
K&L GATES
GLOBAL DATA PROTECTION INSIGHTS
APRIL 2026

OVERVIEW

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.

CONTENTS

INDUSTRY FOCUS

INDUSTRY FOCUS

US HEALTHCARE AND CYBERSECURITY

By: Sarah L. Carlins, Martin A. Folliard, Clarita I. Sullivan

Important changes to the United States' federal standards governing the cybersecurity of patient health information may be coming soon. In December 2024, the US Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS), the agency that oversees the Health Insurance Portability and Accountability Act (HIPAA), proposed the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information[1] (the Proposed Rule). The Proposed Rule was announced during the Biden administration. Thus far, the Trump administration has not indicated any intent to table or abandon it. Consequently, the Proposed Rule remains on track to be finalized in May 2026, with compliance dates for these new HIPAA security requirements potentially coming in late 2026.[2] If finalized as anticipated, this will be the first time since 2013 that the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) will be materially updated.[3]

Since the Security Rule was first implemented, the cybersecurity landscape has drastically evolved. The healthcare industry, as well as many others, has suffered an influx of cybersecurity threats and attacks. OCR recognizes this reality, explaining that the Proposed Rule "seeks to strengthen cybersecurity by updating the Security Rule's standards to better address ever-increasing cybersecurity threats to the health care sector."[4]

Forecasting Key Changes of the Proposed Rule

Both covered entity and business associate clients would be impacted by this Proposed Rule. If finalized as proposed, we have previewed a few of the key changes below.

First, the Proposed Rule will institute new requirements for business associates. Among other changes, business associates will have to provide annual written verification of certain requisite technical safeguards set forth in the Security Rule for their covered entity customers. Similarly, business associate subcontractors will have to provide this same verification to their business associate customers. Such verification must include an analysis by an individual with cybersecurity expertise and a certification of accuracy by an authorized individual at the business associate or subcontractor, as applicable.[5]

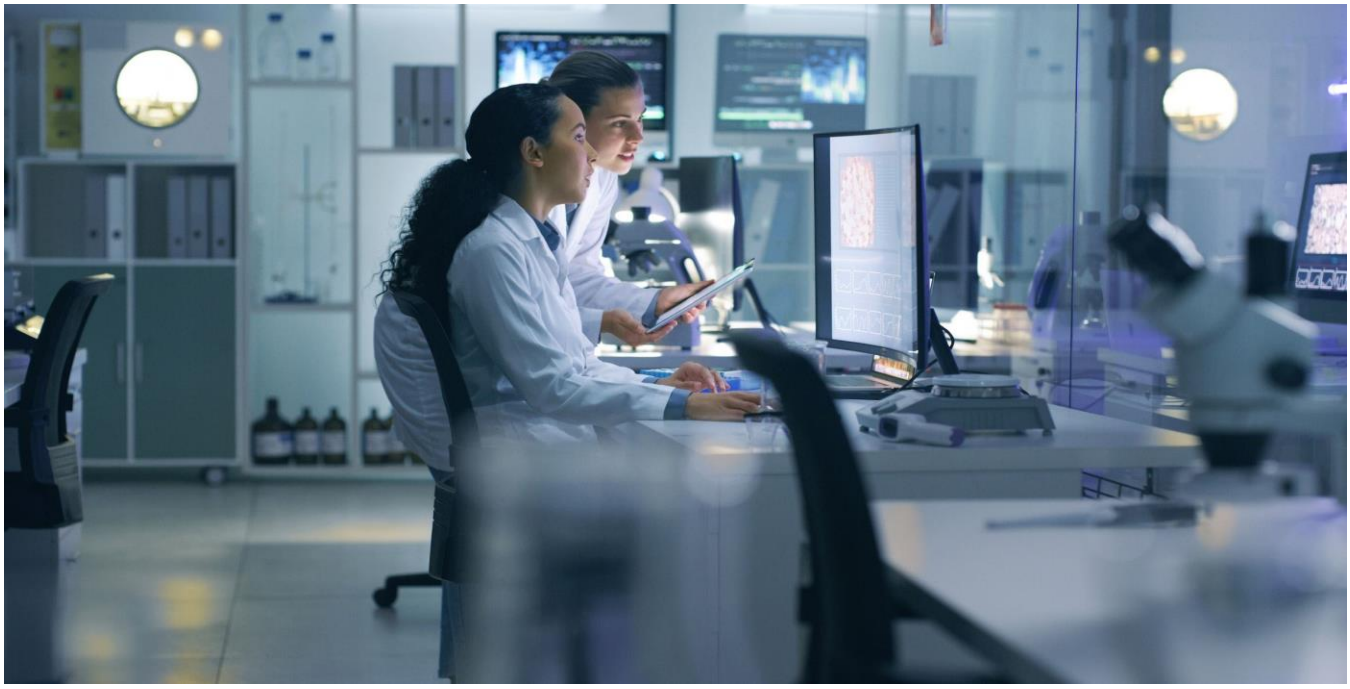
Currently, the Security Rule only requires a business associate to provide written assurances that it will implement "reasonable and appropriate safeguards"[6] to protect electronic protected health information (ePHI), which is a lesser standard. The Proposed Rule introduces these and similar stricter requirements for business associates to better safeguard the ePHI they manage.

