***The Consumer Finance Podcast*: Navigating Emerging Privacy Issues in Financial Services**
Host: Chris Willis
Guests: Rami Haddad of PRA Group and Kim Phan of Troutman Pepper
Date Aired: September 5, 2024

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper's Consumer Financial Services Regulatory Practice. Today, we're going to be talking about a grabbag of interesting and emerging privacy related issues that are of concern to the financial services industry, with a special guest.

Before we jump into that topic and I introduce our special guest, let me remind you to visit and subscribe to our blogs, TroutmanPepperFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. Don't forget about our other podcasts, we have lots of them. We have the *FCRA Focus*, all about credit reporting. *Unauthorized Access*, which is our privacy and data security podcast. *The Crypto Exchange*, about everything crypto. *Payments Pros*, which is all about the payments industry. And our newest podcast, *Moving the Metal*, all about the auto finance industry. All of those podcasts 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 let us know how we're doing. If you enjoy reading our blogs and listening to our podcast, our mobile app is a great way to do it. Just go in to your app store, either iOS or Android, and search for Troutman Pepper. There, you'll find our mobile app that gives you reading access to all of our alerts, and advisories, and blogs, as well as listen access to all of our podcasts all in one place. It even has a great directory of all our financial services lawyers. You can call and email us from right inside the app, so please check it out.

Now, as I said today, we're going to be talking about a variety of emerging and interesting privacy issues. To do that, I'm joined by two guests. First, there's my partner, Kim Phan, who's one of our privacy experts and also one of the hosts of our *FCRA Focus* podcast. I'm very glad to have her here, and glad to have been practicing with her for many years. But we also have a very special outside guest, which is Rami Haddad. Rami is the Deputy General Counsel for regulatory compliance, data privacy and litigation at PRA Group, and we're really glad that he's joining us here today. So, Kim, Rami, welcome to the podcast, and thanks for being here.

Kim Phan:

Chris, it's always a pleasure to join you on the podcast.

Rami Haddad:

Yes. Thank you for having me. We really appreciate it.

Chris Willis:

So, let's dive into some of the sort of interesting goings on that are sort of privacy related that have been happening. Because I like to hear both of your take on what the areas of concern are. Let's start with state privacy laws, which seems like sort of an ever-proliferating group of laws. Because there were a couple at first, and now I feel like there's more and more being enacted. Let's just talk basically about the scope of coverage of these laws. Do they even apply to financial institutions and financial services companies? Let's start with that.

Kim Phan:

The reality is that, the Gramm-Leach-Bliley Act, which is the federal financial privacy law is incredibly useful in that many of the states have recognized, if there is an existing privacy regime that is protecting consumers in this space, then there's no need to add additional privacy requirements on those entities. So, for many financial institutions across the vast majority of these states, there is a wholesale entity level exemption for financial institutions that are subject to the GLBA.

Now, there are a couple of states that have nuances with regard to the scope of the GLBA exemption, and that they are limited to a data level exemption, that's what they're called. Such that the exemption only attaches to the data to the extent it's being collected, used, stored, or otherwise disclosed in ways that are otherwise regulated by the GLBA. Outside of that, you're going to still have to comply with the state privacy law. Typically, that comes into play for things like marketing activity. There's really only three states that financial institutions have to worry about. It's California, Oregon, and Minnesota. But I know Rami has some thoughts about states like Oregon, where the threshold might not even be reached for many financial institutions.

Chris Willis:

Rami, go ahead. I'd love to hear what you think about that.

Rami Haddad:

Thanks, Chris. Kim is absolutely correct. We've seen a proliferation of enactments in the state privacy legislation. We have 19 states to date, three that don't have the wholesale GLBA exemption at the entity level of California, Oregon, and Minnesota. Last, Minnesota is interesting. The question is always the scope, right? Does it apply? If it's not an entity level exemption, and it's a data level exemption, then the question becomes, "Well, what do we do with that? What data is non-GLBA that would be subject to the rule that would otherwise be required for us to comply with that?

