***Regulatory Oversight* Podcast**
**12 Days of Regulatory Insights: Day 5 – Privacy Under the Microscope**
**Speakers: Gene Fishel and Dave Navetta**
**Date Aired: December 10, 2025**

**Gene Fishel (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 this past year in various areas and designed to keep our listeners informed and engaged during the holiday season. I'm Gene Fishel, a counsel here in the firm's regulatory Investigations Strategy and Enforcement Practice group, and part of the firm's state attorney's general team. 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. Today's episode is focused on privacy, and I am pleased to be joined by the supremely experienced Dave Navetta, a colleague of mine here in the firm as we unpack 2025 privacy enforcement trends and take a look ahead to what's coming in 2026. Dave's a partner in our firm's privacy and cyber practice group and advises clients on all aspects of technology and data law, including data privacy, information security, ai, financial reporting, data governance, technology related transactions, and data monetization and use. And Dave and I were going to dress in outfits today, but we're told this was not a video recording. Regardless, Dave, I appreciate you being here today with me.

**Dave Navetta (01:39):**

Yeah, too bad about the costumes.

**Gene Fishel (01:40):**

So Dave, I want to open the floor up to you. Have you comment on what you're seeing as far as privacy and cyber related trends, particularly maybe regulations or litigation that companies should be aware of that has taken place over this past year.

**Dave Navetta (01:56):**

Gene, at the end of the day, there is so much going on. We could probably talk for several hours on trends and things that regulators care about. I'm going to focus on something I've been working on, which I think is interesting related to tracking technologies and consent issues. So stepping back for quite a while now, but increasingly this year especially, there have been a wave of demand letters and lawsuits alleging against companies on their websites that they have violated various wiretapping laws. And the claims basically say when a user visits a website and there are tracking technologies like advertising technologies or analytics technologies on the site that are run by third parties, plaintiffs are alleging that the communication is being intercepted by a third party. When a visitor comes to the site, it could be content of the communication. So if a user puts something into a search bar and the search bar

URL ends sending out content associated with the search, they're alleging that's a wiretapping issue, or they're alleging that there is a pen test or a trap and trace type of interception, which involves metadata.

So all of these laws that are being used, especially in California, Pennsylvania and Florida, even at the federal level to some degree, are laws that were passed in the sixties and seventies intended to address wiretapping on traditional phone calls with probably rotary dials and other things that no longer exist. So plaintiffs have been really creative about that, and there have been some big cases. There's been a case that went to a jury trial against a large tech company, but ultimately the case law is very strong in many ways because plaintiffs are able to get past motions to dismissed oftentimes even to class certification. And so they have leverage and they have settlement value. Now, how does that relate to regulatory issues? What's also happening simultaneously and where these things are coming together are regulators and especially California starting to be more forceful and aggressive and enforcing and companies use of tracking technology, especially when there's an option to opt out of sales or sharing of personal information.

So again, background wise there, many of the state privacy laws have requirements to enable people to opt out of the sharing of their information to third parties for advertising, cross contextual advertising purposes. What we're seeing out there is regulators, similar to plaintiff's lawyers going out to websites, looking at what cookies and tracking technologies and pixels exist, understanding what data is going out and actually going through and having someone test the opt-out process on the site. Now, some sites don't have an opt-out process. That's a different issue, right? So a regulator might come after a site for not having or providing that opt-out option, but what's happening here is regulators testing those options and opt-out mechanism to see if they actually work. And what they're finding in some cases is that they don't work. And actually this is a pretty common theme, even when companies are setting up third party consent management processes and someone is opting out, there are cases where after that opt-out, the transfers to these third party advertising analytics cookies and pixels still is occurring. So that is the basis for regulators to say, A, you're not complying with the CCPA in this case under California law, and B, it's a potential unfair or deceptive trade practice. So we've seen in fact, the largest settlement to date with the California now cow privacy regulatory scheme with Tractor Supply Company of $1.35 million based on this very issue. So I'll pause there for a second.

**Gene Fishel (05:58):**

That is a very timely analysis, and in fact, from my end, looking at how state AGs are approaching the data collection, the tracking sort of thing, one thing that pops into my mind are recent actions against streaming services. And actually closely related to what you just said in California, California AG, Rob Bonta just recently announced a settlement with Sling tv, of course a streaming service, and it was very much related to their opt-out mechanisms and the AG there alleged that Sling had very hard to find methods of opting out of the sale of personal data. I think customers had to go to some web form that was maybe hard to find on the site and fill it out. And we see AGs pushing for a much easier form of opt-out, maybe sort of a one click opt-out mechanism. The other aspect of that settlement coming out of California was also regarding children's use of streaming of the sling in California.

