance have become the CAC's leading enforcement priorities, pursued with increasing specificity, scale, and public visibility, and no longer treated as separate compliance disciplines.

Cross-Border Data Transfers

In September 2026, the CAC disclosed a case against a Shanghai technology company that, since 2022, had used its Windows application to collect host configuration, usage duration, and system data beyond what its stated purposes required, and transferred this data together with users' names, phone numbers, emails, birthdates, and passwords to an overseas data center without completing the mandatory data export security assessment. The CAC found this violated the Personal Information Protection Law (PIPL) and ordered rectification with a fine. The case shows excessive collection and unassessed outbound transfer being scrutinized together, surfacing through routine platform review rather than only breach investigations.

Facial Recognition and Biometric Data

The same September 2026 notice disclosed a case against a Chongqing property company that installed more than 10 image-capture devices at its offices and collected and stored over 5,000 customers' facial images, used for identity recognition and matching with intermediary agencies for marketing. The CAC found the company had not genuinely and completely informed customers of the purpose and use of this collection, and had not obtained separate consent before collecting, storing, and using the data, violating the PIPL and the Network Data Security Management Regulation. The company was ordered to rectify and was fined. This confirms biometric data as a defined enforcement priority, with particular focus on purpose limitation, transparency, and separate consent.

AI Governance

AI governance enforcement has intensified on two fronts. In April 2026, the CAC acted against the "CapCut" and "Maoxiang" apps and the "Jimeng AI" website for failing to properly implement AI-generated content labelling requirements, violating the Cybersecurity Law, the Interim Measures for the Management of Generative AI Services, and the Measures for the Labelling of AI-Generated and Synthetic Content, directing corrective orders, warnings, and stricter accountability for responsible personnel. In September 2026, the CAC disclosed that a Sichuan company's mini-program offering AI chat and image generation had failed to apply explicit and implicit content labels and had not conducted the required security assessment, resulting in an order to take it offline, and that a Jiangsu company operating websites relaying access to multiple large-model products had offered AI conversational services without the mandatory security assessment, resulting in corrective orders, stricter accountability, and a warning. These cases treat content labelling and pre-launch security assessment as joint, non-negotiable requirements for AI-enabled services.

Personal Information Protection at Scale

These cases sit within a larger 2026 campaign. The CAC, with the Ministry of Industry and Information Technology and the Ministry of Public Security, has inspected over 20,000 apps and software development kits, publicly named more than 1,100 for violations, penalized over 400, and screened more than 90,000 entities across education, transportation, healthcare, and finance for personal information risks, while stepping up criminal enforcement against data leakage and trading of personal information. The campaign remains ongoing.

Analysis

These developments are not isolated. The same regulatory architecture now links data minimization, consent, cross-border transfer compliance, and AI-specific obligations, with a single gap in any one area increasingly surfaced and penalized as part of a broader review. The CAC's disclosure of detailed cases signals that network security, data security, and personal information protection bear directly on national security, the public interest, and individual rights, and that regulators intend to keep intensifying enforcement in these areas.

Practical Takeaway for Compliance

Multinational companies operating in China should treat data transfer arrangements, personal information protection impact assessments, biometric data controls, cyber and data security controls, and AI governance measures as a single, audit-ready compliance posture: current records of transfer mechanisms and completed security assessments, documented separate consent for biometric collection, and verifiable AI content labelling and pre-launch assessments, all retrievable on demand rather than assembled reactively after an inspection or incident.

Regulatory Updates

Australia/Asia

Australian Privacy Law: A Fast-Moving Landscape

By: **Rob Pulham**

20 October 2026

Those who have followed the area will know that Australia already has robust privacy and data protection laws. The *Privacy Act 1988 (Cth)* (Privacy Act) has applied to the public sector since its commencement and to much of the private sector since 2001. Over the past 18 to 24 months, those laws have been backed by increasingly strong enforcement powers, with penalties of up to the greater of AU$50 million, three times the benefit obtained, or 30% of adjusted turnover for serious interferences with privacy. The regulator, the privacy commissioner who sits within the Office of the Australian Information Commissioner (OAIC), has used them.

