Regulatory Oversight Podcast: Decoding Privacy Laws: Insights for Small to Mid-Sized Businesses
Hosts: Stephen Piepgrass, Gene Fishel, and Joel Lutz
Guests: Aurelia Lewis and Beth Saunders

Stephen Piepgrass:

Welcome to another episode of *Regulatory Oversight*, a podcast that focuses on providing expert perspective on trends that drive regulatory enforcement activity. I'm Stephen Piepgrass, one of the hosts of the podcast, and the leader of the firm's Regulatory Investigations Strategy and Enforcement Practice Group.

This podcast features insights from members of our practice group, including its nationally-ranked State Attorneys General practice, as well as guest commentary from business leaders, regulatory experts, and current and former government officials. We cover a wide range of topics affecting businesses operating in highly regulated areas.

Before we get started today, I want to remind all of our listeners to visit and subscribe to our blog at regulatoryoversight.com so they can stay up to date on developments and changes in the regulatory landscape.

Today, my colleagues, Gene Fishel and Joel Lutz, speak with Aurelia Lewis and Beth Saunders of Lewis Media. By way of introduction, Gene Fishel is a member of our RISE practice group. He's the former chief of the Computer Crime Section in the Office of the Attorney General of Virginia. Joel Lutz is a member of our Privacy and Cyber Practice group and brings extensive experience in designing and implementing global privacy programs, including 19 years of combined in house and law firm experience.

Our guests, Aurelia Lewis, who is the founder and president of Lewis Media Partners, and a good friend of mine, and Beth Saunders, who is its vice-president, are both alumni of the well known Martin Agency.

Aurelia and Beth together bring over 60 years of world class media channel planning and buying experience to the table. Over the past 26 years, they have transformed Lewis Media Partners into a highly respected media agency in its own right, serving clients in Virginia, the Southeast, and across the United States.

Gene, Joel, Aurelia, and Beth focus on privacy laws and regulations of importance to small to mid sized businesses. They discuss the challenges these businesses face seeking to comply with these laws, and they provide insights into what might attract regulatory attention to these businesses. I know we're all looking forward to this discussion.

Gene Fishel:

Well, thank you, Steven. It's a pleasure to be joined by my colleague, Joel Lutz, from here at Troutman. We're very much looking forward to this very interesting conversation with Aurelia Lewis and Beth Saunders of Lewis Media Partners. I think we're going to cover some pertinent relevant topics concerning privacy, and particularly, as it relates to the laws that are proliferating

Regulatory Oversight Podcast: Decoding Privacy Laws: Insights for Small to Mid-Sized Businesses

at a rapid pace and how they apply to mid and small businesses that have to deal with them. So, I want to kick it over to Aurelia first. Aurelia, if you could maybe just give a bit of an overview of the services that Lewis Media Partners provide, in any pressing issues, you all are seeing on your side?

Aurelia Lewis:

Yes, thank you, Gene. We are an advertising agency that specializes just in paid media. So, we don't do creative here. However, with the consumer privacy laws, that's very top of mind. We're spending a lot of time with Google and Meta, and a number of the digital platforms. So, consumer privacy is definitely a top-of-mind topic here. We handle a variety of clients. We have about 40 clients, and they range in size. One of the questions that we're trying to answer and to help our clients answer is, why should you care, or pay attention to the consumer privacy laws right now? That's a big topic. We're trying to get everyone to stand up and notice that this is an issue, and it's going to be a growing issue.

Gene Fishel:

Well, understandably and right off the bat, as I mentioned, privacy laws, cybersecurity laws, they're proliferating across states at a rapid pace. What I'll say is, these laws do not discriminate based on the size of a company. So, you could be a very large company, you could be a very small company, and you're likely going to have to comply with some privacy statute or regulation. As of right now, just the other day, there are now 16 states that have passed a consumer data privacy protection act, and these had been passed, beginning in 2020 with California. The most recent one was Nebraska, I believe, who passed, what are called CDPAs.