Second, the Proposed Rule will implement more stringent technical controls. In particular, all technology that accesses ePHI will be required to use multifactor authentication, and networks will have to be firewalled to better contain cyberattacks and cybersecurity threats, amongst other controls.[7] Presently, multifactor authentication is not specifically required, as general authentication of an individual or entity seeking access to ePHI is acceptable.[8] Moreover, firewalls are not expressly mandatory but rather serve as an example of a technical safeguard.[9] The Proposed Rule's heightened technical safeguards are intended to better ensure security and safety of ePHI where possible.

Third, the Proposed Rule will require a "technology asset inventory and a network map of . . . electronic

information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI[,]" along with certain implementation elements.[10] Both covered entities and business associates will have to document this inventory and network mapping on an annual basis, as well as in response to changes in their environment or operations that may affect ePHI.[11] At present, the Security Rule only requires that covered entities and business associates institute a general security-management process with certain implementation components.[12] The Proposed Rule's requirements for such explicit, mandatory documentation evidence OCR's heightened cybersecurity expectations.

K&L Gates' Healthcare and FDA practice will monitor any developments to the Proposed Rule as potential finalization in May 2026 approaches. K&L Gates regularly advises on HIPAA matters and welcomes any questions our covered entity and business associate clients may have on the Proposed Rule and its implications.



FEATURED ARTICLES

FEATURED ARTICLES

US CHILDREN'S PRIVACY AND AGE ASSURANCE: INSIGHT FROM THE FTC'S WORKSHOP AND STATE LEGISLATION

By: Eric F. Vicente Flores, Whitney E. McCollum

Introduction

On 28 January 2026, the Federal Trade Commission (FTC) convened a full-day public workshop on age-verification technologies, signaling that age assurance is now a front-line enforcement and policy priority. This article synthesizes the key themes from that workshop and examines parallel legislative developments in California that are reshaping children's privacy obligations for businesses operating digital platforms and artificial intelligence (AI)-enabled services.

The FTC Workshop – Regulatory Context and Key Themes

Regulatory Context

The FTC framed the workshop as both fact-gathering and enforcement-signaling, designed to inform a future policy statement and possible amendment to the Children's Online Privacy Protection Act (COPPA) Rule. FTC Chairman Andrew Ferguson made clear that the agency intends to push COPPA "as far as we lawfully can." COPPA currently applies to operators of websites and online services directed at children under 13, or operators with "actual knowledge" that they are collecting personal information from children. It requires those operators to provide notice, obtain verifiable parental consent, and comply with data minimization and deletion requirements. Enacted in 1998, converging forces are driving regulatory urgency to strengthen COPPA enforcement and expanding its reach: (1) children's pervasive online engagement on platforms not designed for minors; (2) the maturation of more sophisticated verification technologies; and (3) a fragmented patchwork of state and global requirements creating significant operational complexity for businesses.[13]

A Critical Distinction: "Age Verification" vs. "Age Assurance"

"Age verification" is the term commonly used when discussing age-gating concepts, but it is only a subset of the broader concept of "age assurance." Age assurance encompasses self-declaration (generally viewed as inadequate in higher-risk contexts), inference and estimation techniques (often AI-based), and higher-assurance verification using government-issued identity documents or authoritative databases. The workshop explored a "waterfall" approach—a layered method that starts with lower-friction, privacy-friendly approaches and escalates as needed, deleting any data collected solely for age assurance at the end of each stage. Age verification technology providers advocated for "age-aware, not identity-aware" design principles and double-blind privacy-enhancing architectures that confirm a user meets a minimum age threshold without disclosing the user's identity or creating records of browsing activity.

Tradeoffs and Unresolved Tensions

The FTC has not identified any single age-assurance method as definitively superior. What's clear is the need to mitigate core privacy concerns with any method, such as the risk of creating high-value databases of identity documents or biometric data and

retention of sensitive information beyond the point of necessity. On the constitutional front, 13 state age-verification laws have been enjoined, 11 are in effect but being challenged across eight circuits, and there have been zero final rulings, with the constitutionality questions outside the obscenity context characterized as open and evolving.

One of the most significant unresolved legal questions is the "circularity problem"[14] embedded in COPPA's structure: COPPA requires parental consent before collecting personal information from a child, but certain age-verification methods necessarily require collecting personal information to determine whether the user is a child in the first place. The FTC acknowledged this tension and stated that it is actively exploring potential solutions, but no resolution was announced at the workshop.

California's Expanding Children's Privacy Framework

While the FTC refines its federal approach, California continues to function as the most active state-level laboratory for children's privacy regulation, with two recent legislative developments of particular significance.

SB 243: Regulating Chatbot Interactions Involving Minors

California SB 243,[15] effective 1 January 2026, addresses AI-powered chatbot technology in contexts where minors may be present. The law requires covered operators to disclose clearly that a user is interacting with an automated system rather than a human. Where a minor is a reasonably foreseeable user, obligations extend to design-level requirements intended to prevent manipulative or harmful conversational patterns and to ensure that chatbot interactions do not exploit minors' developmental vulnerabilities. Businesses deploying customer-facing conversational AI accessible to minors face immediate compliance obligations, including disclosure requirements, design constraints, and potentially integration with age-assurance mechanisms.