There alleged that pursuant to the CCPA, they were not offering these opt-in authorizations for kids under 16 and obtaining consent that way for the sale of data. And I think what's interesting here is of course, California as you mentioned, is supremely active in this space with the CCPA, they were the first out there. There have been two other recent enforcement actions coming out of Michigan and Florida regarding streaming services. Those two actions involve Roku and they filed lawsuits against Roku. But as I look at these three actions over this past year, California, Michigan, and Florida, what's interesting to me, and it's all related to opt-out and consent and the sale of data, what's interesting to me is the three AGs in those states are attacking this issue under three different legal mechanisms. California is moving under their CCPA comprehensive consumer privacy law. Michigan has filed suit under COPPA, the Child Online Privacy Protection Act, which grants state AGs authority to bring suit.

Yeah, federal law. Yeah, federal law and Florida is proceeding under their consumer protection law. All three deal with, well, one common element is children's data, so let's just put that out there. AGs are very much concerned about how children are operating on streaming services, but really any website and how companies are collecting that data, children and the sale of data very prominent. That was part of the California settlement. But I highlight these three because AGs, they're focused on the sale of data in particular, and each state AG has a different tool basically that they can proceed under. And we've seen that in three different states. Again, the overall message here though is regardless of what law these AGs are proceeding under, companies need to have clear opt-out mechanisms. They need to have clear disclosures in how they're using the data because that's the basis for at least the Florida claim and also be able to obtain consent, particularly when children are involved, a clear consent and in some cases parental consent like under Kapa. You need that if the child's under 13. So very interesting landscape here. Lots of tools that AGS can use that sort of dovetail into what you were speaking of.

**Dave Navetta (09:40):**

It's also coming from the class action lawyers, right, who arguably

The damages associated with a SIP a claim are 5,000 per violation. So even though a settlement was 1.35 million with the Tractor supply company for one of these claims with the regulator, the damages are potentially enormous for the actual lawsuits. Looking at some of the things the regulators care about, just maybe a little bit of a summary for companies that when they're thinking about their opt-out and opt-in processes, the California and other regulators are worried about over verification, requiring additional steps for a user to be verified before they can make a request. That was one issue that they brought up under California. The GPC signals global privacy control signals. The failure to honor those was also a big issue with the regulators. There also needs to be opting out, addressing both online and offline sharing. So when someone opts out of sales altogether, if you're just dealing with your website, you might be missing offline sales that are occurring.

There need to be regular assessments of these technologies. They don't always work properly. So we see a lot of companies trying to do the right thing, but it's complex. Websites are complex, the data transfers are complex. Configuring the consent management process could be complex, so you can have everything there present but not working, which can cause issues. And then if you're going to actually create these processes, keep an eye out for dark patterns,

one area that they were concerned about was symmetry of choice. So if there's a big button that says accept all cookies and a minuscule button that says reject all on the same page, regulators may take the company to task and say that they're employing dark patterns trying to get the consumers to choose these trackers. Those are some takeaways.

**Gene Fishel (11:29):**

And just given the season here, just to tie a bow on this particular topic, it shouldn't be overlooked that both litigators, private litigators, plaintiff's lawyers actually look at what regulators do. They look at the actions regulators take and oftentimes will base their claims on maybe a claim that's filed by a state AG and also all the state AGs talk among each other. They routinely meet. It's no coincidence that both Michigan and Florida, for example, filed suit against Roku. All of these AGs share information they meet on a monthly basis, at least they're now privacy consortiums of certain AGs that share information. And like I said, it crosses over sometimes into the private class action realm. So there are a lot of minefields and private litigation and state regulatory actions often overlap and our similar in claims. But let's move on here for our second part. We want to preview maybe what's coming ahead in 2026 in the privacy cyber realm. What companies should be aware of? Dave, what's on your radar coming up here?

**Dave Navetta (12:41):**

Well, this follows a similar theme to what we just talked about, the sale of data and war regulatory activity around the sale of data. Where the rubber's going to hit the road starting in 2026 are around data brokers. And so the delete act in California is coming online, but other states like Texas also have their own data broker laws. There are a few things to keep in mind here. First, the definition of a data broker, right? Early on around the registration requirements in California for data brokers, the CCPA defined data broker in a way that was more, I would argue, narrow. And really what it defined the data broker to mean is a company who sells information. Again, that's the broad concept of sell under California law related to data subjects or individuals with whom they don't have a relationship. So it wouldn't be someone visiting your website, it would be someone whose data you get from another third party perhaps who you're going to try to send out marketing leads to.