So, interestingly enough, unlike California, Oregon and Minnesota don't have a revenue threshold. The question becomes as to whether or not you control or process the personal data of 100,000 or more consumers in that state. Then, that question, in turn, turns on whether or not that data is outside of GLBA. Is it sold, processed, or disclosed pursuant to GLBA, and if it isn't. The question is, what data is that? So, if all the data that your processing is subject to GLBA, then what's left? Some of the questions that could come about from that is, do people visiting our website that don't log into our website, potentially, and that we don't know our consumers, and therefore subject to GLBA. Is that personal data that we control or process.

The scope is incredibly important, and how you get there, that's the analysis that needs to be done at any level. I'll turn it back to Kim to see if you have any thoughts on the threshold and the scoping.

Kim Phan:

Yes. For California, specifically, most companies are going to get pulled in, because California is the only state that really has a revenue threshold. If you have revenue of $25 million or more worldwide, it's not specific to your revenue in California, and you have information about even one California resident, then you're going to be required to comply with all of the bells and whistles that come with the CCPA.

But Rami, you raise a great point. Oregon could easily just be scoped out, because really, how much business is anyone really doing in Oregon? If you have 100,000 or more consumers in Oregon, certainly, you would still need to comply, but that's an important threshold question to ask yourself. But even if you're not, does it make sense to comply with Oregon regardless, and have a comprehensive privacy program that is uniform across the country? I think as more and more states enact comprehensive privacy law becomes more reasonable for a company to just have a wholesale privacy enterprise-wide program, rather than trying to build out nuanced programs for each individual state.

Rami Haddad:

I totally agree. So, that gets into the question of that probably every person or every in-house privacy attorney, if you have them, or in-house counsel is grappling with across the patchwork of legislation that's come out of the privacy in states. Which is, okay, how do we comply with this piecemeal legislation? How do we comply with all these requirements? I mean, take Minnesota, for example. In Minnesota, there's a data privacy protection assessment requirement. So, if you're engaged in certain processing activities, of course, which is unlike other states. So then, the question becomes, well, if we scope out a comprehensive framework, do we then not need to add all the other nuances? How do we do that? How do we layer new laws on top of the existing laws that we've already complied with, as these new laws come out?

So, I guess a primary analysis is, well, does it apply? And if it does, what else do we need to do that we haven't done already? How do we go about that? How do we layer the additional obligations when new laws come out?

Kim Phan:

Chris, as you can see, you've opened a can of worms on that one. There's no single approach, I guess that has really emerged on how businesses want to approach this. It is still a very new. California's CCPA only came out in 2018, and as you noted, we are now seeing states enact these at a much faster pace. We're up to 20 now. So, how companies are going to address this? It's still very much an open question.

Chris Willis:

Yes. You know, Kim, of course, we love a good can of worms here on *The Consumer Finance Podcast*. So, thank you for noting that. Let me shift gears with the two of you for a minute and talk about artificial intelligence. Now, this is one of the most popular things for the media like to talk about, and politicians like to talk about, and regulators talk about it. But recently, three months ago, Colorado became the first state to enact AI legislation, which I want to talk about in a minute. But let's first back up one more step on the state privacy laws. Some of these state privacy laws, the 20 that you mentioned, Kim, do you address things like profiling and automation? Is that AI or is that something we should think of separately under these privacy statutes?

Kim Phan:

No, the problem is that there's no great definition right now of what should or should not be considered artificial intelligence. Colorado, the state that we're going to talk about in a little bit more detail, their definition of AI was so controversial when they were enacting this legislation. They actually had to amend the bill during the legislative process to clarify, that when we talk about artificial intelligence, we do not mean calculators. So, your TI 85 graphing calculator back from high school, don't worry, it is not artificial intelligence. But it raises the issue that, if you have to clarify that calculators are not intended to be your definition of artificial intelligence, maybe your definition is too broad. So, we're seeing that there's this struggle, the idea of our basic algorithms that the industry has been using for years, is that artificial intelligence? Is the type of credit profiles that consumer reporting agencies have been conducting over the last 50 years under the FCRA, is that going to be considered artificial intelligence?

