The Consumer Finance Podcast – State AGs Unite: New Privacy Task Force Signals Shift in Regulatory Power Dynamics
Host: Chris Willis
Guests: Kim Phan, Stephen C. Piepgrass
Date Aired: May 15, 2025

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper Locke's Consumer Financial Services Regulatory Practice. Today, we're going to be talking about a new joint privacy task force formed by a number of state AGs here in the United States. Before we jump into that topic, let me remind you to visit and subscribe to our blogs, TroutmanFinancialServices.com and ConsumerFinancialServicesLawMonitor.com.

And don't forget about all of the other great podcasts we have. The *FCRA Focus*, *The Crypto Exchange*, *Unauthorized Access*, which is our privacy and data security podcast, *Payments Pros*, and of course, *Moving the Metal*. All of those are available on all popular podcast platforms. Speaking of those platforms, if you like this podcast, let us know. Leave us a review on your podcast platform of choice and tell us know how we're doing.

Now, as I said today, we're going to be talking about a continuing theme that I think we've been experiencing and talking about ever since the election and particularly the administration change, which is the rise in assertiveness and presence of state regulators in areas that matter to financial services companies. Today is no exception to that, because recently, there were a number of state AGs who decided to form a joint privacy task force. Joining me to talk about that are two of my partners, Kim Phan, who's a partner in our privacy and cyber practice group, and Stephen Piepgrass, who's the practice group leader of our RISE group, which stands for Regulatory Investigation Strategy and Enforcement. That's the group within our firm that has our nationally renowned state AG practice in it. Kim, Stephen, thanks for joining me to talk about this today.

Kim Phan:

Thank you for having us.

Stephen Piepgrass:

Great to be with you.

Chris Willis:

Kim, let's start with you. Tell the audience what's happened here. What state AGs did what and what have they said they're going to do?

Kim Phan:

In April, a group of state regulators formed what they're calling the Consortium of Privacy Regulators. These regulators got together and they signed a memorandum of understanding, an MOU. It outlines certain shared goals that they want to have with regard to their state-coordinated privacy enforcement efforts. They want to have regular meetings to share their enforcement priorities and coordinate their investigations. They are looking to leverage technical and legal expertise across jurisdictions, so they don't have to build an entire team, each in their own individual states. They want to align their enforcement priorities, specifically around consumer harm. Things like the exercising of privacy rights, like the right to access or know, as it's often called, the right to delete, and some of the opt out rights with regard to things sales of consumer data.

The regulators that we're talking about are two California entities, the California Privacy Protection Agency and the California Attorney General, as well as attorneys general in Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon, and notably absent is Texas, who I think many of us have recognized as an emerging player in the area of privacy enforcement.

Chris Willis:

Stephen, a couple of notable things that I heard there from Kim. First of all, we have a Consortium of Privacy Regulators, and there aren't any federal regulators in the mix. Give me your impressions about that and what it means in terms of state capabilities and coordination in this area.

Stephen Piepgrass:

Yeah, great observation, Chris. Something I noted, too, as I was reading about this new consortium, interestingly, the FCC had actually pulled together a group of states in December of 2023. Then in October of 2024, announced additional states, joining what they were calling at the time, a joint task force, where they had a memorandum of understanding with those states, all looking at privacy issues, but really convened under the auspices of the FCC, working with all of these different state AGs.

I think it is no coincidence that at this time, with the advent of the Trump administration and the pullback at the federal level of multiple different agencies, that here we're seeing the announcement of a brand-new task force, this time made up of just state actors. That indicates to me that what we have seen happening at the federal level with DOGE and with the, in some ways, gutting of so many of these federal agencies, that the states really are stepping in to fill the gap. Chris, you may, obviously, with your expertise in the financial services space, I'm sure you are seeing this in other areas as well.

Chris Willis:

Yeah, for sure, because there's never been a doubt that there was going to be motivation at the state level to fill the gaps that they perceived to be left by a perception of lax regulatory

enforcement at the federal level. The question is, what practically, from a resource and coordination standpoint, they could and would do? To me, as we heard Kim describe the memorandum of understanding, it's not just that they agreed to have meetings and hold hands and talk about things, but to share resources and share enforcement priorities in a way that would really allow them to replicate the capabilities of some of the federal agencies. To me, I think it's important for the financial services industries to understand there are lots of other areas, like fair lending, or UDAAP, or advertising, or anything like that, where states could similarly decide, “Hey, these are important issues we want to coordinate on,” and form similar task forces like this.

To me, it betrays the fallacy of thinking that because the federal regulators may not be as active, that there won't be a capable regulator on the scene because the states are showing that they have the ability to marshal the resources to do that.

Stephen Piepgrass:

Yeah. Chris, I'll jump in there on that point as well. Those of us who practice in this space know that this happens on a very regular basis with multi-states. In fact, many of the states that are part of this new consortium are the leaders that we see on the executive committees of the multi-states handling major data privacy investigations. We know the assistant AGs and deputy AGs who serve on those executive committees, and I am certain that they are many of the same people who are also part of this consortium. They're used to working together and sharing resources and priorities. This is another way of formalizing that and then bringing, interestingly, that additional CPPA into the mix as well.