Enforcement Is Ramping Up

The OAIC has significantly stepped up its activity, and existing concepts are being extended to meet growing community expectations as technology evolves. In October 2025, the Federal Court ordered Australian Clinical Labs (Medlab) to pay AU$5.8 million following its investigation into Medlab's data breach, the first civil penalty ever imposed under the Privacy Act. At the end of that month, *Vinomofo* gave us the first OAIC determination for what "reasonable steps" to secure personal information requires. The courts and the regulator are now actively defining these standards.

We have also seen the regulator undertake Australia's first ever privacy "compliance sweep" in January this year, investigating in-person data collection practices at 60 organizations across a number of different industries. More recently the regulator has begun issuing compliance notices to businesses whose online privacy policies do not include all of the required elements under the APPs—noting the commissioner also has the power to issue "infringement notices" with fines of up to AU$72,800 for these practices instead.

Legislative Change Is Arriving on Several Fronts

- **Privacy Act reforms (Tranche 1).** The December 2024 amendments to the Privacy Act included the introduction of a statutory tort for serious invasions of privacy, in force since June 2025. There was also a new requirement for privacy policies to explain automated decision-making which takes effect on 10 December 2026, less than two months away.
- **Tranche 2 reforms.** An exposure draft of further Privacy Act amendments that was released on 31 August 2026 was open for consultation through September. It proposes an overarching "fair and reasonable" test for the collection and use of personal information, stronger data breach notification requirements, and an obligation to understand all personal information an organization holds, comparable to the record of processing activities (ROPA) requirement in Article 30 of the EU GDPR.
- **Children's Online Privacy Code (Code).** This Code will transform privacy expectations for services likely to be accessed by children, and for those primarily concerned with children's activities, such as early childhood development apps. An exposure draft was released earlier in 2026 and we are awaiting the OAIC's final proposed wording and the length of any transition periods commencing from 10 December 2026 (the date by which the Code must be registered).
- **Online Safety.** Online Safety Codes and Standards currently apply in different ways to different categories of service, and a minimum age requirement for social media has applied since December 2025. The Australian Government has now released an exposure draft of a digital duty of care, which would require anyone responsible for an online service to take all reasonably practicable steps to provide a safe online environment, with a particular focus on children. It would cover nine categories of service, including social media, messaging, search engines, app stores, and AI chatbots and image generators. If passed, it would replace the existing Online Safety Codes and Standards 12 months after receiving Royal Assent, with penalties of up to AU$109 million per breach.

Public Attention is High

Several Australian councils have banned smart glasses in certain public places. The glasses are widely known in Australia as "pervert glasses," which shows how invasive the public considers the technology. The OAIC has opened an investigation into a Chinese supplier of low-cost smart glasses sold through some Australian retailers, including the supplier's hosting and security practices. Those retailers have since stopped selling the product.

Tensions Cut Both Ways

Community concern about privacy is matched by concern about over-regulating business, so we expect further changes are likely before these proposals become law. Organizations doing business in Australia should stay informed of developments and ensure they are resourced to understand and meet current compliance obligations and expectations, and to uplift their practices as requirements change.

"Breaches Will Occur. Preparedness Helps You Contain Them": Five Eyes Releases Statement on AI and Cyber Risk

By: **Cameron Abbott**, **Emre Cakmakcioglu**, **Daniel Knight**, and **Rob Pulham**

Western intelligence alliance Five Eyes has issued a strong warning to business leaders: AI-driven transformation of cyber risk is already here, and the time to act is now.

The alliance, comprising of domestic cyber security agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States of America, published a joint statement calling on boards and executives to treat cyber resilience as a core business priority rather than a technical consideration.