Assembly Bill 1043: The Digital Age Assurance Act

California Assembly Bill 1043, the Digital Age Assurance Act,[16] signed into law in 2025 and operative 1 January 2027, establishes age-assurance requirements for covered online services that are "likely to be accessed by minors." The act adopts a risk-calibrated approach rather than mandating a single technical method, incorporates data-minimization expectations, and reflects the anticipatory "likely to be accessed" paradigm that international regulators have advanced as an alternative to COPPA's "actual knowledge" trigger. Its scope is broad enough to capture social-media platforms, gaming environments, video streaming services, and online marketplaces.

Why California Matters Beyond Its Borders

California's regulatory approach to children's privacy rarely stays confined to California; the state's outsized consumer market means that compliance with California law often drives national product and policy decisions. The California Age-Appropriate Design Code Act (CAADCA), enacted in 2022 and subsequently enjoined on First Amendment grounds, illustrates the constitutional complexity of this space and the durable downstream influence such legislation can have on product design decisions. The combination of SB 243 and AB 1043 signals that California is moving toward a comprehensive framework addressing not just what data is collected from minors, but how services are designed and what technical mechanisms must be in place before a minor engages with a covered service—a shift from privacy as data governance to privacy as product design.

A Compliance Posture for an Evolving Landscape

The FTC's January 2026 workshop and California's parallel legislative developments together signal that age assurance is transitioning from a best practice to a regulatory expectation. For businesses attempting to future-proof compliance, we suggest several near-term actions:

- *Conduct an age-assurance audit* to assess current mechanisms, identify gaps relative to emerging federal and state expectations, and evaluate privacy-preserving third-party solutions that minimize raw identity data collection.
- *Review post-gate design* to ensure that protective defaults—including content restrictions, contact controls, and advertising limitations—actually activate for identified minor users.
- *Monitor federal and state rulemaking*, including the FTC's forthcoming policy statement and possible COPPA Rule amendment, and assess California obligations under SB 243 (now in effect) and AB 1043 (operative 1 January 2027).

AUSTRALIA: AGE ASSURANCE TECHNOLOGY REACHES MATURITY

By: Cameron Abbott, Rob Pulham, Stephanie Mayhew

The Australian Government released its Final Report on the Age Assurance Technology Trial[17] at the end of 2025. Its findings will underpin the coming into effect of new rules to implement the social media minimum age limit laws, required to be in place by December 10.

The Final Report's key findings are:

1. Age assurance can be done in Australia privately, efficiently and effectively.
2. No substantial technological limitations preventing its implementation to meet policy goals.
3. Provider claims have been independently validated against the project's evaluation criteria.
4. A wide range of approaches exist, but there is no one-size-fits-all solution for all contexts.
5. We found a dynamic, innovative and evolving age assurance service sector.
6. We found robust, appropriate and secure data handling practices.
7. There is scope to enhance usability, risk management and system interoperability.
8. Parental control tools can be effective but may constrain children's digital participation and evolving autonomy.
9. Systems performed broadly consistently across demographic groups, including Indigenous populations.
10. Systems generally align with cybersecurity best practice, but vigilance is required.
11. Unnecessary data retention may occur in apparent anticipation of future regulatory needs.
12. Providers are aligning to emerging international standards around age assurance.

As noted on the eSafety Commissioner's website, there is a range of technologies available to check age, at the point of account sign up and later. It will be up to each platform to decide which methods it uses.

Social media platforms will now need to monitor the development of guidelines by the eSafety Commissioner and ensure that they take 'reasonable steps' to prevent users under 16 from having accounts on their platforms, using steps that are just and appropriate in the circumstances.

It appears these social media age limitation laws born so briskly late last year are now coming of age.

FROM THE FLOOR

FROM THE FLOOR

IAPP UK INTENSIVE 2026 UPDATE

By: Nóirín M. McFadden, Dr. Thomas Nietsch

Nóirín M. McFadden (London) and Dr. Thomas Nietsch (Berlin) attended this year's IAPP Intensive conference in London in February.

Thomas took part in a panel session on international data transfers alongside Emma Bate, director of legal services at the Information Commissioner's Office (ICO), Matt Houlihan, Vice President, Global Affairs, Europe at Cisco, and Gabriela Mercuri, Managing Director, SCOPE Europe. The panel was well attended, and comments made from the stage about the "trauma" of dealing with the aftermath of Schrems II and constantly shifting EU data-transfer requirements were referenced at other sessions during the conference. The panel was subsequently highlighted as one of the top three ranked panels at the conference.

Nóirín hosted a lively lunchtime roundtable on privacy, online safety, and age assurance—a particularly timely topic, as the protection of children's data was a recurring theme across the conference.

The Information Commissioner, John Edwards, delivered his final speech to this conference in his opening keynote. The ICO will be undergoing a restructure as the Data Use and Access Act (DUAA) takes effect and will be steered by a board in the future. The Commissioner's address covered themes of meeting the challenge of regulating privacy in the face of complex changes in technology. He referenced the ICO's investigation into X/xAI over Grok's inappropriate image generation and its decision—issued just the day before the conference—to fine Reddit nearly £14.5 million for the unauthorized processing of children's data.

Other notable talks included a panel on handling complex Data Subject Access Requests (DSARs), with insight into the issues that organizations face with this growing trend, and the ICO's approach to DSARs. Elsewhere, a session comparing the DUAA and the European Union's proposed digital omnibus suggested that the United Kingdom's data-protection regime is holding its own as a robust and secure framework post-Brexit.