There's a lot of concern about the overlap of what they are pulling into these artificial intelligence proposals with existing laws like GLBA, FCRA, and others that I don't think have been resolved yet in any of the proposals so far, and certainly not in the Colorado Act.

Rami Haddad:

I would agree with Kim. I think that's one of the most difficult aspects of what legislators are trying to grapple with, which is, how do you define AI? The words artificial intelligence become ubiquitous since ChatGPT came online. Now. it's become an issue of, "Well, what is and what isn't, and how broad do we define it?" I mean the EU AI Act, which just came into effect, which Colorado borrows heavily from very broad definitions of what AI could be. But yet, we do see those little exemptions about, well, it's not your graphic calculator. Well, if you had to go out of your way to say that, then perhaps it is too broad. So, what does that encapsulate? That's the difficulty.

I think on the state side, California, Virginia, Colorado, Connecticut have addressed automated decision making. If you look at the def – California hasn't enacted it yet, the regulations are still pending on ADM or automated decision making. But if you look at the proposed draft regulation on how that's defined, I would say, it does. It does include artificial intelligence, type algorithms, machine learning. You could easily back into AI through these privacy regulations. So, we have to be careful, because then, you also have duplicative laws that are coming out.

Kim Phan:

Yes. The state privacy laws are not great about taking a uniform approach toward this.

Rami Haddad:

Correct.

Kim Phan:

Because we know that the California Privacy Protection Agency, the first and only state agency that's devoted entirely to privacy. California loves reminding everybody about that. They've been working on AI regulations. Well, they have started a formal rulemaking process this summer, they're nowhere close to having actual rules. They have draft rules that they've released for a public review, but it's by no means what's going to be final. Then, you have other states like Oregon and Minnesota that address things like profiling. Some of those requirements are quite onerous in the state privacy laws. With regard to having to disclose to consumers that that profiling is even occurring, what information is being used to feed that profile. Giving consumers rights to access the data that was used to make a decision in a particular profiling case, and requiring a reevaluation of the decision used in that profiling if there are any corrections that needed to be made to the underlying personal information that led to that decision.

All of that is not even close to what the Colorado AI Act is, but we're already seeing that even in these disparate state privacy laws, we're seeing very strange variations come up that could touch on artificial intelligence.

Chris Willis:

All right. We've talked a little bit about the Colorado law, but I want to just jump straight into it and ask both of you a question. I've read the law and I've heard all about it. It's the first law of its kind, passed by any state in the country, but it might serve as the model or impetus for other states to do something similar. Tell the audience a little bit about the Colorado AI law, what it requires and who it covers, and specifically, does it apply to financial services companies?

Rami Haddad:

Sure. I could start. Absolutely applies to financial services companies. It actually applies to any. It defines it as person, but then person is defined in the act. So, it's corporation, business, partnership, so on. So, if you're doing business in Colorado and you develop or deploy what's defined as high-risk AI systems, you're going to be covered under the law. So then, the question becomes from there, if you're covered, are you deploying or developing? Are you a deployer or developer? There's different obligations.

Are you involved in doing so with respect to high-risk AI system? As that's defined under the law, because the law is really aimed at two things. It's automated decision making, as we said, but really targeted at prohibiting algorithmic discrimination. That's one of the real catalysts behind the law, was to prohibit that. We've seen regulatory bulletins and commentary about that from the CFPB and so forth about the laws apply to you, and they're agnostic as to what methods you use to develop your models. You still have to comply with the law at the end of the day. It doesn't matter if you use AI to do it or not.

The real issue comes down to the way the law is framed, both in the definition of, like we just talked about, which is AI system, which is broad. But also, the fact that it has to be used or deployed as a substantial factor in making a consequential decision. Now, we get into two more definitions. What is the substantial factor? Is it a consequential decision? That's really where I think the analysis has to come in, whether it's – if you think about the consequential decision, it's defined as what has a material, legal, or similarly significant effect on the provision or denial, or the cost or terms. So, those are the main things. Provision or denial, cost or terms. But then it goes on to talk about in what context. It's education, enrollment, employment, financial or lending, and essential government services, healthcare, housing, insurance, or legal. None of those are defined, I think, other than I believe, healthcare.