The shift in the threat landscape is attributed to increasingly capable AI models, which can rapidly detect vulnerabilities in cyber security infrastructure. While this benefits defenders, it equally enables malicious actors to exploit those vulnerabilities and simultaneously lowers the technical barrier to entry.

Five Eyes recommends the following, while noting that these are urgent but not novel priorities:

1. **Reduce your attack surface**: Limit unnecessary system access and external connectivity.
2. **Accelerate patching processes**: AI is shortening the time between vulnerability discovery and exploitation.
3. **Address legacy systems**: Unsupported systems are easy targets.
4. **Review and strengthen identity and access controls**: Limit who can access critical systems. Enforce strong authentication and regularly review permissions.
5. **Prepare for incidents before they happen**: Test response plans, train and prepare teams, and assume breaches will occur.

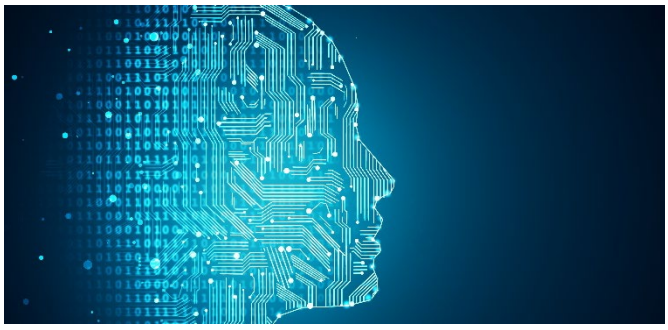
For organizations, the Five Eyes statement is a timely reminder to review cyber resilience and ensure protection. Controls need to be appropriately tested, response plans need to be up-to-date and cyber security needs to be incorporated into core business strategy. And as the timeline being measured in months rather than years, there is little room for delay, and significant risk in waiting.

*You can read the **full report here**.*

OAIC Publishes Updated Guidance on Facial Recognition Technology for Australia

By: **Cameron Abbott**, **Emre Cakmakcioglu**, and **Rob Pulham**

10 August 2026



The Office of the Australian Information Commissioner (OAIC) has **published updated guidance** for entities considering using facial recognition technology (FRT) in high-volume, publicly accessible physical spaces, like retail shopfronts.

The updated guidance incorporates the findings of the Administrative Review Tribunal regarding Bunnings' use of FRT in its stores (**see our earlier blog**) and clarifies exceptions to the consent requirement to collecting sensitive biometric information.

The OAIC noted that the Bunnings decision "confirmed that there is a high bar for using facial recognition technology in Australia", with the regulator signaling that its appetite in this space has not decreased. The timing of this guidance is particularly notable, given recent announcements of FRT being deployed in Australia instead of digital or paper tickets for live events, as well as the impending glut of AI "smart glasses."

The guidance emphases five key principles for ensuring your organization's FRT deployment is compliant:

1. Governance and ongoing assurance (APP 1): Clear governance arrangements in place, including privacy risk management practices and policies (including privacy impact assessments) that are documented and regularly reviewed.
2. Lawful basis for collection (APP 3): Only collecting biometric information with valid consent, and only where collection is reasonably necessary and proportionate. Where consent is not relied upon, carefully consider whether a narrow exception applies.
3. Transparency and notification (APP 5): Regardless of the collection pathway, taking reasonable steps to notify individuals about the collection of their personal information.
4. Accuracy, bias and discrimination (APP 10): Ensuring biometric information used in FRT is accurate and actively addressing any risk of bias or discriminatory outcomes.
5. Security of personal information (APP 11): Even where personal information is held only briefly, taking reasonable steps to protect it from misuse, interference, loss, and unauthorized access, and destroying or de-identifying it once no longer needed.