ENFORCEMENT AND REGULATORY UPDATES

ENFORCEMENT AND REGULATORY UPDATES

AUSTRALIA

Australian Clinical Labs fined AU$5.8 Million for 2022 Medlab Data Breach in an Australian First

By: Cameron Abbott, Rob Pulham, Stephanie Mayhew

The Federal Court has ordered Australian Clinical Labs (ACL) to pay AU$5.8 million in civil penalties following a 2022 data breach involving its then-newly acquired Medlab Pathology business. The breach affected over 223,000 individuals whose data was accessed and infiltrated by malicious actors and is one of Australia's most significant healthcare cyber incidents.

This marks the first time civil penalties have been imposed under the *Privacy Act 1988* (Cth), setting a critical precedent for privacy enforcement in Australia.

ACL was found to have breached several obligations and was fined:

- *AU$4.2 million* for failing to take reasonable steps to secure personal information (APP 11.1), with over 223,000 contraventions of s 13G(a).
- *AU$800,000* for not conducting a timely and adequate assessment of whether the breach was an “eligible data breach” under s 26WH(2).
- *AU$800,000* for delays in notifying the Commissioner about the breach (s 26WK(2)).

Justice Halley described the breaches as “extensive and significant,” highlighting failures in senior management oversight, risk management, and the potential for serious individual harm. Although ACL cooperated, admitted liability, and began improving cybersecurity, the ruling is a warning to organisations handling sensitive information to have robust and compliant breach response processes.

With penalties having increased since ACL's breach, now up to AU$50 million per breach, this case signals a turning point in privacy enforcement in Australia and sends a clear message: serious privacy failures will come with serious consequences.

Key Lessons

13. Plan ahead: Delays in assessing and reporting breaches were penalised. Legal, cybersecurity, and privacy teams must align to ensure incident response frameworks are ready.
14. Cyber due diligence: Poor IT integration during ACL's acquisition of Medlab was noted. Acquirers must conduct thorough data and cyber due diligence, especially when sensitive personal information is involved.
15. Regulatory pressure is rising: This case used the old (lower) penalty regime. Under current laws, boards and executives face even greater accountability.

Mixed Blessings: Decision on Appeal by Bunnings Against Privacy Commissioner's Determination Re the Use of Facial Recognition Technology

By: Cameron Abbott, Rob Pulham

The Administrative Review Tribunal of Australia (Tribunal) has partially overturned the findings of the Privacy Commissioner on Bunnings' use of facial recognition technology (FRT) in its stores.

The Tribunal found FRT use was permitted as an exception to Australian Privacy Principle (APP) 3.3 due to the serious threats faced by staff and customers in Bunnings' stores, but affirmed that Bunnings:

- *Breached APP 1.2* by failing to implement practices, procedures and systems that would have ensured that they complied with the APPs, including not conducting a formal, structured and documented risk assessment of the FRT system from the outset which considered privacy implications—instead, the Tribunal found the steps taken "amounted to random enquiries and actions."
- *Breached APP 1.3* by failing to describe its use of FRT in its public Privacy Policy (statements related to images from video surveillance and other cameras in the stores were found not sufficient).
- *Breached APP 5.1* by failing to provide reasonable notice of its use of FRT in stores. Even Bunnings' entry notice stating that "video surveillance, which may include facial recognition, is utilised" was not sufficient—"use of the word 'may' did not positively convey that Bunnings was collecting individuals' sensitive information through an FRT system [and] fails to inform individuals about the purpose… or the main consequences of not collecting the information."

This demonstrates even where intrusive technology is permitted as a Privacy Act exception, failure to adequately and systematically consider its privacy impacts will amount to a separate breach. If you're going to use this kind of technology, make sure your notices are in order first!

An appeal period relates to the Tribunal's decision. One thing is certain—the expectations on reasonable steps (such as formal risk assessments) continue to increase even in the absence of formal Tranche 2 legislation.

NSW Expands Surveillance Powers and Introduces Public Interest Protections

By: Cameron Abbott, Damien Timms, Maryam Ahmed

The NSW Government has announced legislative reforms that will enhance the surveillance powers of investigative agencies including NSW's Independent Commission Against Corruption (ICAC).

Currently, under the *Surveillance Devices Act 2007* (NSW) (the Act), it is an offence to use a listening device (such as a phone) to record a private conversation. It is also an offence for a person to publish or communicate a private conversation that has come to their knowledge unlawfully, such as through the unlawful use of a listening device.

In 2023, the ICAC sought a temporary exemption allowing it to use such unlawful recordings in investigations. This exemption, originally due to expire in 2026, will now be permanently embedded in legislation and extended to other statutory investigative bodies.

Additionally, the Act will introduce a public interest exception, where individuals or organisations who come into possession of unlawfully made recordings (without having been involved in their creation), can share such material with authorities without fear of prosecution, provided they do so promptly. There is currently no protection in place for individuals acting in the public interest to report criminal activity or corruption.

NSW Attorney-General Michael Daley stated that these reforms are designed to "aid investigations into suspected criminal or corrupt conduct while maintaining important privacy considerations." While the reforms clearly do widen the scope of surveillance powers by government bodies, it is important to remember that the default position is that it remains an offence to use a listening device (such as a phone) to record a private conversation.

