Regulatory Oversight Podcast — Facial Recognition and Legal Boundaries: The Clearview AI Case Study
Host: Stephen Piepgrass
Guests: David Navetta, Lauren Geiser, and Dan Waltz
Aired: June 10, 2025

Stephen Piepgrass:

Welcome to another episode of *Regulatory Oversight*, a podcast dedicated to delivering expert analysis on the latest developments shaping the regulatory landscape. I'm one of the hosts of the podcast, Stephen Piepgrass, and I lead the firm's Regulatory Investigation Strategy and Enforcement, or RISE practice group.

Our podcast highlights insights from members of our practice group, including its nationally ranked state attorney's general practice, as well as guest commentary from industry leaders, regulatory specialists, and government officials. Our team is committed to bringing you valuable perspectives, in-depth analysis, and practical advice from some of the foremost authorities in the regulatory field today.

Before we begin, I encourage all of our listeners to visit and subscribe to our blog at RegulatoryOversight.com to stay current on the latest regulatory developments.

Today, I'm joined by my colleagues David Navetta and Lauren Geiser from the Privacy and Cyber Practice Group, along with Dan Waltz from our RISE practice group, to explore the dynamic landscape of state attorney general actions concerning data privacy and AI. Our discussion will be framed by insights from a recent multi-district lawsuit and nationwide settlement that focused on biometric data, privacy considerations, and then we'll also discuss the varying enforcement approaches of different state AGs.

David, a partner in the firm's privacy and cyber practice group, is a trailblazer in data protection. He's adept at managing complex data security challenges from breach response to cybersecurity risk management. David serves clients from startups to *Fortune* 500 companies across various industries and guides his clients through the intricate landscape of data leverage, and monetization, offering strategic advice that plans deep knowledge of privacy security and data with practical compliance solutions.

Lauren, who I've known for many years, is an associate and litigator in the firm's Privacy and Cyber Practice Group. Based in LA, she focuses her practice on complex business disputes and privacy litigation. Lauren has represented major financial institutions and large data companies in high-stakes litigation across federal and state courts. Lauren also has experience representing clients in state AG matters and SEC enforcement actions.

Dan is an associate in our RISE practice group and has a robust background in navigating the complex intersection of industry and government. Dan's experience as an assistant AG in the

Illinois Attorney General's office has equipped him with valuable insights about regulatory investigations that are helpful to our industry clients.

[EPISODE]

Stephen Piepgrass:

Well, Dan, Lauren, and David, it's great to have you on board the podcast today, and I'm really excited about our conversation. Obviously, the topic here is Clearview AI and the settlement deal that was okayed by the judge, as well as some more recent developments, including a state filing suit. So, maybe it would be helpful for one of you to provide an overview of the lawsuit and bring our audience up to speed on it as part of setting the stage for this conversation. Lauren, do you want to do that?

Lauren Geiser:

Sure. Thank you. Thanks so much for having me, Stephen. You know I'm a long-time listener of this podcast, so I'm very excited to be here today.

So, the Clearview AI Settlement, it's a case rising out of the northern district of Illinois, federal court. It dates all the way back to 2021. So, this case has been going on for a very long time, very long docket, if you want to peruse it. It is a multi-district litigation, also known as an MDL. And what is an MDL? For those who don't know, it's a procedure used in the federal court system to consolidate numerous civil lawsuits with common questions of fact into a single court for pretrial proceedings. This streamlines things, it reduces duplicative efforts, and it's more efficient for the parties and the court. It's different from a class action. And MDL, each individual case remains separate, but in this case, the litigation proceeded as an MDL, but the settlement was essentially negotiated as a class.

So, this case was brought against Clearview AI, and Clearview develops facial recognition software used primarily by law enforcement and retail to identify individuals who have purportedly committed a crime or to exonerate individuals wrongly accused of a crime. It's been the subject of controversy due to its ability to identify any individual using a database of publicly available images scraped from the Internet, which could be considered, according to some advocates, to be a privacy violation.

