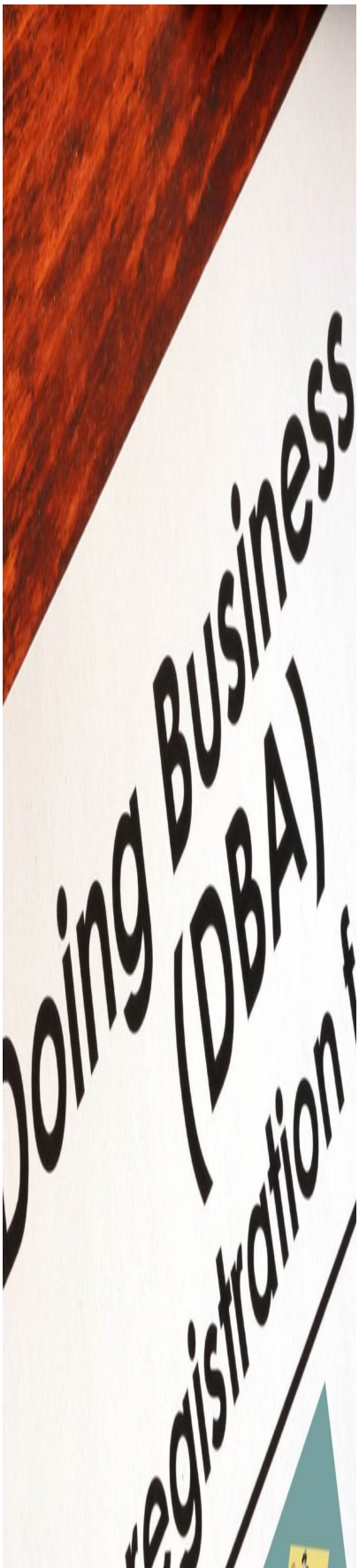
# June 2025 FZLZ Minute

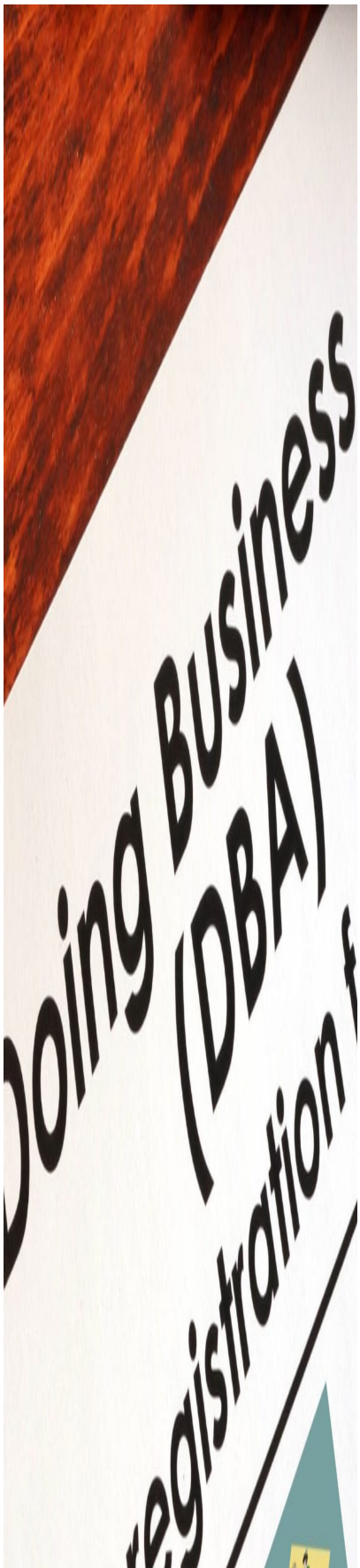
**Delaware** – ***August 1 deadline for businesses to preserve DBA names on a statewide basis***


Doing Business
(DBA)

FROSS ZELNICK

**Prior to a new law enacted this year, companies that wanted to register DBA names in Delaware had to do so in each county they wanted to use them in,More**

## Delaware – *August 1 deadline for businesses to preserve DBA names on a statewide basis*


Doing Business
(DBA)
registration

Prior to a new law enacted this year, companies that wanted to register DBA names in Delaware had to do so in each county they wanted to use them in, which usually meant all of them. (Granted, this burden was less onerous than it would be in any other state, since Delaware only has three counties, New Castle, Kent, and Sussex, the fewest of any state in the union.) Under the new law, effective June 2, companies can register DBAs with the Delaware Division of Revenue and can no longer register them with individual counties.

But this applies to DBAs that have already been registered with Delaware counties. Failing to re-register a DBA with the state by August 1 will cause the DBA to lose its priority such that another filer could claim the DBA if they are the first to file.