CHINA

Recent Enforcement and Regulatory Signals in China: Early 2026

By: Amigo L. Xie

Enforcement Update

Enforcement activity has become increasingly visible and detailed, with regulators releasing typical cases and statistics to communicate enforcement priorities. The Cyberspace Administration of China (CAC), together with the Ministry of Public Security and the Ministry of Industry and Information Technology, has continued large-scale inspections targeting apps, SDKs, and online platforms. The focus areas include the excessive collection of personal information, inadequate privacy notices, failure to obtain separate consent, and neglecting to conduct required impact assessments.

Compliance with cross-border data-transfer rules has emerged as a central enforcement concern. In 2025, authorities disclosed enforcement cases involving multinational corporations that transferred personal information out of China without completing the necessary national security assessments, securing licensed certification, or filing standard contracts. Many of these cases came to light during data breach investigations, highlighting that voluntary breach notifications do not exempt companies from penalties if outbound data-transfer requirements are not met.

Regulators have also targeted technology-driven violations, such as the unlawful use of facial recognition, over-collection of biometric data, and failures to conduct required security assessments or appropriately label AI-generated or “deep synthesis” content.

Recent enforcement actions increasingly integrate data protection, cybersecurity, and AI governance requirements, reflecting a more comprehensive regulatory approach.

Practical Takeaway for Compliance

Regulators now expect organizations to demonstrate documented compliance. Internal audits, data protection impact assessments, records of cross-border transfers, and evidence of remediation are no longer merely best practices—they are considered baseline requirements during enforcement reviews.

Recent cases show that enforcement is no longer limited to imposing fines. Authorities actively employ public naming, app removals, business rectification orders, and close scrutiny of cross-border transfers to ensure compliance. Particular attention is paid to obtaining proper consent, adhering to the principle of minimum necessity, implementing robust security measures, and maintaining thorough documentation of compliance efforts.

Regulatory Update

China's data protection regulatory landscape has evolved significantly, shifting from principle-based frameworks to more operational and enforceable compliance requirements. The most prominent development was the amendment of the Cybersecurity Law (CSL) in late 2025, which came into effect on 1 January 2026. These amendments further harmonize the CSL with the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), and introduce substantially higher penalties for serious violations.

Regulators have emphasized the importance of practical implementation. In January 2026, the CAC issued the Q&A on Personal Information Protection Policies and Regulations. This document provides authoritative guidance on challenges businesses face in complying with the PIPL, including clarifying what constitutes sensitive personal information and explaining requirements for obtaining separate consent for outbound transfers of personal data. Sector-specific guidance has continued to emerge, particularly focusing on industries such as finance, automotive, healthcare, and digital platforms. These

guidelines stress the need for internal accountability, robust data classification, and comprehensive lifecycle management of data.

Regarding cross-border data transfers, the CAC has further clarified three main legal mechanisms for compliance: national security assessment, standard contract filing, and licensed certification. In October 2025, the CAC and the State Administration for Market Regulation finalized the licensed certification pathway, completing the compliance framework and making it formally available from 1 January 2026. Between 2025 and January 2026, the CAC published four sets of Q&A documents addressing data export security management. These resources explain key issues such as the export of personal information, supervision of important data, and rules applicable to foreign-invested enterprises and free trade zones, thus providing clear and accessible solutions for common challenges in cross-border operations.

The CAC also continues to promote the use of "negative lists" within free trade zones, which enable more flexible outbound data flows in these areas. A significant new compliance requirement relates to the personal information of minors. From 2026 onward, organizations processing children's personal data must submit annual audit summaries to the CAC. This reinforces the regulatory focus on the protection of sensitive personal information and the importance of maintaining thorough, documented accountability.

EUROPEAN UNION

European Union Plans to Simplify GDPR and Other Digital Regulations

By: Dr. Thomas Nietsch

As part of its plan to increase the competitiveness of the European Union's tech sector and remove obstacles for tech companies operating in the European Union, the European Commission released a proposal[17] in November 2025 for a regulation providing for the simplification and optimization of several EU regulations, including the GDPR, the EU Data Act, and the EU AI Act (the Digital Omnibus).

The current plans include notably the following changes to the GDPR:

- Article 9 is supplemented with a legal basis for using special categories of personal data for training AI systems or AI models;
- A limitation of data subject's rights under Articles 15–22 of the GDPR if the data subject abuses these rights for purposes other than the protection of their data;
- A limitation of the data controller's obligation to provide a privacy notice to data subjects where the controller obtained the data directly from the data subject, does not process the data in a data-intensive manner, and it can be assumed that the data subject is already aware of the most relevant circumstances;
- For the notification of data breaches, a single point of contact is established, and notification deadlines are extended to 96 hours;
- Placing data on the terminal equipment of data subjects (commonly understood as "cookies") or extracting data from such terminal equipment is also permitted without consent for purposes of aggregated audience measurement and ensuring the security of an offered service; and
- A clarification is added that personal data may be used for the development and operation of an AI model or AI system based on Article 6(1)(f) of the GDPR (legitimate interests balancing test) unless the overriding interests of the data subjects prohibit such use.

The proposal will now be negotiated with the other EU legislative stakeholders, namely the European Parliament and the Council of the European Union.

UNITED KINGDOM

The Data (Use and Access) Act 2025

By: Noirin M. McFadden

The DUAA is coming into force across the United Kingdom, with a series of statutory instruments bringing most of the act into effect.