In 2021, these lawsuits began. They alleged various violations of state privacy laws, including BIPA in Illinois statute that I believe Dan is going to speak more about. But before we get into that, did we want to talk about what biometric data is and have Dave give us some insight into that?

Stephen Piepgrass:

That's a great idea. And I think also helpful in setting the stage. So, Dave, maybe you can talk a little bit about biometric data, which was really at the heart of this case.

David Navetta:

Yes, we're talking about biometric data here as well as some level of artificial intelligence being applied. So, biometric data is basically, imaging associated with certain parts of our bodies, like a fingerprint, for example, or in this case, facial printing or facial geometry that allows for the unique identification of an individual. Everyone has a phone, many phones have logins where you can just have a picture taken and log in. During that process, biometric data is being collected and captured about you and a unique image, facial image is being created such that in theory, no one else should be able to use that facial image to log into your phone.

What we have here with Clearview is Clearview going out and scraping basically the entire Internet, millions and millions, tens of millions of people and images, and using those images to create biometric data points for individuals. I don't think it's an exaggeration to say that everyone in the United States has their information in Clearview's system at this point. So, what they do with it is they make that biometric data available as part of their service to help others, whether it be government, private companies, even individuals, identify people. So, you could take a picture of your mom and you could use the Clearview AI database to confirm that picture truly was of your mom, not a deepfake, for example. Or if you're uncertain about someone's identity in the context of say a retail environment, you can use that biometric imaging and some AI and algorithms and analytics to give you some level of certainty that the person being captured in a video or being captured in a photo is a particular person that is in Clearview's database.

So, that's what it does. I think we're going to see more and more biometric information being captured over time. It's showing up in a lot of buildings out in the world, shopping centers, even there's some use cases in stadium type environments that we're going to be seeing in the future.

Stephen Piepgrass:

Thanks, David. I think that's a really helpful overview. One of the statutes that I think Lauren mentioned was BIPA. Obviously, this is something that Dan in our Chicago office has been following closely for quite some time, one of the leading statutes dealing with biometric privacy. And Dan, I know you also spent some time in the Illinois AG's office. So, this is probably a topic near and dear to your heart. Can you talk to us just a little bit about BIPA and what it does?

Dan Waltz:

Yes, absolutely. Thank you, Stephen, and thank you for having me on. The reason BIPA is important in Clearview AI settlement is that, as Lauren mentioned, seven of the complaints, 16 causes of action arise under a unique Illinois law called BIPA, the Biometric Information Privacy Act. I'd like to take a step back because as Stephen mentioned, I am located in Illinois and Illinois has been at the forefront of passing legislation related to some of these issues that we still consider to be somewhat cutting edge from the legal perspective.

For example, Illinois was the first jurisdiction to pass the Artificial Intelligence Video Interview Act which relates to an employer's use of artificial intelligence recognition in the interview process. Illinois was also one of the first states to pass the Genetic Information Privacy Act. And

similarly, we have the Biometric Information Privacy Act or BIPA, which played a huge part of the Clearview AI settlement.

So, Illinois enacted BIPA in 2008, and the reason for that was because legislators recognized that an individual's biometric data, that the data that Dave just described for us is unique. Unlike a Social Security number or a credit card number, it's something that you can't change very easily. Most consumers, if they get their data exposed in the course of a data breach or something like that, cannot simply go to the doctor and say, “Give me a new face.” So, protecting that biometric data has been a priority for Illinois legislators for nearly 20 years.

BIPA regulates the collection, storage, and distribution of biometric information in response to the growing trend that businesses are increasingly using biometric data for various purposes. And that's true across the country and around the globe. If you think about it, we use our face prints to access our phones. We use thumbprints to open our iPads. Frequently, employers require employees to sign in to work and sign out of work using their thumbprints or fingerprints or hand prints or something along those lines. So, biometric information is being used increasingly to verify our identities. What BIPA does is it imposes a range of requirements on any company who wants to use biometric data. Before the company can use that data, the company must get written consent, must get form-driven consent, must have a privacy policy in place that prohibits the sale or profiting from the use of consumer biometric data. Also, the company has to have a plan or a retention policy in place that requires the company to store the biometric data for only a reasonable period of time.

