

# ePRIVACY NEWSLETTER

FEBRUARY 2025



AMERICAN BAR ASSOCIATION

Science & Technology  
Law Section

## This Issue:

- Message from the Editors
- Important privacy news and developments in January
- Interview with Member
- Privacy job postings & Events
- How to get involved
- Meet our Editors

THE MONTHLY NEWSLETTER OF THE  
AMERICAN BAR ASSOCIATION'S SCIENCE &  
TECHNOLOGY LAW SECTION EPRIVACY  
COMMITTEE

Dear Committee members,

We are pleased to provide you with the ePrivacy Committee newsletter for February, 2025. A special thanks to our law school contributors for their assistance with the preparation of this month's newsletter.

We hope that you enjoy reading these articles!

Keep reading to learn more about the latest in privacy news, exciting events, and job opportunities.

As always, please do not hesitate to reach out to Committee Leadership or the Editors if you would like to get involved in the Committee!

# WHAT HAPPENED IN PRIVACY LAST MONTH?

## **1. NEW DELAWARE DATA PRIVACY ACT TAKES EFFECT**

In January, the Delaware Personal Data Privacy Act came into effect. The act requires businesses to obtain consent before collecting personal information. Delaware's Department of Justice will govern and enforce this act. [See more here.](#)

## **2. BITWARDEN RELEASES TOP DATA PRIVACY APPS LIST**

In January, to help celebrate Data Privacy Week, Bitwarden released its top data privacy applications. The list was created based on feedback from over 3,000 Bitwarden community members. [See more here.](#)

## **3. FTC AMENDS CHILDREN'S ONLINE PRIVACY ACT**

In January, the FTC announced that education tech vendors and companies providing online services to children under 13 will face new obligations for safeguarding personal information. These new obligations will help strengthen data collection and advertising requirements for children targeted advertising. [See more here.](#)

## **4. FCC PRIVACY RULE SHOT DOWN BY THREE PANEL JUDGE**

On January 2nd, a three-panel judge overturned the FCC's rule preventing broadband providers from unfairly throttling internet speed. The court found that the FCC lacked the authority to classify broadband internet service as a telecommunications subject to stricter regulations. [See more here.](#)

## **5. EU COURT FINES EU FOR BREACHING ITS OWN DATA PRIVACY LAW**

On January 8, 2025, The EU General Court ruled that the European Commission must pay damages to a German citizen. The EU is accused of failing to comply with its data protection regulations. Specifically, the EU transferred the customer's data to the U.S. without the proper safeguards. [See more here.](#)

## **6. NEW YORK PASSES NEW HEALTH DATA PRIVACY LAW**

On January 21, 2025, New York passed the New York Health Information Privacy Act (NYHIPA). The bill enforces strict requirements on "regulated entities" that process "regulated health information" (RHI) related to New York residents. The bill is set to take effect in 2026. [See more here.](#)

## **7. ATTORNEY GENERAL BONTA SENDS REMINDER TO CONSUMERS TO OPT-OUT**

On January 29, 2025, California Attorney General Rob Bonta reminded consumers about their right to opt out of the sale of personal information. this right is recognized under the California Consumer Protection Act (CCPA). In addition to this right, Governor Bonta requested that consumers familiarize themselves with the Global Privacy (GPC) browser setting. [See more here.](#)

## **8. OREGON DOJ INTRODUCES DATA PRIVACY TOOLKIT**

On January 30, 2025, the Oregon Department of Justice Launched a data privacy toolkit to assist families in protecting online information. The toolkit guides parents in monitoring, managing, and restricting the collection of children's information. In addition to children's rights, it offers instructions on requesting various information related to personal privacy rights. [See more here.](#)

## **9. FRENCH PRIVACY WATCHDOG INVESTIGATES DEEPSEEK ON AI AND DATA PRIVACY PRACTICES**

On January 30, 2025, the French-based Commission Nationale de Informatique et des Libertes (CNIL) announced it would investigate DeepSeek's privacy practices. DeepSeek is accused of creating multiple privacy risks for customers, leading to potential violations of the GDPR. [See more here.](#)

## **10. ITALY BLOCKS DEEPSEEK AI OVER DATA PRIVACY CONCERNS**

On January 31st, 2025, Italy's Data Privacy watchdog blocked DeepSeek access due to data privacy and ethical concerns. DeepSeek is an Artificial Intelligence application that recently gained popularity as one of the top mobile applications in the world. DeepSeek is accused of creating an environment that is harmful to potential attacks and has insufficient data storage processes. [See more here.](#)