The DUAA amends the UK GDPR and empowers the ICO with enhanced enforcement powers.

Most of the changes to data-protection legislation in the DUAA came into force on 5 February. This marks the most significant operational step yet in the implementation of the DUAA.

The ICO published guidance on the new requirements on 12 February.

Summary of Key Changes

16. Research provisions: people can now give "broad consent" to use their data in an area of scientific research.
17. Automated decision-making: for nonspecial category personal data, the DUAA sets out the full range of "lawful bases" that can be relied on when using personal information to make automated decisions about people. This is expected to simplify regulatory compliance when using personal data in AI systems.
18. Cookie rules: organizations are no longer required to obtain consent to set certain types of cookies, e.g., to collect statistical information or improve website functionality. The ICO now has the power to levy higher fines for cookie noncompliance, in line with the level of fines for UK GDPR breaches.
19. New "recognized legitimate interests" lawful basis: where personal information is used for this purpose, organizations no longer need to balance the impact on individuals whose information is being used against the benefits (e.g., protecting public security).
20. Data subject access requests: codifying the existing regulatory guidance that only reasonable and proportionate searches are required when someone asks for access to their personal information.
21. Data protection complaints: from 19 June, organizations must have a process for handling data-protection complaints within their organization.

US NATIONAL SECURITY FEATURE

US NATIONAL SECURITY FEATURE

THE DOJ DATA SECURITY PROGRAM: A NATIONAL SECURITY RULE, NOT A PRIVACY RULE

By: Guillermo S. Christensen

We continue to encounter US companies that are unaware of the significant new requirements prohibiting or restricting the sharing or export of sensitive US personal data and government-related data to foreign adversaries like China—and compliance is often a complex undertaking. Finalized in January 2025 and fully effective in April, the US Department of Justice (DOJ) Data Security Program (DSP) implements Executive Order 14117. While implementation is sometimes delegated to data privacy counsel, this may cause considerable difficulties because the DSP is not a data privacy or data-protection rule. It is more akin to an export control or sanctions regime.

As the DOJ stated in the Final Rule, privacy protections and national security measures "generally focus on different challenges." The DSP creates no individual data rights, no consent requirements, and no breach notification obligations. Its purpose is to prevent certain countries from accessing, exploiting, and weaponizing Americans' bulk sensitive data and US government-related data for espionage, cyberattacks, and malign foreign influence. Companies accustomed to GDPR, CCPA, or HIPAA must approach the DSP with fresh eyes—it is in some ways more akin to an OFAC sanctions program.

Who Does the Rule Apply To?

The DSP applies to any US person—individual or entity—that knowingly engages in "covered data transactions" with "covered persons" connected to six countries of concern: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. Covered persons include foreign entities 50% or more owned by countries of concern, entities organized or operating in those countries, and individuals employed by or residing there. The 50% ownership rule tracks OFAC sanctions logic and requires careful mapping of beneficial ownership structures—something many companies have not previously had to assess in the context of data transfers.

Corporate structure does not provide a shield. A US parent company whose subsidiary is organized under the laws of a country of concern must treat that subsidiary as a foreign person subject to the rule. Multinational companies touching these six countries face the most immediate compliance exposure. On the other hand, the physical presence of a covered person in the United States may bring them outside the rule's scope, unless they are specifically designated by DOJ—a construct similar to OFAC sanctions.

What Data Is Covered?

The rule regulates two types of data. The first—and broadest in scope—is *government-related data*: precise geolocation data near sensitive US government facilities on the Government-Related Location Data List, and sensitive personal data marketed as linked to current or former US government employees, contractors, or officials. Critically, government-related data carries *no bulk volume threshold*—a single record can trigger the rule. Many companies that bid on US government contracts may already have exposure if they collect former federal employment records or if they identify employees as veterans.

The second category is *bulk US sensitive personal data*, covering six data types: human genomic data, biometric identifiers, precise geolocation data, personal health data, personal financial data, and

covered personal identifiers. Volume thresholds apply—ranging from more than 100 US persons for human genomic data, to more than 1,000 for biometrics and geolocation, 10,000 for health and financial data, and 100,000 for covered personal identifiers. These thresholds apply even where data is anonymized, pseudonymized, de-identified, or encrypted. In the case of GPS-level data, over 1,000 devices will trigger the application of the rule, and many companies access such data routinely for use in security and identity access management programs.

What Does "Access" Mean?

"Access" is the linchpin of the DSP and is defined with intentional breadth. Under § 202.201, the phrase refers both to logical and physical access—including the ability to obtain, read, copy, decrypt, edit, divert, release, or otherwise view or receive covered data through any information systems, cloud platforms, networks, or software.