Among the states, these consumer privacy acts, they can vary based on their provisions, but a lot of them share common elements. And those common elements can really be divided into two categories. One is consumer control over their personal data, and the second is the regulation of data handling, how companies are handling this data. So, when it comes to consumer control, these CDPAs that are coming into effect, they require that companies provide notice from two consumers as to how they're using their data, how they're processing the data. They provide consumers the right to access their data, what data is being collected, or confirm that it's being collected. They provide them the right to delete the data, the right to obtain a copy of the data, the right to correct the data. Also, importantly, the laws required the right to opt out of the sale of data, or from certain targeted advertising.

So, these are generally common themes across these various CDPAs that are being passed. On the data handling side, the laws required that companies limit the collection of certain data to what is adequate and relevant to the purpose it's being used for. Companies have to process it consistent with the notice that they're providing consumers as to what they're doing with their data and how they're collecting it. They have to implement "reasonable, physical, technical, and administrative data security practices surrounding the data."

Finally, when we're talking about types of data involved, many of these statutes, most of these statutes will distinguish between personal identifying information, certain types of that and also sensitive data, and sensitive data often includes children's data, data concerning religious beliefs, sexual orientation, mental health, immigration status, and even geolocation data. With

that sensitive information, most of these statutes require that companies obtain consent prior to processing the data.

So, those are important common themes that companies need to be aware of concerning the CDPAs. There are certain volume requirements that trigger these laws meaning in many cases, for example, in the state laws, companies have to be processing 100,000 consumers data for the law to trigger, or they're obtaining at least 50% of their gross revenue from the sale of that data for these laws that trigger. It's just very important. Of course, I'm giving a broad overview here. It's very important companies be aware of this, pay attention to the volume, and the types of data they're collecting. Of course, consult with appropriate legal counsel to make sure that they're complying with other laws.

Now, the other thing I want to mention is, what kinds of data are we talking about? What are the data points that companies should be aware of? Well, as far as the CDPAs, go, that had been recently passed, it's fairly broad. Let's use California example. California was the first to pass back in 2020. They've been out in front of privacy issues. Under California, these laws are going to trigger with any information that "identifies, relates to, describes, is reasonably capable of being associated with, or reasonably could be linked directly or indirectly, with a particular consumer."

It's a very, very broad bucket of information that can fall within these. Like I said, this can even include internet activity, beyond just your typical personal identifying information, which of course, could be name, address, social security number, financial account numbers, that sort of thing, driver's license numbers. But it can also include that Internet browsing history, search history, geolocation data, as I mentioned. Again, very sweeping acts that had been passed in the last four years. So far, 16 states, you have another at least 10 states now considering this legislation. That is on top of the other privacy laws that have already existed. Database breach notification laws that require notification to consumers and a lot of times, state attorney's general offices when you've been breached. There are data-specific laws, of course, like HIPAA federal regulations applying to medical information that is collected. There's Gramm-Leach-Bliley and financial information regulations. The Securities and Exchange Commission just this past year, promulgated new regulations requiring notification for publicly held companies when they've suffered material cybersecurity incident.

So, lots of regulations and laws across the landscape for companies to consider. If they're not considering them, or following them, it could result in litigation. We've seen the litigation threat facing companies can be from class actions, major class actions, against not only large companies, but mid to small companies, in addition to regulatory actions taken by government entities that companies really need to be aware of. That's the landscape we're dealing with here. Aurelia, do you have any –

Aurelia Lewis:

Yes. Question, because we have a lot of non-profits that we work with, and we are collecting data on that. Are the non-profits excluded from this? We get that question asked a lot. I think it's the other category might be education, higher education. So, those are some of the questions that we're getting as well. Are there companies that are excluded from these laws?

Gene Fishel:

I'm going to turn that over to Joel. Why don't you launch into this?

Joel Lutz:

Sure. Thanks, Gene. So, as Gene said, each of these states that have passed these comprehensive data privacy laws have different thresholds and requirements and exemptions. Most have some kind of exemption for non-profits, but they vary by state. So, you really have to look state by state. Some have blanket exemptions for non-profits. Connecticut, Indiana, Iowa, fall into this where they just say, "This doesn't apply to non-profits or non-profit corporations, as defined under their state laws." So, you have to look at the state law and make sure that your non-profit qualifies for that exemption.