# FROM LITIGATION TO LEADERSHIP: A CONVERSATION WITH TRISH CARREIRO

TRISH CARREIRO | [PCARREIRO@CARLTONFIELDS.COM](mailto:PCARREIRO@CARLTONFIELDS.COM)

 [LINKEDIN](#)



In today's fast-changing landscape of data privacy, cybersecurity, and artificial intelligence (AI) governance, the demand for skilled lawyers has never been greater. Trish Carreiro, shareholder and head of the Cybersecurity and Privacy practice group at Carlton Fields, has built a remarkable career by adapting to these challenges. In this interview, Trish shares her professional journey, discusses the nuances of privacy law, and offers insights for those looking to enter the field.

## ***Charting a Path to Privacy Law***

Like many privacy lawyers of her generation, Trish did not begin her legal career in the field she now leads. "I didn't know this field existed when I was in law school—it wasn't really a thing back then," she explains. Her journey started in general litigation at Wofsey Rosen, one of Connecticut's oldest firms, where she appeared in court almost daily. While the experience was invaluable, she realized her true interest lay in business litigation, which prompted her move to Axinn in Hartford.

"On my first day there, I asked the head of litigation what he thought was next. He mentioned privacy and cybersecurity, and that stuck with me," she recalls. Intrigued, Trish spent the next week immersing herself in the topic, reading every privacy and cybersecurity decision she could find. This deep dive led to publishing articles, earning privacy certifications, and ultimately transitioning her practice to focus on these emerging areas.

The next chapter of her career was shaped by a bold decision: relocating to Florida. "I wanted to be near my sister and escape the cold," she says. After passing the Florida bar, Trish reached out to firms with strong privacy practices, ultimately joining Carlton Fields. "I knew immediately this was the right place for me," she says. Her instinct proved correct—Trish quickly rose to shareholder and practice group leader.

## ***Privacy, Cybersecurity, and AI: Blurred Lines***

As privacy, cybersecurity, and AI increasingly intersect, the distinctions between these fields often become muddled. Trish frequently encounters this confusion, even among legal professionals. "People sometimes mistake me for an IP lawyer or don't realize there's a distinction between privacy and cybersecurity," she explains.

While privacy law focuses on compliance with data protection laws and litigating privacy-related claims, cybersecurity mostly involves preparing for and responding to incidents. AI governance, meanwhile, largely deals with the ethical and legal implications of data-driven technologies. Despite their differences, the three areas are deeply interconnected. "For instance, understanding how data is collected and used is essential to all three," Trish notes.

The rise of AI has brought new complexities to her work. Trish advises clients on AI governance, helping them address risks while navigating a regulatory landscape that is still evolving. “AI governance is fairly nascent right now, but it’s guaranteed to continue evolving as AI becomes more integrated into business operations,” she says. She predicts that the demand for legal guidance will only grow. She views privacy professionals as a natural fit for this work because of their experience with data, technology, and the risks surrounding application of rapidly changing legal requirements to these practices. She says that many of the same mechanisms used for privacy compliance (e.g., data flow considerations, notices and consents, and risk assessments) and concepts (e.g., notice, transparency, the ability to opt-out and/or understand the basis for a decision) underpin AI governance as well. While Trish says that this doesn’t make privacy attorneys qualified to provide insights on AI governance, she believes it helps explain why so many privacy professionals embraced the challenge of expanding their expertise into this area. “Few are better positioned,” she says.

### ***Navigating Media Narratives and Market Demand***

The increasing visibility of privacy law in media has shaped public perceptions of the field, but Trish notes that businesses often underestimate their needs. “Many companies don’t realize how much data they’re collecting or what obligations they have,” she says. For example, clients frequently believe their websites don’t collect data, only to discover otherwise when she conducts a scan.

She also observes that larger companies tend to be more aware of their obligations, while smaller businesses sometimes focus on growth at the expense of compliance. “Sometimes we’re building the plane in flight,” she remarks. Bridging this gap is a key part of her role, as she helps clients align their practices with regulatory requirements and anticipate potential risks.