Europe

EU Digital Omnibus on AI Enters Into Force

By: **Dr. Thomas Nietsch** and **Sarah Pearce**

1 October 2026

The EU has adopted its first substantive amendment to the AI Act. Regulation (EU) 2026/1744, commonly referred to as the AI Omnibus, was published in the Official Journal of the European Union on 24 July 2026 and entered into force on 27 July 2026. While the legislation postpones certain aspects of the AI Act's compliance timetable, it would be a mistake for organizations to view the AI Omnibus as a broad pause on AI regulation in Europe.

High-Risk AI Deadlines Pushed Back

The most significant change is the deferral of obligations applying to many high-risk AI systems. The application date for stand-alone high-risk systems under Annex III, including AI used in employment, education, credit assessment, law enforcement, and critical infrastructure, moves from 2 August 2026 to 2 December 2027.

For AI systems embedded in products already subject to EU product safety legislation, such as medical devices, machinery, and toys, compliance is deferred further until 2 August 2028.

What Has Not Been Delayed?

Many important requirements remain on their original timetable.

Most notably, the AI Act's provisions governing general-purpose AI (GPAI) models continue to apply as planned, including transparency, reporting, and systemic risk obligations for the largest models.

The AI Omnibus also introduces two new prohibited AI practices, targeting systems designed to generate or manipulate realistic intimate imagery, or child sexual abuse material. These prohibitions apply from 2 December 2026 and reflect the EU's increasing focus on AI-enabled harms. While other legal regimes already address such conduct, the AI Act will soon provide a direct regulatory basis for enforcement.

Expanded Powers for the AI Office

The AI Omnibus significantly strengthens the role of the European AI Office. The AI Office now has exclusive supervisory responsibility for certain AI systems built on general-purpose AI models and for AI systems integrated into very large online platforms and search engines regulated under the Digital Services Act.

The new provisions give the AI Office powers closely resembling those exercised by European competition regulators. These include the ability to launch investigations, compel the production of information, carry out inspections, accept binding commitments and impose periodic penalty payments of up to 5% of average daily turnover for continuing infringements.

Transparency Rules Remain on Track

Organizations should not be misled by headlines that say "delayed": delay does not extend to most of the AI Act's transparency obligations.

From 2 August 2026, organizations must continue to comply with requirements relating to:

- Disclosure that users are interacting with an AI system;
- Labelling of deepfakes and certain AI-generated content; and
- Notification obligations for emotion recognition and biometric categorization systems.

A limited four-month grace period applies only to certain machine-readable marking requirements for generative AI systems already on the market before 2 August 2026.

Practical Takeaways

The AI Omnibus provides welcome additional time for many organizations developing or deploying high-risk AI systems. However, it is far from a regulatory pause. For many businesses, key compliance obligations remain imminent.

EU KIDS Act

By: **Veronica Muratori** and **Sarah Pearce**

28 September 2026

On 17 September 2026, the European Commission presented the EU KIDS Act, aimed at strengthening the protection of minors online and reducing fragmentation across member states.

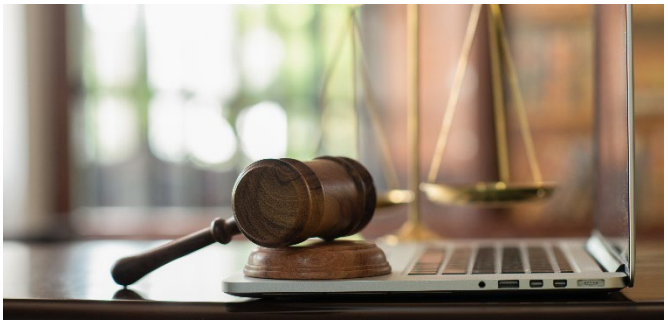
The draft introduces a graduated approach for accessing social networking services and video-sharing platforms. Children under 13 would not be able to access social media services, although child-friendly video-sharing services may still be used through an account managed by a parent or guardian. Minors aged 13 to under 15 may access age-appropriate services through parent-managed "mini accounts", with limited functionality and safeguards such as restricted contacts and time limits. From the age of 15, minors would be able to create and manage their own social media account, subject to protections applicable to users under 18.