So if a company were to sell that data, then they could be considered a data broker. Pretty straightforward. What happened though in the regulatory scheme under California's privacy laws, the definition of data broker was arguably expanded. Now you can be an organization with a direct relationship with the consumer comes to visit your website, but if you go out and buy data about that person, maybe from a data broker to enrich your data about that consumer, your customer, at least the data we're talking about that you purchased, obtained from a third party, that activity in selling that data could be considered a data brokerage activity. So now suddenly companies who thought they were in the clear because their data that dealt with companies that they had a first party relationship with no longer were in the clear and could be considered data brokers. So the first step really now, but in 2026 especially, is to figure out whether you are a data broker and many companies know their data brokers, but other companies may be inadvertent data brokers and may not be fully aware that some of the data that they're supplementing to their customer or profiles and sending off to other third parties could be a sale and it could make them a data broker.

So that's the first issue that needs to be dealt with. Then the delete act itself is coming online. So the Delete Act big picture is a one-stop shop for opting out of sales by data brokers and there's a technological component to it. So in 2026, California regulators, Cal Privacy are going to be putting out regulations and developing the delete request and opt out platform, which ultimately is something that data brokers need to register for. And what it will amount to is a mechanism whereby individuals, California residents in particular can use the drop mechanism to opt out of all sales by all data brokers and data brokers starting August 1st, 2026 will be required to check the drop mechanism every 45 days to determine if people opted out of sales. And then if they have opted out of sales data, brokers will have to then stop the transfer or selling of personal information associated with the individuals who dropped out of sales.

So that could cause a huge sea change in terms of how data is being transferred, because now instead of having to go to every single website that you visit and opting out of sales, and obviously not even in some cases being aware that third parties have your data to be able to opt out of sales. Now the onus is on the data brokers to check this mechanism and allows people to do a one-stop shop and stop their data from being transferred. So that's going to be a big effort for our companies, especially those who are not aware or may not be aware that they could be considered data brokers. They're going to have to do some homework to figure out whether they're actually transferring data in a way that puts them in that category. And in fact, we've seen some regulatory activity by the California regulators and others really questioning whether certain companies are data brokers as it stands today. And so I suspect that there will be more activity when the DELETE Act comes out or regulators are questioning companies as to why they haven't registered to be a data broker and therefore comply with the delete Act down the line.

**Gene Fishel (17:08):**

And in fact, I know some other states actually are using the Delete Act, California Delete Act as a basis for similar legislation in their states, and it's going through as usual, California's on the forefront. I'll just touch on very quickly here, a couple developments in AI that are going to come online. And really starting January 1st, 2026, we have California recently passed the Frontier AI Act, which addresses sort of the most advanced general purpose AI systems that exceed the capabilities of current models that comes online January 1st. That's going to require developers to publish their AI framework and how they've assessed and mitigated risks associated with that. And also companies are going to have to start reporting critical safety incidents to an office of emergency services in California. That's one thing coming online that's going to affect privacy of cyber. Also, Texas's AI law that was passed earlier this year goes into effect January 1st, 2026.

It's a fairly comprehensive act where companies, it applies to both developers and deployers of AI systems. They have to disclose AI use in a healthcare environment. They can't deploy or develop systems that infringe on any sort of constitutional right. That's a pretty broad provision and they can't develop or deploy. Companies can't develop or deploy AI systems that cause some sort of harm. Also mention Colorado's AI Act. There's been a lot of debate in their legislature. It's been delayed. That is an act focused on algorithmic discrimination. Right now, it's set to go into effect, I believe in June of next year. It's sometime in the summer. I think there's going to be more debate on that. So just keep an eye on Colorado. But in any event, AI of course is an exploding issue across the country, is going to greatly affect how companies use

AI systems in touching personal identifying information. And companies need to be aware that they are effectively granting consumer data requests and data subject rights pursuant to comprehensive consumer privacy laws. Dave, I didn't know if you have any other final comments on ai. So I think there's

**Dave Navetta (19:35):**

Obviously the three laws that are specific to ai, but probably about 20 privacy laws. Well, there are 20 privacy laws. Several of the privacy laws also regulated automated decision making and profiling, which ultimately a lot of AI is involved in those types of activities. So a lot of these laws require data privacy impact assessments if there's automated decision making that involves consequential type decisions or certain types of profiling that can result certain decisions made against or with respect to individuals. So not only do you have to worry about these AI laws specifically, but make sure that you're checking these privacy laws as well because they have some backdoor AI requirements in them that could be substantial

**Gene Fishel (20:21):**

Privacy laws and also consumer production laws, AGs of signal. They will look at AI systems in that context too. Well, Dave, thank you again for taking time to discuss the ever evolving regulatory litigation slash litigation landscape in the privacy and cyber realm. It's going to be an interesting year coming up, a lot of activity for privacy, and I hope our listeners gleaned something this discussion, and I 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 insight series. Please make sure to subscribe to this podcast via Apple podcast, Google Play, Stitcher, or whatever platform you use, and we look forward to our next discussion. Thank you.

**Dave Navetta (21:10):**

Thanks, Gene.