In the state of Illinois, BIPA has been used by plaintiffs' attorneys for quite a while now to sue companies who unknowingly or without intending to violate BIPA deployed a fingerprint or face recognition clock system, for example, at their facilities, and that unless the employer complied with the specific notice disclosure policy retention requirements of BIPA, that employer could be subject to litigation from the employer. The way that we saw a lot of these cases rising up in Illinois is that plaintiff’s attorneys would file a class action on behalf of all employees who worked for a specific employer seeking the statutory damages for each violation of BIPA. And that's really where BIPA becomes unique and important from the private individual standpoint.

BIPA is unique in the sense that it does include a private right of action. It is not something that attorneys general can only enforce. So, individuals can come to court and demand their statutory damages. BIPA's private right of action allows individuals to recover $1,000 or actual damages for a negligent violation of BIPA and up to $5,000 or actual damages for an intentional or reckless violation, plus reasonable attorney's fees and costs. The way that the statute was interpreted was and the way that it is still interpreted to this day is that every scan, every thumbprint scan, every time you clock in and out of the office, can be a violation of BIPA. Not only can each individual scan be a violation of BIPA, but you can violate different sections of BIPA at the same time.

So, for example, if the employer did not have a primacy policy in place, that scan of that employee's fingerprint violates that provision of BIPA, but it also violates the informed consent provision, assuming the employer didn't have informed consent. In other words, every scan of an employee's fingerprint could cost the company up to $3,000. These were very popular class action vehicles. It was almost like, and it is to this day, almost a person, a type of statutory penalty. That's consistent with precedent from the Illinois Supreme Court in the Six Flags case.

There's been one amendment that I want to just briefly touch. In August of 2024, the legislature recognized that allowing three statutory violations for each fingerprint or each face scan was a little bit excessive. So, the statute had to clarify just recently to say that every thumbprint is one violation, regardless of how many different statutory violations might be involved. Now, it's only $1,000 per scan instead of 3,000 for a negligent violation.

It's a really interesting law. It's resulted in a lot of press-worthy settlements. So, it's been an interesting piece of legislation from a privacy perspective that is somewhat unique to Illinois.

Stephen Piepgrass:

Dan, interesting and interesting to the amendment, but obviously from our client's perspectives, that sort of cold comfort, $1,000 per thumbprint collected is still a hefty potential penalty.

Lauren, maybe you could talk with us a little bit continuing the conversation about the litigation about this particular settlement and how it worked.

Lauren Geiser:

Yes, absolutely. So, as I said, this case is old. It's been going on for a while. After about six months, they tried to settle multiple times. It's kind of like a winding meandering path to get here. But the parties negotiated for about six months, they retained retired federal judge from the Northern District of Illinois, Wayne Anderson, to oversee settlement negotiations. And they landed on a settlement agreement providing the settlement class. Because again, I said this is an MDL, but the settlement was essentially negotiated as for a class. The agreement provided the settlement class with a payout from a 23% equity stake in Clearview.

Now, this is what the court called, in its own words, a Goldilocks percentage. It represents the outcome of a delicate balancing act by the parties. To large of a percentage, ran the risk of preventing Clearview from attracting the investors necessary for the startup to grow and provide relief to the settlement class, but to small of a percentage would not have been commensurate with the injuries of the settlement class. As the court said, the zealous advocacy of their claims by lead class counsel. So, this Goldilocks percentage, this just right percentage was 23%, and that's what the parties agreed to.

But that's not the end of the story. I mean, what does 23% equity stake mean? The settlement fund will be funded and paid by the triggering of one of four events that the parties agreed on. The first event is the occurrence of an IPO, initial public offering. The second event is the occurrence of a liquidation event, such as a merger or consolidation or sale of all, or substantially all of Clearview's assets.