So, what is financial? What is lending? In our case, that's pretty broad. So, if it's not defined, and you're engaged in what could be construed as financial or lending, and you deploy this high-risk AI, and it has a substantial factor in playing provision or denial, or cost or terms, you're going to be in scope for the law, and it is pretty onerous. There's a lot of requirements. Many of which are the disclosure requirements that you have to provide. Also, we said, first of their kind, which is you have to tell the consumer that you're using this high-risk AI system.

Chris Willis:

Yes. Let's talk a little bit more about the requirements of the Colorado statute. You mentioned Rami, the disclosure requirements. My recollection is that there are disclosure requirements by a developer to a deployer. So the deployer can then make disclosures, both generally to the public as well as to specific consumers who are impacted by one of these high-risk decisions, as you've just defined it, in the act. So, there's that. But then, there's also another sort of more substantive directive in the Act about bias and discrimination. Kim, do you want to tell me about that?

Kim Phan:

The layers of disclosure that are required by the Colorado Act are where I think is most of the burden. So, you have developers of AI, you have the deployers of AI, you have the subjects of AI, then you have the attorney general who is mixed up in all of this So, developers have to provide disclosures to deployers. Deployers have to provide disclosures to consumers. Developers and employers have to provide information to the attorney general. So, if the Attorney general wants to step in, the attorney general has the information needed to do so. All of this, I think I went through the law, and there was 10 different notices or disclosures to different entities within different steps of the AI decision-making process is really quite burdensome.

While there is some language that says you don't have to reveal trade secret information, but if you're explaining how your AI works, here's the data sets that are the basis for it. Here's the reasoning and logic behind how the AI makes a decision making. Here's the results that you can expect. If you're laying all of that out on something that you've internally developed, how is that not trade secret information that they're asking you to hand over into the public space with regard to what you're trying to do. So, I find it very, very document heavy, the obligations that are being laid out by the Colorado AI act that I think won't be beneficial to industry. I don't know that it will add additional protections to consumers. So, I don't know what it's actually achieving. But again, I think, as you noted, Chris, could potentially be the framework that other states follow, which I think is very troubling.

Chris Willis:

Kim, these disclosure requirements to consumers, there are these general public disclosures of like, I'm using an AI decision-making tool, and here's how it works, like you were just talking about. But there's also this requirement of disclosure to a specific consumer whose transaction is impacted by the use of AI. Notably, in the financial services industry, we're used to adverse action notices. We give somebody a notice if they're decline for credit or they don't get the terms that they applied for. But if we say yes to them, we don't give them a disclosure. We just say yes. This statute seems to impose that notification obligation, whether the answer is yes or no, right?

Kim Phan:

That's correct. So, you have a frontend notification to the consumer saying, "We are planning to use AI, and here's all the information about the AI we might use." Then, there's a backend disclosure about, "We did actually use AI, and here's the decision and all the reasoning that went into that decision. So that, if you want to appeal our decision, we can." The need to impose a process by which a consumer can then appeal and challenge an AI decision. All of the benefits of AI, the efficiency, the efficacy, all that goes away if you didn't have to revert back to a whole process anyway. It would be required regardless of the result. So, it could be a positive result. Yes, you get credit. It could be a negative result. No, you don't get credit. But either way, you have the disclosure obligations. It's not contingent on what the actual result is.

Chris Willis:

Yes. Then, just one last thing I want to highlight for the audience about the Colorado statute is, there's this very undefined duty in the statute that people who develop, and I think it's just developers are required to take steps to avoid or mitigate algorithmic bias or discrimination by the use of the technology. Of course, like I'm a fair lending lawyer, so that is interesting to me in that, what does it mean? Does it mean I'm not going to violate the Equal Credit Opportunity Act and I'm going to apply my same old fair lending testing like I've been doing for many years? Or, is there room for somebody to argue that no, this requires something different than compliance with like our specific nondiscrimination statute? Does either of you have a take on that?