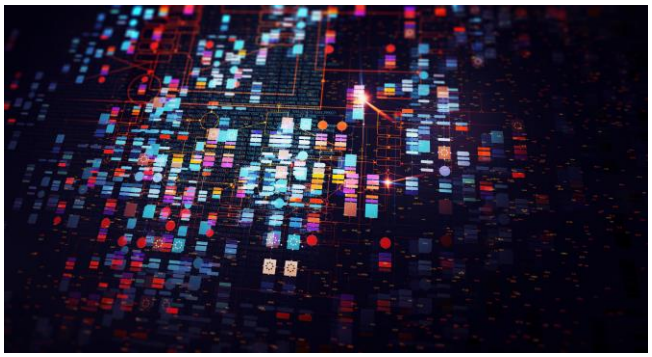
Three implications companies frequently underestimate: first, the physical location of data inside the United States is not sufficient to ensure compliance—remote access by a covered person to US-hosted data can still be a violation. Second, the DOJ has declined to distinguish between "access" and "export"—the ability to access sensitive data is treated as functionally equivalent to exporting it. Third, access is determined without regard to security measures—encryption or tokenization does not determine whether a covered data transaction has occurred, though those protections are critical to whether a restricted transaction may lawfully proceed under the CISA security requirements framework.

What Transactions Are Covered, and What Are the Penalties?

The rule creates a two-tier framework. *Prohibited transactions*—primarily data brokerage, broadly defined to include the sale, licensing, or similar commercial transfer of covered data—are categorically barred when involving a covered person. Companies often interpret "brokerage" narrowly as a "data broker" business model; the DOJ's definition is far wider. *Restricted transactions*—vendor, employment, and nonpassive investment agreements—may proceed only if mandatory CISA security requirements are satisfied, including access controls, MFA, encryption, and 10-year recordkeeping. Exemptions exist but are narrow and fact-specific.

When a prohibited transaction is offered and rejected, a report must be filed with the DOJ's National Security Division within *14 business days*. This is an important obligation that companies must factor into their compliance program.
Penalties are severe by design. Civil penalties reach the greater of US$368,136 or twice the transaction value. Willful criminal violations carry up to US$1,000,000 in fines and 20 years imprisonment.

We expect the DOJ to begin announcing enforcement actions in the near term. The enforcement emphasis at the federal level is already quite clear: the FTC recently sent warning letters to 13 data brokers under the related PADFAA statute, which similarly prohibits transfers of Americans' sensitive data to foreign adversaries, including China, Russia, Iran, and North Korea.



LITIGATION CORNER

LITIGATION CORNER

SOUTH CAROLINA'S AGE-APPROPRIATE CODE DESIGN ACT: A NEW FRONTIER FOR PRIVATE RIGHTS OF ACTION IN DATA PRIVACY

By: Michael J. Stortz, Isabella F. Sparhawk, Tre A. Holloway

On 5 February 2026, South Carolina enacted the Age-Appropriate Code Design Act (the Act) that immediately imposed significant obligations on covered online services[19] likely to be accessed by minors. While the statute shares many features with similar "age-appropriate design" laws in other states, it stands out for a unique provision: a private right of action for certain violations linked to the South Carolina Unfair Trade Practices Act (SCUTPA). This development places South Carolina at the forefront of a new and largely untested area of data privacy enforcement, raising important questions about how such private rights might function in practice and what risks and opportunities they present for both businesses and consumers.

The Private Right of Action: A Distinctive Feature

Most state-level age-appropriate design codes and broader data-privacy statutes rely exclusively on public enforcement by attorneys general or regulatory agencies.[20] The Act, however, explicitly provides that violations of its prohibition on "dark patterns," which are defined as user interfaces designed to subvert or impair user autonomy or choice,[21] constitute an unlawful trade practice under SCUTPA.[22] This definition is broad and focuses on the effect of the design rather than the intent behind it, capturing a wide range of manipulative digital practices. SCUTPA, in turn, allows individuals who suffer an "ascertainable loss of money or property, real or personal" as a result of an unfair or deceptive act to bring a private lawsuit for damages, potentially resulting in injunctive relief, civil penalties, and actual damages, and in some cases, treble damages and lawyers' fees.[23]

How Might the Private Right of Action Work?

The statute's reference to SCUTPA means that private plaintiffs must still meet SCUTPA's threshold requirements, which could prove challenging in practice. First, a plaintiff must show that they suffered an "ascertainable loss" as a result of the use of a dark pattern. Many of the harms such as compulsive usage, emotional distress, or privacy intrusions affecting minors do not easily translate into economic loss. Plaintiffs may attempt to frame losses in terms of unwanted in app purchases, subscription fees, or the diminished value of personal data.

Second, causation may prove difficult. Plaintiffs will need to connect a specific design choice, such as an infinite scroll feature or a confusing opt out flow, to a concrete financial loss.

Courts may struggle to distinguish unlawful dark patterns from design decisions that are merely persuasive, common, or industry standard.

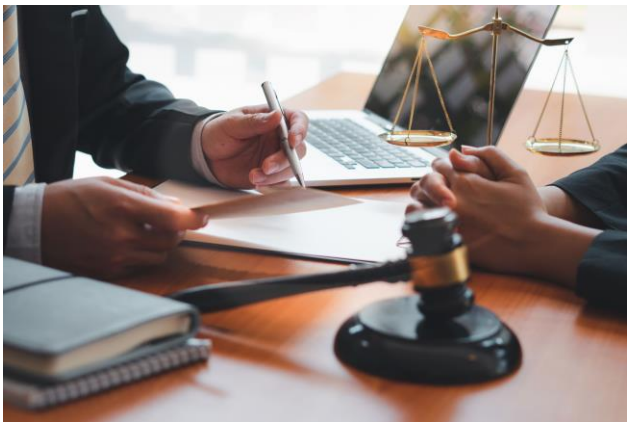
Third, standing issues loom large. Although the law is framed around protecting minors, SCUTPA claims are traditionally brought by consumers who have themselves suffered economic harm. Whether parents can sue based on harms to their children, and under what circumstances, is likely to be contested early and often.