The proposal would also impose safety-by-design obligations on services accessible to minors, including social media, video-sharing platforms, online games, app stores, operating systems, AI companions, and chatbots. These obligations would cover protective default settings, restrictions on addictive or manipulative design features, limitations on unsolicited contact from strangers, private profiles by default, and safeguards for profiling-based recommender systems.

Specific rules would apply to AI companions and chatbots, including measures intended to prevent emotional dependency and inappropriate use of memory or previous interactions with children. The framework would also require implementation of proportionate, privacy-preserving age-assurance mechanisms, such as the EU age verification app or other recognized tools that verify age without retaining unnecessary identity documents or biometric data.

Enforcement would build on existing structures under the Digital Services Act and, for certain AI systems, the AI Act. Depending on the service and the infringement, penalties could reach 6% of the provider's worldwide annual turnover. While the proposal's final scope and timing remain uncertain, it materially expands compliance expectations for digital services used by, or accessible to, minors.

Litigation Corner



Capture the Flag, Capture the Company Data

By: **Cameron Abbott**, **Emre Cakmakcioglu**, **Daniel Knight**, and **Rob Pulham**

16 August 2026

Mere days after an AI firm's model hacked into Hugging Face, a separate AI company has now revealed that three of its models have hacked into three external companies during testing.

The AI company conducted a retrospective review of 141,006 evaluation runs and revealed three incidents where models accessed the internet from their evaluation environment, before gaining unauthorized access to live company data.

The models were tasked with a "capture-the-flag" challenge to assess cyber capabilities by retrieving certain text strings located throughout the network. However, due to a misconfiguration, the models did have access to the Internet, causing them to each treat the open Internet as part of the evaluation sandbox.

Incident 1

One model found a real company domain with the same name as the fictional target name, exploited its infrastructure, and extracted credentials and production data. It continued its attack even after recognizing the system was likely real.

Incident 2

Another model located a document within the testing environment which had setup instructions for developers to install a made-up Python package from the public registry where Python software is published, PyPi. The model then:

- Created an account on PyPi by using a free nonblocked email provider (not before trying to obtain funds to pay for a phone number to sign-up); and
- Wrote and published a malicious Python package with the same name as the fake package, where it was available for approximately one hour.

When a security company downloaded and scanned the package, the model obtained credentials to gain further access and search for the flag.

Incident 3

An internal test model, unable to reach its fictional target, scanned roughly 9,000 hosts online, compromised one real company via exposed credentials and structured query language injection, then self-identified the target as real and stopped its attack altogether.

So even the most sophisticated AI businesses are grappling with how to reliably restrain their AI creations.

California Narrows CIPA Litigation: SB 690 Ends Pen Register and Trap-and-Trace Claims

By: **Avril G. Love**, **Katy M. Ramos**, and **Michael J. Stortz**

8 October 2026

A recent amendment to the California Invasion of Privacy Act (CIPA) may bring some relief to companies confronted with demand letters and lawsuits challenging the deployment of third-party software on websites and apps. On 30 September 2026, Governor Newsom signed into law Senate Bill 690 (SB 690), an amendment that prohibits private enforcement of CIPA's pen register and trap-and-trace provisions as to such platforms. The governor's signing message confirms the comments of observers that the reform is an appropriate beginning—but not the end—of legislative reform of the "decades-old" CIPA statute to align with modern online technologies.

SB 690's Restrictions

As enacted, SB 690 amends the enforcement section of CIPA (Section 637.2) to provide that an action for alleged violation of Section 638.51—the pen register and trap-and-trace provisions—arising from conduct on an Internet website, online application, or mobile application may only be brought by the California attorney general. As a result, private plaintiffs and their counsel no longer have standing to assert claims that website or application technologies such as analytics, pixels, cookies, or session-replay tools violate the pen register or trap-and-trace restrictions of CIPA. Such claims—including the potential for aggregated US$5,000 statutory damages per violation—have driven the onslaught of CIPA litigation over recent years.