### ***A Day in the Life of a Privacy Lawyer***

Trish’s day-to-day work is as varied as the field itself. “One moment I might be drafting a privacy policy or negotiating a data processing agreement, and the next I’m on the phone with opposing counsel in a class action,” she explains. Her work often involves advising clients on new technologies, such as mobile apps or AI tools, and ensuring their data practices comply with privacy laws. The fast pace and constant evolution of privacy law are what keep her engaged. “The laws are changing, the technology is changing, and even cultural norms around data are changing,” she says. “It’s never static, which is one of the reasons I love it.”

### ***High-Stakes Litigation and Risk Management***

One of the most challenging aspects of Trish’s work is high-stakes litigation, particularly class actions involving privacy claims. These cases often involve large groups of individuals and statutory damages, combined with novel theories and a dearth of consistent case law, making them complex and potentially costly. When navigating these situations, Trish focuses on three areas: the law, the facts, and the motivations. Her analysis of the law focuses on what the law actually says, the legislative history behind that phrasing, the nuances and intricacies of existing case law, and the unspoken “why” behind existing decisions. Her analysis of the facts focuses on the relative strength of the claims alleged, the alignment with prior decisions, the available evidence, and the potential narratives surrounding those facts. Lastly, Trish stresses the importance of never forgetting the motivations and goals involved, which she describes as essential for resolving the dispute “as efficiently as possible.” “Sometimes we can get rid of these cases without a single filing or payment. That’s a good day, but you need to be able to explain why that makes sense not only for the defendant, but for the plaintiffs and their counsel as well.”

Trish's approach to risk management is informed by her litigation experience. She works closely with clients to evaluate their options, balancing legal compliance with business objectives. "I might present two reasonable paths and assess the litigation risks and costs for each," she says. "It's about finding solutions that align with the client's goals while minimizing future risks."

### ***Pressing Challenges and Best Practices***

One of the greatest challenges is simply the speed of progress. Trish explains that the applicable laws, the litigation risk, regulatory enforcement priorities, and the technologies and data being used are constantly changing and demand relentless education and fresh analysis to accurately address. She explains: "It is a constant cycle, which will either you thrill you or chew you up and spit you out." For Trish, there is always more to learn and analyze because it's not just about what's required or risky now. "We are always racing to stay ahead." That's where Trish's superpower comes in: thinking practical compliance with a litigators' paranoia. "When I read a law, I don't just read what it says, I read what it can be made to say," then build compliance from there. Trish keeps close track of regulatory and industry calls and class action litigation to fine-tune her risk evaluations, but stresses that, "The risk calculations are constantly changing."

### ***Approaching Constant Change and the Impact of Litigation***

With so much in flux, Trish finds it helpful to "try and build from what's already in place, but build in a way that recognizes that more change will come." As for what that change will look like, Trish predicts global approaches will continue impacting U.S.-requirements and class action litigation risk will continue placing excessive demands on businesses. The risk of class action litigation is often most economically dealt with by building a compliance program that does more than what the law would require, simply to mitigate litigation demands. "For businesses, that means we sometimes go an extra mile to reduce arguments that we didn't complete the one required mile. It's effectively regulation by threat of baseless litigation." While Trish would love to see courts take a firmer hand in dismissing some claims (privacy-focused as well as those following data breaches), she's not holding her breath: "I hope it happens, but I'm not optimistic – there's too much money in it for plaintiffs' firms. With the incentives being what they are, I think we'll continue seeing aggressive litigation at the expense of our businesses, and ultimately consumers. Usually the biggest winner in a privacy litigation is the plaintiff's lawyer, not the consumer."

### ***Business Development Through Integrity***

For Trish, successful business development is rooted in honesty and a genuine commitment to client needs. "I'm not here to sell something just for the sake of selling it," she explains. Her approach is client-service focused, even if that means recommending a lower-cost solution or delaying a project. Her reputation for integrity has led to a steady stream of referrals and opportunities. Industry conferences, mentors, and networking events, particularly in life insurance privacy issues, have also been valuable sources of new clients.

When asked for advice for young lawyers, Trish emphasizes three principles: "Pursue what interests you, take on hard challenges, and learn to adapt." She acknowledges that her own path wasn't linear but believes that each step brought her closer to her dream role.

## **Certifications and the Role of the IAPP**

Trish sees certifications like the Certified Information Privacy Professional (CIPP) as essential for anyone looking to enter the field. “They’re often a baseline requirement for privacy positions,” she says. She also encourages networking through IAPP, which she credits with helping her recruit talented professionals.