Other states limit which non-profits are exempt based on the activities of the non-profits. These can get very specific state by state. So, privacy laws in Delaware, for example, only exempt the non-profits that are dedicated exclusively to preventing and addressing insurance crime and non-profits that provide services to victims of certain crimes of violence. So, you can see that's a very specific type of nonprofit in Delaware that's exempt. I raised that to say you really have to go state by state and know which state your non-profit is potentially under the jurisdiction of and then look at the exemption there. There is, at least one state, Colorado, that does not having an exemption for non-profits.

I think the moral of that story is, generally a lot of them exempt non-profits, but you really have to look state by state.

Aurelia Lewis:

Gotcha.

Joel Lutz:

Just, Aurelia, to pick up on the broader question of who do these laws apply to? And what do you do when you have a small or mid-sized company? Really, I mean, Gene mentioned the thresholds. But each of these states has some small business exemption, but they all craft them a little different. Most set a threshold of the volume of data that you collect about people and say, "If you're under this volume, then you're exempt, effectively considered a small business." Usually that's 100,000 consumers, which seems like may seem like a lot depending on how big your company is. But it's always important to remember that, that 100,000 counts visitors to your website if you collect data about them, like through cookies. So, the data that Gene was mentioning that we don't usually or haven't historically, in the US thought of as personally identifying information, like IP address and device ID, things that online trackers pick up is now considered personal information under these statutes.

So, if you simply have a website and have some data analytics, cookies running on it, that collects that type of information, each of those visitors can count towards the 100,000 consumers that would reach the volume.

Some other states lay on a revenue threshold for the small business exemption. And usually, it varies by state that do that, but usually, it's around $25 million in gross revenue. Then a few states kind of take the approach, like we mentioned with the non-profit exemption, and they just say small businesses, as defined under our state law are exempt. So, again, I think this just highlights the first question when a company hears about the privacy regulations, the new privacy laws that the states are passing is, does this apply to them? And you really have to look at the jurisdiction, the type of business you are, the type of data you're collecting, to figure out, does this apply to me or not?

Aurelia Lewis:

I will say, Joel, yesterday, we had a good meeting with a non-profit and I asked them the status of what they were doing on there and it was a very good conversation. I was really happy to hear that they were being proactive, and looking at the situation. So, I applaud Joel. That's not really our field, but it was great that they were leaning into it. That was good news.

Joel Lutz:

It is good news. There are other reasons for non-profits to consider taking actions, taking some compliance steps, even if they are technically exempt from the statute. One, is really, just like you're doing with those non-profits and building trust in you as a service provider. They want to build trust with their clients. So, disclosing what data you collect about people is now the norm. They can also protect you from some of the litigation that Gene mentioned. Even if you're exempt as a non-profit, there may be other business reasons to consider taking some of these steps around transparency and telling people what data you have about them. Because that's, frankly, what consumers are beginning to expect in the United States now.

Aurelia Lewis:

Definitely. So, Joel, I think you just hit on a great point about compliance. Most of our clients, or all of our clients, really want to be compliant. But there's so many nuances around that, that one of the most common questions we get is how do I know that I'm in compliance?

Joel Lutz:

That's a tough one. Obviously, that's why we're here. But I think it starts with some amount of data management or data governance. Those can be big fancy words. But it really comes down to for small companies that have grown big enough for this to be a concern. They need to know, have some idea of what personal data do they collect? And as Gene pointed out, that definition is now very broad for the type of data that we're talking about.

First of all, have they identified what personal data they're collecting? Then they need to know who do they collect it from? So, in what context do they collect it? Is it customers of theirs? Are they acting as a service provider for another company? Is it business to business? Because we didn't talk about this but most states privacy laws don't apply to business-to-business personal information. It's really focused on consumers. Big exception is California, their privacy statute. Even though let's call it consumer privacy statute, it does apply to business-to-business personal data and employee data.

But you have to know what data you're collecting and who you're collecting it from. Then, you need to know some things about where are you storing and processing that data? So, in what systems? Which part of your technology are you doing that in? What are you using it for? And who are you sharing it with? Because those are keys to the privacy regulations and compliance. You have to tell people what data you collected about them. You have to tell them what purpose you're using it for. You have to tell them who you're sharing it with, at least, the categories or types of other companies that you're sharing it with and what they're using it for. Then, you have to be able to respond to the data subject rights request.