The third event is a payment by Clearview of an amount equal to 17% of Clearview's gap recognized revenue for the period commencing on the date of final settlement approval and ending with the election of this option, which expires on September 30th, 2027. Or the final triggering event is the amount the settlement class will receive if it elects to sell its right to receive the settlement stake payment. It's a really interesting settlement and we love a creative settlement. I mean, we often negotiate, especially in these cutting-edge privacy case, for – we

try to think outside the box about how parties can resolve matters. But how does it actually unfold? How does this unfold if the settlement class decides that they want to cash in?

So, they appoint a settlement master who has the right to, upon reasonable notice, they can inspect Clearview's books and records, they can request to receive biannual interviews with Clearview's management team, and they can request to receive information regarding the price and terms of any secondary sales of Clearview stock. In addition to holding the 23% stake until one of the four triggering events we discussed earlier. The settlement master also has the authority to sell the settlement class's rights to a third party, which would immediately distribute the proceeds to the settlement fund.

That can only take place if the settlement master determines that's in the settlement class' best interest. Everyone's favorite part of a settlement, attorney's fees. The settlement fund will serve as the source of all attorney's fees, which are 39.1% of the settlement fund. So, that's really what it looks like, and we're just really taking it all in and thinking about how this will play out. The settlement master has a really important job and an ongoing job. The parties settled this matter, but it's not really certain what's going to happen, how much the parties will be paid and what's triggering event they will choose.

So, it is a very creative approach to settling an action where the company is a startup, but the damages alleged are very high. We've been watching that and thought it was very interesting from a litigation perspective.

Stephen Piepgrass:

We mentioned that one of the things of the settlement that will become relevant is that there's no injunctive relief associated with it. That is also somewhat unusual in this context. Although, Clearview had a different lawsuit brought by the ACLU, which did include some measure of equitable or injunctive relief, meaning the settlement with the ACLU prohibited Clearview from taking certain actions associated with the use of their data and the services they were offering. So, I think that's a relevant point for some of the controversy behind this particular settlement.

Lauren Geiser:

Yes, absolutely. It's interesting the interests that this settlement creates, right? Because if plaintiffs filed suit against Clearview for its conduct, but then, is there a part of them that's hoping that the conduct continues and the company thrives so that their 23% stake is fair and beneficial to them? It's an interesting point.

Stephen Piepgrass:

On that point, the sweet spot, 23%. Dan mentioned it a second ago, BIPA and the statutory penalties up to 5,000 per violation, when you're a company that is scraping millions and millions of facial images and taking all these various steps to provide this service to thousands of customers, the number of violations they had multiplied by anywhere from 1,000 to 5,000 - person or a violation probably is in the billions and billions of dollars.

So, if you literally awarded a settlement or even a judgment on that account, Clearview is completely out of business, right? That is what I think they're trying to balance here is to try to get some sort of remedy out that can actually be beneficial to the consumers who are affected by this without just completely putting Clearview under.

Lauren Geiser:

Yes. One interesting point to note, getting down to the dollars and cents in the court's published settlement agreement, it stated that as of January 2024, Clearview's value was estimated to be approximately $225 million, making the settlement worth $51.75 million, just to kind of put a figure out there that corresponds to this amorphous 23%.

Stephen Piepgrass:

Yes, the other interesting piece about this settlement that I thought, Dan, I think I'm sure you found interesting as well, was that it was approved over the objection of 22 states, state AGs, including the District of Columbia, and that's CAFA of states the ability to be notified in cases of class action settlements, and then state AGs can weigh in and object. And that's what these states did through an amicus brief led by Vermont, which then turned around and filed its own suit against Clearview AI.

So, Dan, maybe you could talk just a little bit about that process and its ramifications.

Dan Waltz:

Yes, absolutely Stephen. So, you're right, we had 23 AGs, 22 states, and also the District of Columbia who filed an objection under their CAFA authority. The objections are primarily to two issues. The first one was specifically the concern for the consumers and the monetary relief the consumers would get. And the AGs were concerned that by providing us equity stake, there's no guarantee that consumers will get anything.