Rami Haddad:

I think with respect to discrimination, I think we've seen some that regulators come out and talk about that. When AI started to come on the scene, it become more, like I said, prevalent and ubiquitous in terms of that. With respect to Colorado, I don't know that it's going to be any different than what's going to be required, generally speaking, about what's happening on preventing discrimination and fair lending that we've seen bulletins from other agencies.

In the sense that, if you haven't already, you should start working immediately on an AI governance program internally. You should base it on a certain standard that is recognized, such as NIST potentially or ISO. You need to have that documented, and it needs to be based on some of the overarching tenets, like fairness, and ethics, and transparency, and privacy.

Obviously, if you're deploying certain models versus others, traditional regression models versus new machine learning or black box models, you need to really work with counsel or on debiasing the model to the extent you can. How do you do that? How do you debias the model to really prevent sort of what the general discrimination that could arise under these laws on the new laws if others copy what Colorado has enacted?

Chris Willis:

Okay. Well, I think we've talked enough about the Colorado statute, although we could probably enjoy ourselves doing that for a little longer. But there's a couple more topics I'd like to ask the two of you about. Let's move to the subject of online tracking technologies. So, let me ask the two of you to address first, in private litigation, how are plaintiffs effectively applying CIPA and other state surveillance laws to online tracking technologies, cookies, and pixels, and things like that.

Kim Phan:

So, this type of litigation is one of my little pet peeves. I do not understand how this type of litigation continues. It seems illogical to me that you can apply what are essentially very archaic laws to modern technology. For example, some of the wiretapping laws that were intended for, back when people had a physical wire between their landline phone to another third party, and someone could listen in on their calls. Well, it's the Internet, so there is no wire that is being tapped. So, how does that even apply?

Even in the cases where you could argue that there is a physical connection to the Internet, an ethernet cord, or something along those lines. Most of the entities that are being alleged as the third parties listening into these conversations are actually third-party service providers, agents of the financial institution, Google Analytics, or one of the other session replay companies that are hired by the financial institution to listen into these communications. That's what the argument, that when someone browses your Internet and they click on different things, that's a communication as to what they're interested in, and it becomes a conversation.

So, anyone listening in on that conversation is treated as a third party, which is fine. But again, if they're the agent of the bank or other financial institution, it's for the bank's benefit. So, these arguments drive me crazy, but we are seeing that they are having some success, mainly in California, but we're seeing this spread across the country, Florida, New York, Pennsylvania, even others. They are at least surviving Motions to Dismiss. Many of these cases are making it all the way through, they settle. It would be great to have some more case law that illuminates on how these laws are applicable today, but we're still very early in this process. This litigation is only a couple years old.

Chris Willis:

So, Rami, from the in-house perspective, should companies be doing things like conducting cookie audits or taking other proactive measures with respect to these kinds of tracking technologies?

Rami Haddad:

Absolutely. I agree with Kim. It's very frustrating to see antiquated laws being weaponized in this manner. I mean, we've seen on the federal level, you see the Electronic Communications Privacy Act. But most frustrating, I think we've seen some litigation that has kind of died down recently with respect to the Video Privacy Protection Act, VPPA. Which was, if you look at the law, it was back in the eighties when I think some judge rental records at a video store were disclosed.

Kim Phan:

Robert Bork.

Rami Haddad:

Bork. Thank you, yes. I mean, we're talking about rental records at a video store from the eighties, and here we are, we're seeing it materialize in today's world and the digital age. I mean, the Boston Club case was the great case. So, the meta pixel tracked the user's viewership of the video on the website. So, akin to a rental record, so now your viewership of the video was then tracked, and therefore, without their consent. In any event, the VPPA, it's kind of died down, but the CIPA and other states that have similar sort of wiretapping laws, those are concerning. Because we've seen an inconsistent application by the courts and decisions that have come out, particularly in California. The lawsuits alleging that all these mechanisms that are dropped on the website, cookies, pixels, web beacons that are akin to pen registers, or trap and trace devices.