One other thing I should say, although I mentioned the FCC, and somewhat of the pullback at the federal level, I do want to emphasize that there is still a very strong role for federal regulators in this space as well. Obviously, the FTC regulates in this space, HHS and its OCR still primary regulators, especially when it comes to cyber incidents and have a real focus on HIPAA issues in particular. Then, of course, the SEC also plays a role. All of those will continue, but there's really no question that the states really are stepping it up.

Kim Phan:

Well, when you talked about those various federal agencies, I was just thinking in my head with, as we know, this emphasis on federal efficiency and trying to cut budgets, what we were seeing before, where we saw this regulatory one-upsmanship amongst the federal regulators, everyone wanted a piece of cybersecurity and privacy. I think we'll see even an increase in that area. It's very much a bipartisan issue, that they can all get aligned and seek federal dollars to bring enforcement in these areas, where other areas like fair lending may fall to the wayside.

Stephen Piepgrass:

That's a great point, Kim. Interestingly, you had mentioned Texas not being a part of this particular consortium. It's not a partisan issue for Texas. Texas is really at the forefront in a lot of ways. It may be a priority issue, as to what their focus is versus what these other states are. Frankly, in many ways, I know the folks at that privacy division very, very well respected in this area. They are a force to be reckoned with independently as well. You're right. This is not a

partisan issue. Different states do have different priorities, but there are different things driving that apart from partisanship.

Chris Willis:

Well, Kim, I think that's a perfect juncture to pivot back to you. I mean, we've talked about the formation of the task force and some of its larger implications, but let's just return back to the subject of privacy, which of course is your core area of expertise. We have a task force. They want to work together, and they've said how they're going to work together. What kinds of specific privacy issues do you think that they will be working on together? What are the hot topics you think that they'll address?

Kim Phan:

I think it's the same areas that we've seen lots of enforcement activity in recently, pronouncement, things of that sort. It's the categories of personal information that we would typically think of as more sensitive. Financial information certainly is included in that, as well as health information, geolocation, biometric data, and certainly, any information that involves, say, a protected group, or what are considered more vulnerable populations—children, veterans, and we're seeing an increase in attempts to protect individuals who have been victims of domestic assault or violence. I think we'll perceive that there's going to be a focus in some of those, again, less controversial, more bipartisan areas where they can get alignment.

Chris Willis:

Kim, based on that and based on those areas of priority, the financial services industry obviously thrives on PII and other sensitive personal information from the standpoint of credit underwriting, from the standpoint of fraud prevention, servicing and collections, and even from the standpoint of marketing. What do you think the takeaways are from an industry standpoint in our industry, financial services, from the advent of this task force and what it may be doing?

Kim Phan:

Well, I have to say, as a financial privacy lawyer of almost 20 years, these are very exciting times, though I am sympathetic to the many companies who are trying to navigate these evolving waters. But I think there's also a very unique education opportunity right now. The technical requirements to perform a data mapping exercise, where you're assessing what your incoming sources of data are, what your internal enterprise uses of that data are, what external third parties you're sharing with. Not only can that be a valuable resource to business teams within a company, it also serves as an incredible resource to help provide education about the complexity of the financial ecosystem to what are typically very under-resourced, under-staffed state agencies and enforcement offices. I think if companies think about it, it could be an opportunity, though I think also, there's a lot of potential for threat here.

Chris Willis:

Thanks for that, synopsis, Kim. Stephen, one of the things that I wanted to ask you about is, you had mentioned the previous task force that had been organized by the FCC, and now we have this new one independent of any federal regulator. Do you see any difference in the types of issues that the states are focused on now versus what they have been in the past?

Stephen Piepgrass:

Yes, so apart from the states that are involved, and there was significant overlap between these two groups, but to me, one of the biggest distinctions is when the FCC set up that task force back in 2023, and then when they were talking about it again in 2024, the focus of that task force, the primary focus was really cybersecurity issues, fraud, data breaches, that sort of thing. The focus of this privacy consortium, when you read what the states are saying about it, the focus really is about data, and what happens to the data. For that reason, I think companies that deal in data need to pay very close attention to what this consortium is doing. Kim, you may have some thoughts on that, because I know that had advised businesses in this area on a regular basis.

Kim Phan:

Yeah. Data security has been very much taking up all the air in the room for a long time, right? With large-scale data breaches that we're all very familiar with. Many companies have very robust and mature cybersecurity programs, where they are performing assessments, they're doing vulnerability scans, they have SOC 2 audits. There's a very established regime around what the expectations are in the area of data security.

Data privacy is very much taking the world by storm right now. Really, that shift happened when the European Union General Data Protection Regulation went into effect back in 2020. This is really something that has evolved in just the last five years, where the focus is shifting away from, how do you protect the data to where did you get that data, how are you using that data, and who are you giving that data to? It is figuring out that and being able to explain that to state regulators is where I think companies should be devoting a lot of time right now.