“Certifications show initiative and a serious commitment to privacy law,” she adds. For Trish, the effort required to earn these credentials demonstrates the kind of dedication she values in her team.

## **The Future of Privacy Law**

As privacy law continues to evolve, Trish remains optimistic about its future. She sees increasing demand for legal expertise in privacy, cybersecurity, and AI, driven by rapid technological advancements and new regulations. “The constant change is what makes this field so exciting,” she says. “It challenges us to adapt, innovate, and provide real value to our clients.”

Looking ahead, Trish believes that privacy professionals will play a critical role in shaping how businesses navigate the complexities of data governance. “It’s about building trust and aligning data practices with both legal requirements and shifting risks and expectations”. We are building the future every day.”

**About the Interviewer.** Stephen G. Novosel, JD, M.P.S., is a Certified Information Privacy Professional (CIPP/US) and an advocate for data privacy, cybersecurity, and responsible AI use. An entrepreneur and AI and Zero Knowledge Proof evangelist with a military background, he has been deeply involved in the blockchain and cryptocurrency space since 2017. He previously spent over a decade as a consultant, helping attorneys and members of the Am Law 200 better serve their clients. As the author of this series, Stephen explores the challenges and opportunities of technological transformation in the legal profession. If you are interested in participating in this series, Stephen can be reached at [team@datprivc.com](mailto:team@datprivc.com).



## PRIVACY ISN'T DEAD, IT'S HIRING!

Looking for a job in privacy? Below are some open positions:

- [Junior Associate for Health Care and General Privacy Counseling](#) (Fenwick)
- [Privacy Counsel](#) (Morgan Lewis)
- [Regulatory Counsel, Privacy](#) (Google)
- [Senior Counsel – Privacy & Data Protection](#) (Mastercard)
- [VP & Senior Counsel, Privacy – U.S. Products & Services](#) (American Express)
- [Deputy General Counsel, Chief Privacy Officer](#) (Commonwealth of Massachusetts)

## OPPORTUNITIES: CONNECT AND LEARN!

Below are some great events where you can connect with other privacy professionals and learn about emerging topics:

- [2025 Antitrust Data Privacy Conference](#)  
Feb.6 (ABA)
- [Sleeping giant of privacy, security and e-discovery data deletion](#)  
Feb.19 (IAPP)
- [Ethical & Secure File Sharing](#)  
Feb.18 (ABA)

## CONTACT INFORMATION

Do you have a job opening or an event that you'd like to submit to our next newsletter? Have questions about how to get involved? Contact Committee leadership:

1. Elliot Golding – Co-Chair –  
[egolding@mwe.com](mailto:egolding@mwe.com)
2. Donata Stroink-Skillrud – Co-Chair –  
[donata@termageddon.com](mailto:donata@termageddon.com)
3. Paul Lanois – Co-Chair –  
[paulanocom@aol.com](mailto:paulanocom@aol.com)

## GET INVOLVED

Membership in our committee is what you make of it! Check out the areas in which we need help and contact us to get involved.

1. Let us interview you for the monthly member spotlight for a future issue of the newsletter;
2. Volunteer to speak at an CLE or a brown bag session;
3. Draft an article for Jurimetrics or the Sci-Tech Lawyer.

# MEET OUR EDITORS



## **Donata Stroink-Skillrud**

Donata is a data privacy, technology, and contracts attorney practicing law in Chicago, IL. She is the President of Termageddon, LLC, a software company that has generated thousands of Privacy Policies. Donata is also a Certified Information Privacy Professional with a concentration in U.S. Law. She is the Co-Chair of our ePrivacy Committee, member of the Cybersecurity Legal Task Force, and member of the Science and Technology Council. Donata is also the Chair of the Chicago Bar Association's ePrivacy Committee. She often speaks at events on the topic of privacy, educating technology professionals about their obligations.



## **Landon L. McKinney**

Landon is a Certified Privacy Professional for Europe (CIPP/E) and a J.D. Candidate at Suffolk University Law School, where he is Co-Founder & Secretary of Suffolk Law's Data Privacy & Cybersecurity Law Association ("DPCLA"). He was most recently employed as a Law Clerk at Mullen Coughlin, a firm uniquely dedicated exclusively to representing clients facing data privacy events and information security incidents. During his time as a paralegal, Landon supported trial attorneys in federal and state court in all phases of litigation and in all aspects of compliance with the Electronic Communications Privacy Act.