***Regulatory Oversight* Podcast**
**12 Days of Regulatory Insights: Day 8 – How State AGs Are Rewriting Social Media Rules**
**Speakers: Ashley Taylor and Ron Raether**
**Aired: December 15, 2025**

**Ashley Taylor (00:04):**

Welcome back to the special holiday edition of our *Regulatory Oversight* podcast series, the 12 Days of Regulatory Insights. This 12 episode series is focused on key highlights and trends from the past year in various areas and desire to keep our listeners informed and engaged during the holiday season. Before we get started today, I wanted to remind all of our listeners to visit and subscribe to our blog at RegulatoryOversight.com so you can stay up to date on developments and changes in the regulatory landscape. I'm Ashley Taylor, partner and co-leader of our state AG team, and today I'm joined by Ron Raether to discuss the regulatory landscape of emerging trends in social media consumer protection, and how state investigations and litigation are defining the regulatory landscape. Ron leads the firm's privacy and cyber team and brings nearly 30 years of experience advising companies on privacy, security, data governance and risk mitigation. He counsels clients on data monetization, targeted advertising, and the use of algorithmic tools and regularly addresses product design and user experience, children and teen privacy biometrics and content moderation issues. Ron, thanks for joining me today.

**Ron Raether (01:13):**

Well, thanks Ashley. It's a pleasure to be here with you and your audience. I can't think of where else I'd want to be during the holidays.

**Ashley Taylor (01:21):**

Well, Ron, let's jump right in and talk, if you would with me about state AGs and what they are doing in the social media context.

**Ron Raether (01:31):**

We're seeing a number of trends, and what I'd start off with is where every marketing department begins, and that's with artificial intelligence and AI specifically, what the AGs are focused on is what we call AI washing. So that is a trend by some companies to market and sell, that they have AI or AI functionality within their services or products when actually they dull. And so the AGs are looking at false advertising, UDAP deceptive trade practice claims. They're also going further with respect to ai, and that's actually looking at the predictive analytics and the algorithmic predictions, including algorithmic pricing. So we're seeing instances in which the AGs are exploring both the consumer effect of algorithmic pricing as well as the potential market antitrust implications of the same, and we're engaged in interacting with respect to those issues.

The other thing we see is consent and compliance management programs, specifically with consent management, they're really digging in on transparency and clarity.

So there was the settlement this week or late last week with the California AG gaming app provider where the attorney general was critical of their notice program, finding that it was confusing to a reasonable consumer. So we're seeing more and more AGs question both the clarity and transparency as well as where those consent management practices fit within the consumer flow, the work product flow, and a lot of that we're also seeing in private litigation with respect to tracking technologies. As to compliance programs, generally we see the attorneys generals looking beyond the policies. No longer are they providing companies with the benefits of cure provisions or safe harbors. They're actually now starting to dig into the maturity of the programs, how the products and the companies are actually complying with their privacy policies. Are they testing it? Are they doing audits? So looking beyond just what's on the paper, looking at the maturity level.

**Ashley Taylor (03:51):**

Ron, you mentioned algorithmic pricing, and as most of our listeners will know, state AG matters are often driven by policy concerns. So what are the policy concerns that AGs have been focused on with respect to algorithmic pricing? In some ways, it would seem that they would be pleased that it would be consumer specific pricing, but just talk to us about the policy implications that they seem to be focused on.

**Ron Raether (04:17):**

Well, whether justified or not, the AGs seem to believe that under certain circumstances, algorithmic pricing can artificially inflate the cost of goods or services to consumers. So basic antitrust concepts of price fixing, that obviously depends on both the information that's used for training the models. So for example, is it non-public confidential information that's being exchanged among competitors? In other words, something that's not out in the public domain. And then likewise how the algorithms themselves are functioning and operating. So is it machine learning? Is it a waterfall process? Is it a large language model? And then how that logic flows, how it works, and then likewise, what is the output and what's the ultimate impact on the market? It's important in being prepared for those types of inquiries to be able to answer those baseline questions that each of those areas create. So the source of the information that you're using, making sure you have that down, understanding the logic and the algorithm that's being employed by the software, how it operates, how it functions, what becomes visible, and then what the market effect is.