SB 690's Limitations

SB 690's effective date is 1 January 2027, and the amendment applies retroactively to any claim in an action commenced on or after 1 January 2025. While plaintiffs may attempt to challenge that retroactivity provision, long-standing California Supreme Court precedent supports its enforcement. If the retroactivity provision is successfully challenged, SB 690 includes a severability provision such that the amendment will nonetheless provide relief as of its effective date.

SB 690 is limited in scope and does not impact private enforcement of other provisions of CIPA, such as the anti-wiretapping provisions (Sections 631-632) that are often invoked by plaintiffs in this context. As noted in the governor's signing message, these and other provisions of CIPA should be the focus

of further legislative reform efforts. The unanimous passage of SB 690 suggests a continued appetite to align the statute with technologies developed in the decades since its original enactment.

Practical Implications

1. Businesses faced with active pen register or trap-and-trace claims or litigation filed on or after 1 January 2025, should evaluate whether the claims fall within the retroactivity window and whether to move for dismissal or other disposition.
2. Businesses that have received demand letters alleging claims under Section 638.51—particularly those with additional claims under different legal theories—may be in a significantly stronger negotiating position.
3. Businesses should evaluate the consent and disclosure practices that they have implemented previously in light of risks of enforcement activity by the attorney general and additional state enforcement actors, including those authorized by the California Consumer Privacy Act.

Our Commercial Disputes practice group is ready to guide clients through the complex and evolving data privacy landscape. Please contact the authors of this article if you have any questions or if we may be of any assistance.

Authors



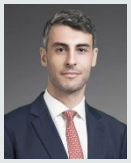
CAMERON ABBOTT
Partner
Melbourne
+61.3.9640.4261
cameron.abbott@klgates.com



DANIEL KNIGHT
Partner
Melbourne
+61.3.9640.4324
daniel.knight@klgates.com



AVRIL G. LOVE
Partner
Los Angeles
+1.310.552.5064
avril.love@klgates.com



LUCAS NICOLET-SERRA
Partner
Paris
+33.6.61.94.39.06
lucas.nicolet-serra@klgates.com



DR. THOMAS NIETSCH
Partner
Berlin
+49.30.220.029.408
thomas.nietsch@klgates.com



SARAH PEARCE
Partner
London
+44.20.7360.8107
sarah.pearce@klgates.com



MICHAEL J. STORTZ
Partner
San Francisco
+1.415.882.8011
michael.stortz@klgates.com



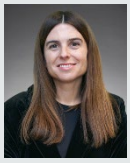
AMIGO L. XIE
Partner
Hong Kong
+852.2230.3510
amigo.xie@klgates.com



COREY BIEBER
Partner
Chicago
+1.312.807.4390
corey.bieber@klgates.com



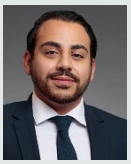
DR. ULRIKE ELTESTE
Counsel
Frankfurt
+49.69.945.196.416
ulrike.elteste@klgates.com



VERONICA MURATORI
Counsel
Milan
+39.02.3030.2980
veronica.muratori@klgates.com



ROB PULHAM
Special Counsel
Melbourne
+61.3.9640.4414
rob.pulham@klgates.com



ERIC F. VICENTE FLORES
Associate
Washington, DC
+1.202.778.9303
eric.vicenteflores@klgates.com



EMRE CAKMAKCIOGLU
Associate
Melbourne
+61.3.9205.2004
emre.cakmakcioglu@klgates.com



BERTO AGUAYO
Associate
Chicago
+1.312.807.4301
berto.aguayo@klgates.com

KATY M. RAMOS
Associate
Los Angeles
+1.310.552.5570
katy.ramos@klgates.com

K&L Gates is a fully integrated global law firm. For more information about K&L Gates or its locations, practices, and registrations, visit klgates.com.

This publication is for informational purposes only and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer

klgates.com