More details:

- Once a DBA is registered in Delaware State, it remains active as long as the business license does and need not be renewed.
- Even if a company is not doing business in Delaware, it can register its DBA with the state, if it owns a Delaware Business License or Trade Name Only license. Trade Name Only is a new type of Delaware license for entities seeking DBA protection. Entities may find they need such a license for contractual, intellectual property, or other legal reasons.
- Notarization is no longer required when registering a DBA.

So, those who have registered a DBA in a Delaware county should re-register it with the state now. Those who do business in Delaware under a name that is different from the name of their legal entity but have never registered it with a Delaware county should register the DBA with the Delaware Division of Revenue as soon as possible. If someone else does first, you will have lost the opportunity.

**Copyright – *District court finds fair use defense applies in a copyright infringement action even though the defendant never answered or appeared* – *Romanova v. Amilus Inc.*, No. 23-828 (2d Cir. May 23, 2025).**


COPYRIGHT

Jana Romanova, a professional photographer, published in *National Geographic* a photograph of a woman with two pet snakes. When Amilus Inc. reprinted Romanova's photograph on its website without her permission, she sued for copyright infringement. Amilus failed to answer the complaint or respond to a motion for a default judgment. But instead of granting a default judgment, the district court did something highly unusual: it ordered Romanova to explain why the defendant's publication of her photograph was not "fair use." Romanova submitted a response, but the district court dismissed the complaint with prejudice, concluding that the fair use defense was "clearly established on the face of the complaint."

The district court found that the defendant's purpose in using the photograph was, as stated on defendant's website, to focus on the "ever-increasing amount of pet photography we find online."

On appeal, the Second Circuit reversed. In a 43-page opinion, Judge Pierre Leval wrote that the district court's decision "depended on a misunderstanding of the fair use doctrine." Fair use, Judge Leval explained, "turns on whether *the copying of the original* communicates a message that differs from the message of the original – not whether the copier separately declares such a message." The opinion goes on: "Amilus's republication of the snake image did not show that there was a growing trend to publish pet photos online. . . . Notwithstanding what Defendant said about Plaintiff's image, its unauthorized copying and distribution of the image communicated no message other than what the original image communicated." Amilus's conduct was "commercial exploitation of Plaintiff's work, selling it to its own customers for its own profit, competing in a market that the copyright law reserves exclusively to Plaintiff."

The Second Circuit reversed and remanded, with instructions to enter a default judgment. One member of the Second Circuit panel, Judge Richard Sullivan, would not have reached the fair use issue. "I would reverse on a narrower ground," he said, "without wading into the merits of Amilus's unasserted fair use defense. In my view, the district court procedurally erred in *sua sponte* raising the affirmative defense of fair use on behalf of a non-appearing defendant, which is reason enough on these facts to reverse and remand the district court's order."

## DATA PRIVACY

### USA – *A Decade-Long Freeze? U.S. Congress' Proposed Moratorium on State-Level AI Regulations*

On May 22, 2025, the U.S. House of Representatives narrowly passed H.R. 1, informally called the One Big Beautiful Bill Act ("OBBB"). Buried within this massive budget bill is a controversial provision pertaining to artificial intelligence that would block state and local governments from "enforc[ing] any law or regulation regulating AI models, AI systems, or automated decision systems during the 10-year period beginning on the date of the enactment of this Act." This moratorium would broadly affect state-level regulation of AI systems – from popular models like ChatGPT to more obscure models used in business, research, public utilities, and education. Under the House's draft, any state law imposing a "substantive design, performance, data-handling, documentation, civil liability, taxation, fee, or other requirement" on covered AI systems would be barred, unless such law were imposed under federal law or were effectively a neutral or generally applicable law that applied equally to AI systems and models and other technical systems and models.

Unsurprisingly, this moratorium drew immediate backlash from state legislators and consumer advocates favoring more hands-on AI regulation, while large tech companies – like Google and OpenAI – welcomed the moratorium as a means to dismantle a burdensome regulatory "patchwork" that could hinder model expansion and development. The fate of the OBBB stood with the Senate, which proposed amendments to make the moratorium more palatable to critics and avoid procedural challenges. Congress aims for final enactment on or around July 4, 2025. Notably, the moratorium had been linked to eligibility for federal broadband funding and narrowed to apply only to "generally applicable law[s] . . . ," the scope and interpretation of which remains unclear. By specifically tying the moratorium to approximately $42 billion of federal funding and limiting the scope of its reach, the Senate's amendments were designed to shield it from being disqualified under the Byrd Rule, which requires that all parts of a budget reconciliation bill primarily address budgetary matters.