**Ashley Taylor (05:38):**

So Ron, we've talked about the public policy, and I want to ask you now how state AGs are going about advancing their public policy concerns. Are they using the traditional tools of civil investigative demands and subpoenas, or are they being more creative

**Ron Raether (05:57):**

So they're still continuing using their traditional tools? I think what they've supplemented that with are internal resources that go beyond basic lawyering skills. So understanding the law, understanding policy, investigative skills such as writing docket requests and specifications. They now are employing technologists, so individuals that better understand the technology. But I think more critically for our clients, they're actually deploying and using technologies to do pre discovery, investigate before the investigation to do discovery so that they're more informed when they write the subpoena or the CID. So for example, you or I might use a product like Ghostly to go out and look at a URL for one of our clients to determine what cookies are being are out there, where in the technology or the cookies being presented to our devices, where in that process does the cookie consent appear? We've been using it on the private side. The AGs are starting to use it before they in their pre investigation endeavors. So they're there asking tougher questions that they're certainly more informed as you engage with them. And I think as a consequence, that changes somewhat our approach to them.

**Ashley Taylor (07:20):**

Ron, have you seen any states in particular emerge as leaders in this area?

**Ron Raether (07:26):**

So it is primarily the states that have a data privacy act, and each state is emerging, frankly, depending on their policy, their goals set for that office. And so red states and blue states both have an interest on the privacy side, the technology tracking side, they emphasize often different policies that are more central and important to the politics of that particular state. But we've been interacting a lot with California, Colorado, Oregon, obviously Texas, but really any of the states that have data privacy statutes. We know that Indiana, that statute goes into effect on January 1st, 2026. Ashley, you and I have had interactions with Indiana on data security and other privacy, so we know the activity and how active the Indiana AG can be. So it's really all the above.

**Ashley Taylor (08:25):**

I wonder, Ron, if you could identify for the audience a few of the core focus areas. So I'm going to identify the obvious ones, privacy and data use, but talk about some others that you see states identifying as their core areas of focus.

**Ron Raether (08:42):**

So one thing the states are focused on is the data type. So what is the nature of the information that's being collected? There's a focus on children kid information, so that's COPA or state laws. Again, I mentioned that gaming app settlement recently with the California AG. The company had an age gate for some of its apps, but for not all of its apps. It had an age gate for kids that were 13 or younger, which would be compliant with COPA, but it didn't capture 13 to 16 years old, which is the relevant date range for California and California compliance. The other area we see a lot is health information. So whether that's actually PHI, it's regulated by HIPAA or other

information that could be tagged or seen to be indicators of more sensitive, what most consumers would consider to be more sensitive information. And then the last thing is bias. So depending again on whether it's a blue or red state, they're looking for not just direct indicators of bias, but also more subtle ways in which a product or an algorithm might result in some type of inherent bias within the solution.

**Ashley Taylor (10:05):**

So Ron, I want to take a step back and I want to think about this ad tech ecosystem and there a number of players in this ecosystem, but I want to focus our discussion on one in particular at this point. Data brokers, they seem to have attracted the attention of state AGs. I know a number of states now require them to register. So talk about how states are approaching data brokers practices and the obligations that certain states are placing on them to both register and what this scrutiny means for platforms and app developers that rely on the broker data.

**Ron Raether (10:39):**

And if anybody's really interested in hearing more about my opinions on data brokers, you can go to my LinkedIn page. I do believe that at the moment, data brokers is a term that's been over applied, and I think likewise has been given a derogatory meaning even when it shouldn't be. And that's sort of what's driving the AGs and the states data brokers becomes a generalized easy target, but there's obviously a lot more complication involved when you start to dig into the details. I think with respect to data brokers, the state legislatures and the AGs have concluded that because of the volume of data that they're receiving as well, as well as where they might sit in the data ecosystem, that they require additional regulation. The CPPA in California recently created an enforcement strike force to go after data brokers. We're going to likely see a similar focus on that particular market segment going forward.