In other words, if Clearview AI folds, then 23% equity stake, 23% of zero is still zero. So, there was the concern over whether or not the consumers would get any real monetary relief in this settlement. A second primary concern for the AGs was the lack of any meaningful and junctive relief. Essentially, what happened here is that Clearview AI had settled a lawsuit by the ACLU a couple of years prior, and that was specifically an Illinois class of litigants.

In that Illinois class, there was limited injunctive relief afforded primarily to Illinois residents. That's really the limit of the injunctive relief afforded. But the existence of the injunctive relief in Illinois allowed the judge to say, “Well, I understand your concerns, State Attorney Generals, with respect to the business practices, but it's not fair to say that there is no meaningful objective really because of what occurred in the ACLU case a couple of years earlier.”

Stephen Piepgrass:

Yes, and I think that was probably coupled with the fact that really BIPA was the primary statute and it applies in Illinois that gave teeth to this lawsuit, and that at least was addressed in the

settlement, put the states on somewhat of a weaker position than they might otherwise be when they filed an objection because the ones that were objecting did not necessarily have a legal hook like BIPA as Illinois had.

Dan Waltz:

That's a really good point, Stephen. You're absolutely right. There are a few other instances of Biometric Information Privacy Act. Texas and Washington have fairly robust ones that mirror Illinois, but those do not provide a private right of action. And then other states like Colorado and California reference biometric data in their comprehensive consumer privacy acts, but they're markedly different from BIPA. So, you're absolutely right.

I think, Judge Coleman did mention the fact that Illinois was unique in the sense that it actually had a statute and a law to enforce around the environmental information privacy at issue. So, when you think about it like that, the legal position of the state is to object is weaker.

Stephen Piepgrass:

Yes, that in many other cases lack. As you all know, and as our listeners know, we often like to wind up things with takeaways and maybe I'll start with my thoughts on that, and mind deal with this objection by state AGs. As companies are thinking about class actions, always keep in mind that notice provision under CAFA. It may be worth it to try to avoid objections, reaching out to attorneys general and working with them to get them comfortable with settlements, particularly ones that have significant public policy ramifications. That's something that class counsel sometimes don't think about until the end, But it can be worth it even earlier in the negotiations to reach out and try to work with the AGs and do your best to avert spin-off litigation like what we saw here in Vermont.

So, that's my takeaway. Lauren, do you have any of those? And maybe then we'll turn to Dave and then Dan.

Lauren Geiser:

From a litigation perspective, because I am a litigator in Troutman's privacy group, I'm based in Los Angeles. I just think that this settlement really does provide precedent for creative settlement negotiations and terms. I know the AGs obviously are not a fan of the 23% because it could be nothing for the class, but it could also be very lucrative to the class, depending on how this unfolds and how Clearview performs.

So, from a freedom of contract perspective and from a creative settlement perspective, I think this is a really innovative settlement agreement and something that we're keeping in mind for our clients as we litigate and as always try to resolve matters to the parties and our client's satisfaction whenever we can to keep things from ballooning or getting bigger, which is always a risk in privacy cases because it's all over the news, it's everywhere and navigating that is challenging. So, it's a creative settlement and we're interested to see if or similar settlements arising from biometric data follow.

Stephen Piepgrass:

Dave, how about you? Any takeaways for our listeners or for clients who are thinking about this particular settlement and particularly the collection of biometric data more generally?

David Navetta:

Key takeaway here, it ties to statutes that provide for statutory damages without necessarily a need to prove hard. Whenever you have one of those, plaintiffs are going to be interested, and we're seeing that in California with the SIPA law. We're seeing it in a lot of other jurisdictions, which means, from my perspective, I'm a privacy and cyber lawyer at the practice here at Troutman partner. I advise companies in order to avoid this type of liability and this type of risk.

