# Consumer Finance Monitor Podcast (Season 9, Episode 38): The "Confidence Advantage": Why Privacy, Cybersecurity, and AI Governance Are Becoming Business Imperatives

Speakers: Alan Kaplinsky, Greg Szewczyk and Amy Worley

Alan Kaplinsky:

Welcome to the award-winning Consumer Finance Monitor podcast, where we explore important new developments in the world of consumer financial services and what they mean for your business, your customers, and the industry.

This is a weekly show brought to you by the Consumer Financial Services Group at the Ballard Spahr law firm. I'm your host, Alan Kaplinsky, the founder and former practice group leader for 25 years, and now senior counsel of the Consumer Financial Services Group. I am pleased to be moderating today's program.

For those of you who want even more information about either the topic we're going to be talking about today or any other topic in the world of consumer financial services, don't forget to consult our blog, consumerfinancemonitor.com. Since our topic today is going to deal specifically with privacy, also don't forget to consult the privacy blog.

Greg, what is the name of the blog? You remind me.

Greg Szewczyk:

It's the CyberAdviser blog.

Alan Kaplinsky:

Okay. If you want more information, I said you'll hopefully find it on the blog. We also regularly host webinars on subjects of interest to those in the industry. So if you want to subscribe to our blog or to get on the list for our webinars, just visit us at ballardspahr.com.

If you like our podcast, please let us know about it. You can leave us a review on whatever podcast platform you're using to access the program today. Also, let us know if you have any ideas for other topics that we should cover or any speakers that we should consider inviting as guests on our show.

Today, we're going to discuss a topic that's become critically important for every company operating in the digital economy. That is how organizations can build trust and confidence with customers, regulators, business partners, and other stakeholders in an era increasingly shaped by data, cybersecurity threats, and AI.

Our discussion is going to focus on a recently published book entitled The Confidence Advantage: Optimizing Privacy, Cybersecurity, and AI Governance for Growth. The book explores how companies can move beyond viewing privacy, cybersecurity, and AI governance solely as compliance obligations, and instead to treat them as strategic business imperatives that can foster growth, innovation, and customer trust.

The book is available on Amazon for purchase. I highly recommend that if you're interested in this subject, that you, in order to get more information, you ought to consider purchasing the book.

Well, first, I want to welcome our very special guest, Amy Reeder Worley. Amy is managing director of BRG based in Raleigh, North Carolina, and Washington, DC, specializing in helping organizations create value by managing cybersecurity, privacy, and AI risk. She advises senior leaders and boards on building governance structures that drive confidence, resilience, and long-term growth.

She's also the author, of course, of the book we're going to be talking about today, Confidence Advantage. She strongly believes that creating a confidence culture where digital trust is actually embedded in the culture and evidence in daily work drives enterprise value.

Amy, a very warm welcome to you.

Amy Worley:

Thanks so much, Alan. Happy to be here.

Alan Kaplinsky:

Okay. Let me also introduce a Ballard Spahr colleague who has frequently been a guest on our show. He's really not a guest. He's part of our Ballard Spahr law firm, and that's Greg Szewczyk.

Greg chairs Ballard Spahr's Privacy and Data Security Group. He regularly counsels clients on privacy, cybersecurity, data governance, incident response, and the rapidly-evolving legal issues surrounding AI. Greg brings substantial practical experience advising companies across a broad range of industries.

Greg, a welcome to you as well.

Greg Szewczyk:

Great to be back on the show, Alan.

Alan Kaplinsky:

Okay. I have a lot of questions for you, Amy. The way we're going to proceed, I'm going to ask you the questions, and after you respond, I have invited Greg to chime in on anything where he thinks it's appropriate to do so. At the end of the program, I have some very specific questions I want to pose to Greg about your book and the concept.

Amy, what is it that prompted you to write the Confidence Advantage? What audience did you have in mind when you wrote it?

Amy Worley:

Yeah. This was kind of a passion project of mine. While I am an attorney, I have been in consulting since 2019 and work with really where Greg sort of gives the legal advice, I go into the organizations and try to help the clients build the legal advice that they've been given.