At the time of publication of this article, the Senate has approved a revised version of the moratorium, now restyled as a "temporary pause," that satisfies the Byrd Rule by tying compliance with the ban on state-level enforcement of AI legislation to availability of $500 million in funding aimed at supporting the modernization, development, and deployment of AI systems. However, the revised text contains a deobligation provision that applies to the $42 billion in previously obligated broadband funding to the

states, in addition to the new $500 million. The result is that a state that accepts any portion of the newly appropriated $500 million, and is later found to have violated the moratorium, could possibly have any previously obligated broadband funding clawed back. Notwithstanding recent changes in the proposed language, the backlash against these provisions of the OBBB remains strong, even across party lines. The upcoming days will determine whether the OBBB, including the "temporary pause" in its current form or otherwise, will be enacted by the July 4th target date.

It remains unclear how the current draft may impact enforcement of state data privacy laws. General laws involving human rights, employment, or IP infringement by AI may be permitted to be enforced, while more specific privacy regulations – such as those addressing AI profiling, algorithmic bias, deceptive advertising, consumer protection, and governmental AI use – may still be banned from enforcement. States such as Colorado, Utah, Tennessee, California, Illinois, Maryland, Wisconsin, Alabama, Oregon, New York, and Texas have already enacted such regulations, and roughly 20 states have passed or introduced legislation that may become unenforceable if the OBBB, as drafted, becomes law.

In response, state lawmakers are advocating for removal or revision of the moratorium and generally favor adopting a tailored federal framework that facilitates state-level experimentation and enhanced AI protections. Currently, no such federal framework exists in the U.S., in contrast to jurisdictions including the EU, China, Brazil, and South Korea, which are taking the lead with respect to regulation. The EU AI Act remains the most comprehensive AI legal framework and continues to spark debate as its provisions come into effect.[1] **Takeaway**: Although the fate of the OBBB's AI moratorium remains unclear, the importance of monitoring the evolution of domestic and global AI regulation continues to grow. In the absence of a harmonized set of state AI regulations or a comprehensive federal AI law, global frameworks such as the EU AI Act will continue to have significant effects on U.S. companies and consumers, and the proposed moratorium will not halt extraterritorial enforcement of such laws. Given the evolving AI regulatory landscape and that the proposed moratorium will not halt extraterritorial enforcement of global AI laws, we advise our clients to (i) map their current and planned uses of AI systems and memorialize sources of creation and training of AI systems; (ii) monitor global AI regulatory frameworks and develop applicable AI governance policies and practices, as appropriate; and (iii) consult with counsel to facilitate compliance with rapidly evolving AI regulatory frameworks.

European Union: Artificial Intelligence Act – Extraterritoriality.

## USA -The Ninth Circuit Widens Personal Jurisdiction in Online Privacy Matters

The Ninth Circuit Court of Appeals recently issued a decision that expands the contours of personal jurisdiction for e-commerce websites and platforms. The key question in *Briskin v. Shopify, Inc.* has been whether the global e-commerce platform Shopify was subject to specific personal jurisdiction in California for allegedly violating the California Consumer Privacy Act (CCPA). The Ninth Circuit, addressing the matter *en banc*, reversed its prior three-judge ruling that had upheld the lower court's dismissal of the plaintiffs' claims based on lack of personal jurisdiction. The reversal of opinion on personal jurisdiction will doubtless affect companies that operate commercial websites on a national scale.

In this class action lawsuit, Brandon Briskin, a California resident, alleged that Shopify, Inc., a Canadian-based online retail business with U.S. affiliates, had installed tracking cookies on his device without his knowledge or consent. These cookies allegedly collected sensitive personal data, which Shopify then used to create marketable consumer profiles that it sold to or shared with third parties.

In its defense, Shopify took the position that its actions were not expressly aimed at California, but rather, operated on nationwide scale and therefore did not target specific states. The Ninth Circuit dismissed this argument, citing the U.S. Supreme Court's decision in *Ford Motor Co. v. Montana Eighth Judicial Dist. Ct.* (2021), where it rejected the notion that "because a nationwide company is everywhere, it is jurisdictionally nowhere except in its principal place of business and state of incorporation."

Shopify further argued that its actions would have had to be considered "differential targeting" of a specific state for the company to be subject to specific jurisdiction. The Ninth Circuit dispensed with this argument too. It concluded that Shopify's contacts with California demonstrated purposeful direction toward the state, including because Shopify installed trackers, collected personal data, profited from consumer profiles it created based on that data, and could use its geolocation tracking technology to determine that Briskin was located in the state. Consequently, the court held a business operating anywhere in the country can be subject to jurisdiction in a state where its conduct causes harm, so long as the connections with that state are not "random, fortuitous, or attenuated."