I think what has happened here, not only from a plaintiff's point of view, but from the AG point of view is a particular company kind of going arguably to an extreme when it comes to scraping and the use of biometric data and really wanting to make an example of that company, right? To really send a message that these types of behavior and the AG is fine and the plaintiff's mind is not all right.

So, when I'm advising clients and my takeaway ultimately is to think about what you're doing as an organization Now, more than ever, companies are scraping and trying to leverage the data they have, whether it be biometric data, location data, health data, whatever it may be. And there are some footballs and some traps that can happen if that's not done correctly and done with an eye towards the potential risks, not only from the litigation point of view and the state AG and federal AG and international regulator point of view, but even from the customer relations point of view.

Taking all of these things into account now is more important than ever if you're a company that's heavily reliant on the use of personal data to provide your business, product services, what have you. That's my takeaway is be proactive. Use this particular red flag as a way to analyze your own practices, and hopefully avoid a similar outcome.

Stephen Piepgrass:

Great points, Dave. Dan, I'll give you the last word. Any final takeaways on your end before we wrap up?

Dan Waltz:

I'll take the last word, Stephen, thank you. From my perspective, the most interesting thing about this settlement is how the plaintiff's attorneys leveraged the interests of the AGs to create a settlement that really protects clear Clearview AI and protects the private individuals who stand to receive compensation from the settlement. So, really it was the negotiation by Clearview AI's counsel, I think, who set this up in a way that helps ensure that Clearview AI has a long path forward that won't be crushed by regulatory pressure.

So, when state attorneys general act, they typically act in the interest that their constituents, their voters, in the act pursuant to their parens patriae authority. In this case, there's a question, what does parens patriae authority mean? On the one hand, the class is set to potentially receive millions of dollars, tens of millions of dollars through the equity stake. But on the other hand, the AGs don't interpret any meaningful injunctive relief in the settlement. So, if the AGs were to pursue their goal of being pull injunctive relief on the one hand under their parens patriae authority to protect their constituents, that risks or places in jeopardy any sort of monetary relief because the injunctive relief the AGs want is for Clearview AI to stop doing its business, which will render its business value virtually nothing. The class individuals will not get any money at the end of the day.

So, there's a balancing act that every single AG is going to have to do now, and that is whether it is more important from their policy and electoral objectives to ensure that the individuals receive the monetary compensation or to ensure that there is, from what the AG's perceive as, sufficient injunctive relief. Pitting those two issues against each other really creates an interesting dynamic. I think that is going to have a lot of AG scratching their heads. There is at least one state, as Stephen had referenced earlier on in the podcast, Vermont, which has seemingly made that decision. And Vermont did, in fact, file its own lawsuit on April 25th. That lawsuit, essentially, if successful, will preclude Clearview AI from operating within that state. More states that follow suit, create greater jeopardy for Clearview AI's business model for the jeopardizing the potential monetary relief of the class.

It's just a really interesting dynamic, very cool to observe in real time, and definitely worth watching those subsequent state AG litigations that come from this.

Stephen Piepgrass:

I agree. I think we will all be watching this closely, and particularly looking to see what happens with that Vermont case. David, Lauren, and Dan, thank you again for joining me today. I've thoroughly enjoyed our conversation, and I'm confident our listeners have appreciated your insightful perspectives. Thank you to our audience for tuning in. Remember to subscribe to this podcast on whatever platform you choose, and we look forward to having you join us again next time.

Copyright, Troutman Pepper Locke LLP. These recorded materials are designed for educational purposes only. This podcast is not legal advice and does not create an attorney-client relationship. The views and opinions expressed in this podcast are solely those of the individual participants. Troutman does not make any representations or warranties, express or implied, regarding the contents of this podcast. Information on previous case results does not guarantee a similar future result. Users of this podcast may save and use the podcast only for personal or other non-commercial, educational purposes. No other use, including, without limitation, reproduction, retransmission or editing of this podcast may be made without the prior written permission of Troutman Pepper Locke. If you have any questions, please contact us at troutman.com.