But if you are in-house and you have a marketing or strategy team, whoever's in charge of your web development or marketing, highly, strongly recommend that they work closely with legal and compliance. The last thing you want to avoid is some marketing or web development, potentially dropping a tracking mechanism, or beacon, or pixel on a website, and you don't know about it, or inadvertently, at least. Somehow, you fall trapped to one of these CIPA claims or VPPA claims inadvertently, because you didn't know. So, you should scan the website on a regular basis for sure.

Chris Willis:

Okay. Thanks for that. Let me hit one more topic with the two of you before we wrap up. That's just to sort of round up where we are on cybersecurity. So, I know Kim that the Federal Trade Commission recently updated the Gramm-Leach-Bliley Act safeguards rule. Are there any highlights or pain points relating to that updated rule that you'd like to share with the audience?

Kim Phan:

It actually was probably a long time in coming and a bit overdue. The GLBA safeguards rule hadn't been updated in 20 years, so it probably was time. But I think the FTC has implemented a very onerous process in ways that it probably didn't need to. It cripped pretty heavily from the New York Department of Financial Services, Cybersecurity Regulations, and the National Association of Insurance Commissioners Model law. It picked bits and pieces from both of those, and have put into place a process that is very prescriptive. The old safeguards rule was very much flexible in approach, like, do what makes sense for your organization based on the types of products that you make available to consumers, and the number and type of consumers that whose data you have.

So, it's very much built around the idea that whatever your risks are, you would appropriately address them. Now, it's very much, you have to have encryption, you have to have multi-factor authentication, you have to have a data inventory, you have to have a disposal policy that's being regularly updated, you have to have change management and training. It is very, very much a checklist of the things they are expecting you to have. For certain financial institutions, that can be problematic.

I think, a major pain point we're seeing for many financial institutions that have to now comply with this is certainly with regard to legacy systems, older systems that it's harder to update for some of these more modern expectations. While many companies were already working on shifting data away from legacy systems to more modern systems, it's just a lot. It can take a long time. That's the reality of the technology. Being able to do so on the FTCs timeline can be challenging.

Chris Willis:

Rami, what's your perspective on this coming from in-house? Kim talked about some of the pain points on implementation. What's your view on that?

Rami Haddad:

Yes, absolutely. I think we went from – and not without probably good reason. From the FTC standpoint, it's probably a long-time coming in. The fact that the older version of the safeguards rule was kind of, suffice to say, kind of squishy. It was kind of, do what makes sense, but very vague, general language. Technical, administrative, procedural safeguards. Then, you're left up to your own devices. Whereas, now, we have more of a blueprint. You need to follow this blueprint, encryption at rest, transit, so on and so forth.

I think the modern consumer is going to get accustomed to that, and I think they already have. If you're dealing with a financial institution as a consumer, you go to a bank, you're accustomed to now to getting MFA, you're accustomed to getting that security email or that text message. Probably not without good reason. I mean, threat actors have become more sophisticated. If you think back about how we got here in the first place, the reason for the breach laws that started out at the state level going into the conversation around privacy, and why we have now privacy laws. It you look back at a history of data breaches, significant ones that have happened over time, and that are concerning, and that sort of reduce the trust that people have in financial institutions and other institutions by safeguarding their personal information.

So yes, they were onerous, I would agree. There was some flexibility left in the rule about how to enact some of these, especially with respect to legacy systems. But if you're trying to comply with these, there's going to be cost, cost of compliance, and that's just cost of doing business.

Kim Phan:

One other thing I wanted to point out about the GLBA safeguards rule is the new update, the latest final rule that was announced earlier this year with regard to data breach notification to the FTC. I found increasingly that companies find it very challenging, the reality that that breach notification requirement is triggered by any nonpublic personal information, being subject to unauthorized access if it impacts over 500 consumers or customers.

The reality is nonpublic personal information is an incredibly broad term. It applies to pretty much everything that gathered with regard to the provision of financial product or service. So, I have clients who, maybe something was just mis-mailed. So, it was only the name and&