Moreover, the statute does not create a private right of action for all violations of the Act, only for those involving dark patterns. Other obligations, such as data minimization, parental controls, and reporting requirements, remain enforceable solely by the attorney general.

Legal Challenges and Future Developments

As the law currently stands, on 1 July 2026, the covered online service must issue a public report

prepared by an independent third-party auditor that contains a detailed description of the covered online service as it pertains to minors, including its covered design features, its use of personal data, and its business practices.[24] The public report must be submitted to the attorney general, who shall post it in a prominent place on his internet website.
However, it is important to note that the Act is already facing legal challenges, including a lawsuit filed by NetChoice, a nonprofit trade association for internet companies, shortly after the law's enactment.[25] While many challenges will likely focus on constitutional questions such as preemption, First Amendment concerns, and the scope of state authority, the fate of the private right of action will be closely watched by privacy professionals and litigators alike. If the law survives judicial scrutiny, South Carolina's experiment could serve as a model for other states considering similar legislation.



Conclusion

The Act marks a significant development in the landscape of data-privacy regulation, particularly through its introduction of a private right of action tied to SCUTPA. By empowering individuals to seek redress for harms caused by manipulative “dark patterns,” the Act not only raises the stakes for online service providers but also opens new avenues for consumer protection and legal innovation. However, the practical impact of this provision remains uncertain, as courts and litigants grapple with complex questions of standing, causation, and the definition of actionable harm. The ongoing legal challenges and the law's fate will be closely watched for precedent-setting decisions in the realm of children's online data privacy.

ENDNOTES

ENDNOTES

[1] 90 Fed. Reg. 898 (proposed Dec. 27, 2024) [hereinafter, Proposed Rule].

[2] *Id*. at 900-1.

[3] *Id*. at 899.

[4] *HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information Fact Sheet*, US Department of Health and Human Services (Dec. 27, 2024), https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html.

[5] Proposed Rule, at 1,016.

[6] *Id*. at 916.

[7] *Id*. at 1,014, 1,018.

[8] *Id*. at 926.

[9] *Id*. at 928.

[10] *Id*. at 937.

[11] *Id*. at 1,013.

[12] *Id*. at 934.

[13] Andrew Ferguson, Chairman, FTC.

[14] Sara Kloek, Vice President, Education and Youth Policy at Software & Information Industry Association.

[15] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB243

[16] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043

[17] https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

[18] https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report

[19] S.C. Code Ann. § 39-80-10 “Covered online service” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that owns, operates, controls, or provides an online service that conducts business in this State, is reasonably likely to be accessed by minors, determines the purposes and means of the processing of consumer's personal data alone, or jointly with its affiliates, subsidiaries, or parent company and either: (A) has annual gross revenues in excess of twenty-five million dollars, adjusted every odd-numbered year to reflect changes in the Consumer Price Index; (B) annually buys, receives, sells, or shares the personal data of fifty thousand or more consumers, households, or devices alone or in combination with its affiliates, subsidiaries, or parent company; or (C) derives at least fifty percent of its annual revenue from the sale or sharing of consumers' personal data.

[20] California's Age Appropriate Design Code Act, enacted in 2022, is enforceable solely by the state attorney general and expressly disclaims a private right of action. Maryland followed a similar path with its “Kids Code,” enacted in 2024, which relies exclusively on public enforcement and has been partially stayed amid constitutional challenges.

[21] S.C. Code Ann. § 39-80-10 (5) “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

[22] S.C. Code Ann. § 39-80-60 (C) Covered online services are prohibited from using dark patterns. (1) Use of dark patterns by a covered online service shall constitute an unlawful trade practice under Section 39-5-20 of the South Carolina Unfair Trade Practices Act. (2) A covered online service that violates the provisions of this section are subject to the provisions, penalties, and damages of the South Carolina Unfair Trade Practices Act.”

[23] S.C. Code Ann. § 39-5-140.

[24] S.C. Code Ann. § 39-80-70 (A).

[25] NetChoice filed a Complaint challenging the law on 9 February 2025.

EDITORS AND AUTHORS

EDITORS

Whitney E. McCollum
Partner
Seattle, San Francisco

Michael J. Stortz
Partner
San Francisco

Dr. Thomas Nietsch
Partner
Berlin

AUTHORS

Cameron Abbott
Partner
Melbourne

Jake Bernstein
Partner
Seattle

Sarah L. Carlins
Of Counsel
Pittsburgh

Guillermo S. Christensen
Partner
Washington, DC

Eric F. Vicente Flores
Associate
Washington, DC

Martin A. Folliard
Associate
Research Triangle Park

Tre A. Holloway
Associate
Washington, DC, Charleston

Alice MacHenry
Trainee Solicitor
London

Stephanie Mayhew
Senior Associate
Sydney

Noirin M. McFadden
Consultant
London

Rob Pulham
Special Counsel
Melbourne

Isabella F. Sparhawk
Associate
Charleston

Clarita I. Sullivan
Associate
Research Triangle Park

Amigo L. Xie
Partner of K&L Gates LLP and Registered Foreign Lawyer
Hong Kong

K&L GATES

K&L Gates is a fully integrated global law firm. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.