That means the request to delete, the request to know what data you have about them that Gene mentioned earlier. It really starts with some level of data management and data governance, and just knowing what data you have, knowing where it is, knowing how you're using it, and who you're sharing it with. That's the foundation, and you can do that in various levels of detail. Obviously, some bigger, more mature companies may have a lot of tools and technology to do that. But for small companies, it may just start on a spreadsheet, really going through their different lines of business and understanding what data they're collecting.

Beth Saunders:

So, Joel, what are the biggest challenges you're seeing for companies right now with components?

Joel Lutz:

I think the biggest challenge does start with that foundational layer. Because we think of companies in today's technology world as knowing all about their data. But I think that's really the exception, not the norm. So, it does start with that. The first challenge is just having that base level of knowledge of the data you have and how you're using it. But overall, coming from the regulations, I think the two biggest operational challenges for companies are around digital tracking, and probably those data subject rights that Gene mentioned. So digital tracking, involves using common technologies online or in your app that automatically are collecting information about users of the site or app. And that's usually done through some kind of tracking technology, like a cookie, a pixel. If it's in an application, it's usually a software development kit or an SDK, as the IT guys call them.

The challenge with these is that they're often invisible to the user. The user is just visiting the website or using the app. They may not know that you're automatically collecting data about them and sharing it with third parties for analytics or for advertising. But what you need to know is as the site owner or the application owner, you're still responsible for that data collection, and use. If you were those third parties that are collecting that data, use the data in a certain way for advertising, or to create a profile, people that is derived from several different sources or different companies websites, then you have to allow those users to opt out of the data.

That's a challenge, right? Because some companies don't even know that they're collecting that data, because the marketing team or the IT team just put these trackers on their site, and for good reason to get analytics about how people use their site, or to advertise to potential clients and grow the business. But you first have to get your arms around that you're collecting that data. Then, you have to tell consumers, you're collecting it and give an opt-out.

So, in today's market, the way companies usually do that is to implement some consent management platform, on their site or in their app. And a consent management platform is really a fancy name for what we usually experience when we're surfing the Internet as cookie banners, right? There's popups that tell you, “Hey, this site uses cookies. Do you want to allow all cookies or some cookies?” Usually, that's a way to tell people we're using these cookies. You didn't know it, you wouldn't know it if we didn't tell you because they're behind the scenes. They're invisible to you. But you have the right to opt out of some of the cookies that share data with third parties, especially for targeted advertising.

Just implementing that operational piece on the web is a challenge because like I said, a lot of companies don't even know that they have that data. Similarly, the other thing Gene talked about was the rights that these state privacy statutes give consumers to ask you, “Hey, what data did you collect about me?” Request that you delete the data or correct the data. So, if you get one of those requests and you haven't done that data management, where you know what your sources of data collection are, where you're storing and processing that data, it can be a real challenge to find out whether you have data about the person that wants to delete it or wants to know what data you have about them, and then implement that action, meaning tell them what data you have about them or delete their data.

Those two things, I think, because they have operational lifts for companies that are built on top of some level of data management or data governance are where we see the biggest challenges because it's no longer about just putting an extra line or sentence in your privacy policy, or just having a privacy policy that has a lot of legal ease. It's about actually implementing operations with your data that respond to the consumer rights.

Beth Saunders:

All good points. Many of our clients have said it's in my privacy policy. So, those are all good reasons to bring that up, put it right in front of the consumer who now has an expectation of being able to opt out should they choose.

Joel Lutz:

Absolutely.

Gene Fishel:

So, I want to pivot in this little last segment. Oftentimes, despite our best efforts, compliance may fall short, whether intentionally or unintentionally. As we alluded to earlier, that can result in class actions brought by plaintiff’s attorneys or regulatory actions by federal or state regulators.

I want to focus a little bit on enforcement and maybe some red flags that companies should be aware of to potentially, and hopefully avoid getting caught up in litigation. Again, whether private or state action. Generally speaking, I'm going to focus a little bit on the CDPAs that have been passed, because that's kind of the elephant in the room and has provided more tools for regulators. And in some cases, consumers on the private right of action side, what's important to know is across these 16 CDPAs, all of them grant enforcement authority to mostly a state attorney general office to enforce and near certain statutory penalties. Some of them in limited circumstances also grant a private right of action. California, for example, has a limited private

right of action in their CCPA, where that can potentially expose a company to again, a class action, or a private suit. So, that can be the basis for private litigation, in addition to general tort theories. But we have also seen state attorneys general start to become active in enforcing these laws.