Chris Willis:

Well, and Kim, it's funny that you and Stephen are talking about the use and distribution of data, because one of the biggest headlines of the CFPB towards the tail end of the last administration was the CFPB's effort to use the Fair Credit Reporting Act to get at what they termed “data brokers,” which is the same entities that both of you have just been talking about. It strikes me that there were so many efforts by the CFPB to educate and inspire state regulators to go after a whole laundry list of issues. The CFPB even published a playbook for states, not only for regulatory actions, but also for legislative measures. This strikes me as another example of where the states might be interested in picking up where the CFPB left off under Rohit Chopra with dealing with data brokers.

Kim Phan:

It's possible, Chris. There's about five states right now that have enacted data broker legislation, California being one of them, and they have been very robust in their enforcement of entities they believe should have registered under their data broker registry and have made appropriate fines and penalties for failure to do so.

One thing that I would distinguish on the state level that is different from what the CFPB was trying to do, the state data broker laws are very much focused on third-party entities, entities that don't have a direct consumer relationship, but basically, deal in buying and selling data. The CFPB had expanded that in their proposed regulations, where they had wanted to include entities, any entity, including their first-party data that engaged in sales of that data's third parties.

I don't know that that particular rulemaking had advanced far enough for the states to pick that up, but it's possible, certainly, that a group of this type could look at that and think about putting together a model law that other states could decide to implement.

Chris Willis:

Kim, you've been talking about some of the priorities of the state regulators. Do we have any insight into what they're actually talking about and thinking about here in the present moment to give us a further clue about their priorities?

Kim Phan:

I have the opportunity to attend the International Association of Privacy Professionals Global Privacy Summit in Washington, D.C., a couple of weeks ago, and they had a number of these state regulators attend and speak on various panels, which gave a little bit more insight than just the press release on what they're planning. The California Privacy Protection Agency Deputy Director of Enforcement, Michael Macko, specifically said that he's hoping not only for this consortium to meet on a periodic basis, but also, for targeted check-ins whenever a specific issue might arise on the state level. He even mentioned how they might pursue investigation, potential prosecution violations, that there is a lot of steps in between, and that an investigation could involve multiple alleged violations, but any prosecution would hone in on a few of them to, according to him, maximize a remedy with a subset rather than the whole spectrum of potential violations.

Connecticut Deputy Associate Attorney General, Michele Lucan, actually characterized the consortium as a benefit for companies to deal with a group of regulators, versus answering individual complaints from multiple sources. And Oregon Senior Assistant Attorney General, Kristen Hilton, noted that specifically for Oregon's purposes, they may or may not pursue some of the same types of claims that the other more aggressive state regulators are pursuing and that their emphasis in Oregon at this stage is simply education and outreach, especially since the Oregon privacy law currently has a cure period in place until January 1st of 2026.

Right now, they're working with companies to get them in line before they start thinking about any enforcement action, even when they do pursue enforcement, it would most likely be only for facial violations of the law. They're not looking to take up creative theories of violations.

Chris Willis:

That's very interesting. Well, let me, Kim, give you the last word on the podcast. We have this new consortium of AGs and other state regulators. We know the kinds of issues that they're going to be active on and how it's different from the past based on what Stephen told us. What's the takeaway for industry? What should we be doing from a compliance, policy, contracting standpoint in light of the fact that we have this new consortium on the beat now?

Kim Phan:

Companies really should be thinking about how they address privacy in a holistic way. They needed to devote the same type of resources and staff to privacy that they did a few years ago when they were thinking about making robust cybersecurity programs. They need folks who are dedicated to privacy to be thinking about how to comply with all of these various obligations in the multiple states, because any one of them could potentially trigger an investigation.

Once they have those staff and resources, they need to be focused on things that are, let's say, the lowest hanging fruit, right? Carefully reviewing privacy policies. That's the most public facing statement about what a company is doing with regard to data, making sure that it is accurately describing what the company is doing, having robust processes to respond to consumer complaints, inquiries, privacy requests, because it's so easy for a consumer to go running to Attorney General with a complaint. And as we know, many enforcement actions are going to be driven by the number of consumer complaints that are filed against them. So, little things like that, just doing some basic cleanup to make sure they're presenting a privacy protective front, while also building out many of these processes need to happen in the backend in order to honor many of these new very technical requirements.

Chris Willis:

Okay, that makes good sense, and it's great advice to industry. Kim, thank you for joining us today to share that insight. Stephen, thanks to you as well for sharing your insight about the activity of the state AGs, which of course, I know you and your colleagues in our RISE group do very intently all the time. Of course, thanks to our listeners for tuning into today's episode as well. Don't forget to visit and subscribe to our blogs, TroutmanFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. While you're at it, why not visit us on the web at troutman.com and add yourself to our consumer financial services email list. That way, we can send you copies of the alerts and advisories that we send from time to time, as well as the industry only webinars that we put on at times throughout the year. Of course, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.