I think it's critical, however, as we think about data brokers to help companies answer some simple questions like are you a data broker or not? It may seem like a simplistic question, but as you start to dig into the details, when you look at the definitions, when you look at how most companies engage in data collection and distribution practices, it's not as simple as it may seem. The other things are more practical, right? We have clients that intend to comply with the laws, but if you look at the delete act for example in California, what does it mean to actually delete information? Again, I think most people that are not tech savvy think, well, you just push a button and it goes away forever. But in reality, it's a much more complicated question, especially if you're in a regulated industry or there are other reasons for why that data needs to be kept simply by creating a right to delete and then suggesting that a data broker ought to be held responsible or reliable when there might be some residual data. There might be technical reasons as well as legal reasons why that information remains retained. So there's going to be a great need for discussion at a policy level as well as a practical level with the attorneys general. And I think it provides a ripe opportunity to have a constructive conversation as to have it achieve the proper balance between expectation of privacy while still allowing commerce to flow effectively.

**Ashley Taylor (13:13):**

So around all of our listeners operate in the business world and they have to make day-to-day decisions in the context of all of these, in many cases, conflicting regulatory obligations, and they're anticipating what the regulator will think about something in the future, even when the regulator may not fully understand the technology. So want to end today's podcast with a question. If a company approaches you and says, help me develop a playbook today, give me three concrete steps, you would advise that company to take with respect to social platforms to ensure that they have taken into consideration the patchwork of state laws.

**Ron Raether (13:59):**

So the first would be, this is the old Boy Scout motto. Be prepared. I think a lot of companies don't look at privacy, cybersecurity compliance as an area that requires any real attention, realizing that it's a cost center, but also you have to acknowledge that the regulators, and even in private litigation, they're becoming more sophisticated, more nuanced in terms of what they're expecting. I mentioned earlier about the maturity model. A lot of organizations have privacy policies on paper, but they're not actually implemented in practice. I mean, that gaming app settlement in California is a perfect example of that. So there wasn't the right individuals involved, there wasn't the right testing, auditing to make sure they had a mature compliant model. We do tabletop for data breach and incident response. Why not do tabletops to make sure that your privacy compliance program can stand the tennis of what the regulators are likely to come in and push in pull.

And this includes that technologist issue that I was talking about earlier, deploying some of those tools that we use, being proactive in running those tools against your environment to see what the regulators might be saying. The second thing would be you have to do more with less. I understand that concept, but with the resources that you have to be able to dedicate, make sure that they're applying in areas that provide the greatest RO. I think a lot of times companies are looking at compliance programs out of the box as opposed to really customizing them towards their business operations and really the sensitivities that those operations are likely to garner attention from the regulators and others. The last thing I would say is when a regulator comes knocking, or even better, if you determine that there's an issue and you made the cost benefit analysis and determined that you should reach out to an AG, you should do that.

I wouldn't wait for the AG to find something, be proactive. Ashley and I, you and I have done that with the AGs that's in the home state of where our clients are located. Having that conversation upfront, allowing them to be involved in the solution, but importantly, do damage control with the other AGs and other states becomes critical. And then importantly, dawn off skate during the investigation. Don't pretend like the AG isn't as educated or as knowledgeable about your business. I think that's changing. It's better to have a candid, open conversation that allows you to work towards a mutually beneficial solution.

**Ashley Taylor (16:42):**

So Ron, your comments actually brought to mind what will be now my final question for our listeners who are focused on compliance in particular, is there a key metric you would highlight for them that you deem to be important?

**Ron Raether (17:00):**

So what I would say is do what you say, and it sounds simple, but I think it's easy to write a policy or put a program in place so that if you have to sell your company or you're engaged in due diligence or for a variety of other audiences, you can point to and say, I have a program, or I have a compliance process in place. But you need to test that. You need to include the right personnel that are kicking the tires and making sure that you're actually engaging in conduct that's consistent with your policies. And I think that's where many companies have shortcomings and fail. And it sounds simple to say. It can be complicated, especially where you have a company that has multiple offerings, you're going through acquisitions, you're bringing in new technologies, things are constantly changing when it comes to technology, but being operationally effective as well as administratively effective in compliance becomes a key to long-term success.

**Ashley Taylor (18:12):**

Well, Ron, I want to thank you for joining us today, and I know our listeners appreciated hearing your expertise in this area, and I appreciate you taking the time to join me on our podcast today. Also, want to thank our audience for tuning into this special holiday series. Tune in for our next episode as we continue our 12 Days of Regulatory Insights series. And please make sure to subscribe to this podcast via Apple Podcast, Google Play, Stitcher, or whatever platform you use, and we look forward to seeing you the next time.