I'm going to use the first two CDPAs that were passed as an example, California and Virginia they were wanting to. The statutory penalties for violating both of those statutes is $7,500 per violation. That's the statutory remedy prescribed in the statute. There's also injunctive relief that is allowed, which means these state entities can compel companies to make certain changes to the way they operate, the way they process data. We have seen several examples of that recently, in California. There have been notable actions taken recently against DoorDash and Sephora, various other breach settlements that have come out. I can tell you when I was in the Virginia Attorney General's office, and I was handling privacy matters, we would of course, receive breach notices per our data breach notification law. I can tell you that the vast majority of breach incidents occur within small to mid-sized companies. They're not the large companies that you often hear about in the news.

Again, oftentimes, the breaches might involve one person's information, a handful of persons' information, not the million. With some of these privacy statutes on the state side, data breach notification, and the threshold was CDPA. Sometimes it doesn't matter how many people are affected for a regulator to find a statute to enforce whether it's consumer protection, or again, data breach notification.

So, I say all this to remind companies that, again, it doesn't matter the size of your company, it doesn't necessarily matter even the size of the breach for one of these state laws to be triggered, or even one of the federal regulations I mentioned. Now, to kind of wrap up, states get thousands of notices of breaches that they investigate. What are red flags to them? They can't investigate every breach. Most states can't. And the same goes with the federal regulators. There are certain aggravating factors regarding a data incident or a breach that will kind of raise a red flag for a regulator. That'll be one the size of the breach. Again, it doesn't necessarily matter the size, but that's one fact, or the larger the breach might garner more attention.

But beyond size, the type of data involved here. I mentioned sensitive data. If we're talking about children's data, health data, medical data, that's likely to garner the attention of regulators. The population demographic, a more vulnerable population that is affected, say the elderly or children would garner more attention. Even the publicity the breach gets. If there's a lot of media publicity, in some extraordinary circumstance surrounding a breach, that might garner the attention of a regulator.

Again, paying attention to the data points collected and the data points involved and appropriately, consulting counsel beforehand, on the compliance side, but also quickly, should you suffer an incident quickly, alerting your legal counsel to help mitigate the damages, considering all these factors we've talked about today will go a long way towards resolving it. So, with that being said, I want to turn it back over to Aurelia, Beth, and Joel, for conclusion and any takeaways you all might have on what we've talked about today.

Aurelia Lewis:

I think it's a great conversation, quite honestly. I think it's also one that we'll need to continue. Again, I feel like we're just starting even though we've been working on this for a couple of years. I feel strongly that this is just going to be a conversation that's going to be part of our everyday language moving forward. So, I appreciate the time that we've spent together. But I do think we'll be spending more time talking about this and educating our clients about this. I just appreciate what you've done for us so far.

Joel Lutz:

Thanks, Aurelia. We certainly look forward to spending more time with you as well, but hopefully, in a compliant fun way.

Aurelia Lewis:

Yes, exactly.

Joel Lutz:

I think for companies, for small and mid-sized companies, I think the takeaways are first just being aware that these issues are out there. And then secondly, when they're confronting the issues, really, it comes down to asking some of those questions to know what might apply to them, and asking some of those internal questions to know what data they have and how they're using it, because that will be key to figuring out where their risks are and how best to address them in a business forward manner. Hopefully, this helps at least raise those issues and give some guideposts on what to look for.

Aurelia and Beth, we enjoyed having you and working with you. As always, thanks for participating in this podcast and we look forward to tackling these issues with you.

Stephen Piepgrass:

Gene and Joel, thank you for your engaging conversation with Aurelia and Beth. I've no doubt that your insightful dialogue and valuable perspectives resonated with our listeners as much as they did with me. And a big thank you to our audience for tuning in. Remember to subscribe to this podcast through Apple Podcasts, Google Play, Stitcher, or whatever platform you choose to use.

We look forward to having you join us next time.

Copyright, Troutman Pepper Hamilton Sanders 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 Pepper 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. If you have any questions, please contact us at troutman.com.