I noticed a trend over time, and we're going to talk about this a lot today, of clients sometimes, especially data privacy officers, data security officers, having a hard time getting the CEOs and the board to really understand the value of what they're doing and to fully understand both the risk and the competitive opportunity that compliance in this space provides.

So, the audience of the book is not really, although I invite privacy professionals and CISOs and others to read it, the audience is really executives, and it's intended to inform about the complexities, regulatory, statutory, litigation complexities in this space. And then what is my passion, which is the opportunity to create digital trust to drive organizational value.

There's some good research in that. I'm actually working on my second book, and so I'm still in the research and it's actually growing, that this is becoming a real differentiator for consumers in the marketplace. Do they trust the organization that they're doing business with, with their data?

Alan Kaplinsky:

Okay. The title of your book focuses on confidence rather than trust. What distinction are you drawing, Amy, between those concepts? Why is that distinction important for business today?

Amy Worley:

Sure. Some of it was a little bit of a pet peeve that I've had. As a former chief privacy officer, people would say we're building trust, we're building trust, and I would say, show me. Show me. So in English, this is not true in Latin-based languages, but in English, trust has a connotation of a feeling. I trust my friends. I trust my husband.

Confidence is an evidence-backed belief. I have confidence that my team is going to show up and strive for excellence every day. Why do I have confidence in that? Because I have years of evidence that that's what they do.

So, the distinction that I'm drawing is evidence-based confidence that leads to digital trust, but the focus is on establishing the evidence and not sort of sitting in the loosey-goosey, we want customers to trust us, and getting more into the how and why should they trust us, because we have evidence that we've done the things that we're supposed to do.

Alan Kaplinsky:

Okay. Amy, one of the book's central themes is that privacy, cybersecurity, and AI governance should no longer operate in separate silos. Why does the traditional siloed approach no longer work?

Amy Worley:

Because the data doesn't care what silo it's in. Historically, we built these disciplines up because they were different academic disciplines, different disciplines focused on the personnel in the organization. I'm a weird person that has cybersecurity certifications in addition to privacy and AI, but generally these live in different people. So, we built the orgs around the people.

As we have become a digital economy and as we're becoming an AI economy, the data doesn't care which discipline you're in. It just needs to be governed effectively. So, the point of the book is to create a shared language and a shared risk structure. I'm not trying to get rid of the separate experts. You will still have cybersecurity experts. You'll still have privacy experts, still have AI experts.

But from an organizational change management, risk management point of view, these are all data issues. So, the confidence by design framework is designed to create a common vocabulary and a shared risk structure around the data. Because in the same way when I talk to clients about international data transfers, the data doesn't really care what node it's sitting on either.

So looking at it from the point of view of what is the resource that we need to be taking care of, the resource we need to be taking care of is the data. Thinking about it in silos creates budgeting challenges. It creates operational challenges. Those teams don't always speak the same language.

It's been my experience, especially I talk to a lot of boards, that they don't understand the different languages that are coming up to them are actually talking about a common risk. I give an example in the book where a CEO said to me, "Oh, we're fully GDPR compliant," as if that meant they had no data risk at all.

So, what I'm trying to do is break down those silos and think about data risk as data risk writ large. And then the other side of that coin, data opportunity as data opportunity writ large.

Greg Szewczyk:

Amy, I'd actually be interested to see if you've had similar experiences that I've seen, which is in some ways, the AI compliance piece with some of my clients, especially outside of the GDPR context, has in some ways operated to break down some of those silos, especially for the domestic companies where you see more of that really established silo between the privacy functions and the GRC, InfoSec functions, because that AI piece for some of them forced them to blend together more.

I am fully on the same page with you where breaking down those silos has been really, really helpful because we've seen a lot... The privacy will lean a little more legal in some ways and the InfoSec leans more CISO, IT tech, and they really need to work together. We've seen a lot of synergies form through AI governance. I'd be interested to see if you've kind of been able to leverage the AI governance in the same way.

Amy Worley:

1,000%. What the listeners can't hear is that I was putting my hands up in the air when you said that. Yes. I would definitely echo that that has been my experience as well. AI governance, which is what I'm spending a lot more time on, as I'm sure you are at the moment, really requires cross-functional alignment. So, we've been using the confidence by design framework as a way to just give a shared vocabulary across these functions.