In an apt analogy to the pre-internet era, the court stated that "there would be no doubt that the California courts would have specific personal jurisdiction over a third party who physically entered a

Californian's home by deceptive means to take personal information from the Californian's files for its own commercial gain." The judicial panel held that even when an online platform creates a "nationwide audience[] for commercial gain," its conduct is "expressly aimed" toward a specific state when it contacts the state's residents based on its own choice (i.e., installing trackers) rather than random or isolated events.

The Ninth Circuit's decision in this case effectively broadens the application of personal jurisdiction in the context of online commerce and increases the risk of litigation or regulatory action. The court removes the requirement for differential targeting. Now, deliberately collecting data from California residents using common tracking technologies may create personal jurisdiction in the residents' home state.

**Takeaway:** Commercial activities conducted online may not be subject to traditionally defined legal boundaries. Depending on how purposeful or intrusive a company's conduct is with respect to data collection, it may be subject to specific jurisdiction in all states, even those without comprehensive privacy laws. Businesses should review their consumer-facing privacy notices to ensure transparency about their collection, use, and sharing of personal data. Moreover, they should evaluate the necessity of all aspects of their data collection—especially through common tracking technologies and geolocation mechanisms—to mitigate potential risk from regulators and plaintiffs.

## INTERNATIONAL

### Thailand – *Acquired distinctiveness through use (Kiddie's Paradise Inc. v. Department of Intellectual Property)*

In 2017, Kiddie's Paradise Inc. filed for a variety of goods in Class 28. The Registrar rejected the application as descriptive of "playthings," a decision upheld by the Board of Trademarks on appeal. In 2024, while the IP & IT Court agreed on further appeal that WEPLAY was non-distinctive for the covered goods, it found the mark registrable based on evidence of continuous use in Thailand, conclusively demonstrating extensive sales and advertising (online and print) for over 10 years. On February 25, 2025, the Court of Appeal for Specialised Cases (Court of Appeal), on appeal by both

parties, went even further, finding the term WEPLAY was suggestive (not descriptive). When combined with the figurative element, the Court of Appeal held that the mark as a whole was inherently distinctive. In a similar case involving Hewlett Packard's LASERJET mark, the Registrar and Board rejected the mark as descriptive, the IP & IT Court found the mark inherently distinctive, and the Supreme Court held on final appeal (November 2008) that the mark was registrable based on acquired distinctiveness, not inherent registrability.

Takeaway: Although the Registrar and Board appear to continue their more conservative approach, the Thai courts are more inclined to take into account evidence of long-term use when considering registrability of terms that might otherwise be deemed descriptive. Trademark owners active in this jurisdiction are advised to carefully maintain documentation of use, including invoices, advertising material of all kinds, as well as any other evidence of local presence.

## Canada – *Quebec French language requirement – coming into force June 1, 2025 for language on goods and public signage*

*Section 51.1 of the French Charter and section 7.1 of the Regulation*

Under these provisions any generic or descriptive language on goods, labels or packaging must be translated into French and affixed to the goods themselves or on a medium attached to the goods, and be as prominent as the non-French language. There are certain exceptions – for example, the "brand name" or company name need not be rendered in French, even if generic or descriptive. Examples are set out in the practical guide here. While the guide is in French, there is an English translation. There is a two-year grace period (to June 1, 2027) for compliance with section 51.1 for products manufactured before June 1, 2025.

*Section 58.1 of the French Charter and section 25.1 of the Regulation*

Under these provisions, when a trademark (even in part) appears on public signage or in commercial advertising in a language other than French, the "markedly predominant" requirement applies. Thus, non-French terms must be accompanied by French terms, and the French text (a generic or descriptive term or a slogan) must have the greater visual impact. Again, examples of compliant and non-compliant usages are set out here. There is no grace period for compliance with Section 58.1 relating to public signage or commercial advertising.

We note that there is a “recognized trademark exception” for non-French trademarks that are registered in Canada or have been in use with goods or services in Canada. Such marks need not be translated into French when on goods, in a commercial publication or in public signage and commercial advertising, so long as no French version of the mark is registered in Canada. However, the exception has limitations. Seek advice to understand the applicability of this exception. Also, this summary does not address the many other complexities relating to compliance. So, do consult with counsel to learn more.

**Takeaway:** Non-compliance with the French Charter and Regulations can be subject to fairly harsh sanctions including, without limitation, fines, potential loss of business permits in instances of repeated non-compliance and potential destruction of goods, advertising material, and signage. The Office Québécois de la Langue Française also has the power to make criminal referrals. Accordingly, trademark owners active in Quebec must take care to comply.