But we're also seeing some, what we call, tech debt, so some delayed cybersecurity upkeep that companies for cost reasons or prioritization had deprioritized. Now that they want to go AI forward, they're realizing that in order to do that, they've got to get that house in order. So, yeah, it's a good time to be in this space because the market is sort of not necessarily forcing, but really encouraging this move and breaking down silos.

Greg Szewczyk:

Yeah. I'm interested to see if we see even more of that outside of just pure AI governance. But as we see laws, like the CCPA have the cybersecurity audit come into play, since we have had traditionally the different legal structure here under the GDPR where things are housed together, just continue to see that trend. But we'll just kind of have to wait and see a bit. But I'll kick it back over to you.

Amy Worley:

I was just going to say, I published a paper a few years ago based on an old Flannery O'Connor short story called Everything that Rises Must Converge.

Greg Szewczyk:

I have that in my library.

Amy Worley:

That's where I think we are. I think you can't really have privacy without security, and you can't optimize AI without both.

Alan Kaplinsky:

Okay. Amy, you referred in your discussion with Greg to the concept of confidence by design. Can you explain that framework for our listeners and describe how organizations can actually begin to implement it?

Amy Worley:

Sure. First, let me say that it's not brain science. What I did is I took the NIST Responsible AI Framework, the GDPR principles, ISO 42001, and kind of put them in a plain language framework of 11 principles. I will say in the second book, I'm updating because as AI has gotten more advanced, I've added an observability prong that I think is really important on the AI side.

But they are a set of positive statements that everybody in the organization can learn that are culture-changing and mind shift-changing. I won't go through all 11 because it would take too long, but examples are we are proactive, not reactive. That's the by design. We're going to build confidence into the products or services that we offer.

One key theme of the book is that I think these are component parts of your product. Whether you sell medical devices or you sell accounting services, digital trust is a component of that. It's a part of what you sell. It's not a compliance bolt-on or add-on. So, we're proactive and reactive. We are positive value sum, not negative value sum.

I would point people to the book for all 11, but it basically takes the GDPR principles for lawful processing and the basic principles for ethical AI puts them in common affirmative statements. They're designed so that an organization can roll them out to everybody. Everybody can learn them.

You don't have to be an expert in any one of them. What we want is for people to just be able to raise their hand and say, "Wait a minute. Do we have an accountable person here? I'm not sure." Or, "Wait a minute. Does this need to be reviewed by our responsible AI team?" We want an organization of issue spotters, not necessarily an organization of experts.

Alan Kaplinsky:

Okay. Based on your experience, what are the most common mistakes that organizations make when they're adopting generative AI technologies?

Amy Worley:

Yeah.

Alan Kaplinsky:

What foundational governance measures should they have in place before deployment?

Amy Worley:

I'm so excited to answer this question because I'm researching it right now. What it's looking like is that the primary mistake is, I call it the FOMO approach, which is to go really fast, implement tools, and then build governance on later.

What we see is a lot of reversals and rollbacks, where a company has gone out with a really bold consumer-facing AI strategy. It hasn't gone great mostly because of process and governance failures. And then, they're having to go back to the market and adjust, retool, recalibrate.

It's really worth it to take a little bit of time and get the governance in place first, because you take a real brand hit and you take a real confidence hit when you go out. Especially with a consumer-facing AI, you have a problem and then you have to roll back. If you had governance in place, likely that problem could have been spotted before it became market facing.

Greg, I don't know about you, but a lot of what I'm seeing is like, let's go really fast and then let's govern. That's not necessarily the best order.

Alan Kaplinsky:

Right.

Greg Szewczyk:

Yeah. I mean, it all depends on, from my standpoint, dealing with so much of the legal team of when they get to get involved, because if they're getting pressure from the business team and they're not in there early, we need the stamp of approval. So kind of building off that confidence and trust, you see these multiple layers of building confidence and trust of the legal team needing to build confidence and trust with the products team so that they can then get that next layer of confidence and trust with the public.

But completely agree that you have these competing forces of you need to build that confidence and trust, but then they've got that underlying pressure of we need to get out there first. It's a tough thing to balance.

Amy Worley:

It really is. The one thing that I really focus on when people are in a big hurry is explainability and now observability as we're going agentic. You've got to be able to see what's going on in your environment and have some feedback loops, so that you can adjust as you're going because nothing's perfect and you are going to have to iterate.

So, you've kind of got to have windows into what's happening so that you can see before your customer calls you angry about something that your AI did.

Alan Kaplinsky:

That raises a question in my mind about how organizations balance the desire to innovate. I mean, constantly, it's the only way you can... Particularly if you're a public company, you've got to be constantly innovating because you've got to come out with new products and you've got to grow by some huge percentage every year.

How do they balance that and move quickly with the need for these appropriate controls and governance? The two things seem to... They don't necessarily work smoothly together. They seem to clash to some extent.

Amy Worley:

I would push back on that a little. I actually go with da Vinci on this. I think that constraints are imperative to art. So, what we say is if you get your governance structures in place and they're iterative and they're working well and they're pulled through, then you move at the speed of innovation.

Confidence by design should be built into your software development life cycle, into your product life cycle, and it should just be a part of the way you work. There are often some stutter steps at first when you're getting started because this is a change.

One of the other problems we see is too much policy and people process and not enough technology implementation. A lot of governance, not all of it, but a lot of governance can be built into the tools. You can build in traceability, you can build in alerts, you can build in observability.

So, making sure that your tech stack has the governance built in will also help you operate at speed. But there are some growing pains when you first get started, but then it should operate as a part of your innovation flywheel.

Alan Kaplinsky:

Okay. Let's get into some practical guidance for our listeners. For companies that are just beginning this journey, where should they start, particularly if they have limited resources?

Amy Worley:

What data do you have and where do you have it? You can't govern blind. I have a cheeky little pirate data map in the book. The illustrations are kind of funny. But whenever we get called into an engagement, I'm always like, "Can I see your data flows and your data maps?" I could say about 50% of the time, I get this really awkward silence.

That's where we start. It's made even more complex by AI because AI often will reach out and find the data that you didn't know you had and then surface it for you and begin to inference on it. So, that's where we start. Where's your data? What systems does it talk to? What are the controls around it? And then, we work out from there.

The other thing I will add is if you are a shop, and most are that are working with AI, then we also start with an AI inventory, what you know you have, and then what you don't know you have and everybody's using behind your back.

Alan Kaplinsky:

Right. Right. Let's talk about the role of boards of directors and senior management. What role do you think they should be playing in overseeing privacy, cybersecurity, and AI risks?

Amy Worley:

At this point, they're all board level risks, and there are different ways. I see more and more boards that are surfacing them just as a data risk, which I love because I think that's the right way to talk about it. But they need to be having conversations with executives about active risk management.

Accountability is crucial. I talk about this all throughout the book to the point that I had some readers send me paragraphs that they'd sent to their CEOs. You can't actively do risk management without accountability. So, what boards ought to be doing is saying, "Who owns these risks? How are we tracking them?" And be looking for reports on what are the cybersecurity

risks that we're tracking right now? What are the privacy risks that we're tracking right now? What are the AI risks that we're tracking? Who owns them?

You're not really doing risk management if you don't have a risk owner. All you're doing is letting yourself know that you're going to have a really bad day. Somebody's going to have a really bad day at some point in time in the future. I tell organizations, if you don't know who's accountable, just ask yourself whose day is going to be ruined when it happens. That is usually the accountable person.

Alan Kaplinsky:

Right. Amy, can you share an example of how a company actually transformed privacy, cybersecurity, and AI governance from a compliance obligation into a competitive advantage?

Amy Worley:

Sure. In the book, I point to a study by McKinsey. I'm sorry, I should have brought my little pile of studies in here with me, but I didn't. But in that case, they did surveys over, I believe it was several hundred organizations, and found that companies who had matured across all three domains were 1.6 times more likely to grow EBIT by 10%. So, there really is a revenue add to doing it.

In my own client base, I don't usually track down to the EBIT numbers. That's just not usually how our engagements work. But I have definitely heard from senior leaders that, oh my gosh, now that we can see, we actually have visibility into our data, our data flows. We have so much more opportunity to use that data for innovation, for creative product design. So, that's kind of how it works.

I mean, on the one side, yes, you're reducing risk. But the way it works on the revenue generation side is if you have clean, controlled, mapped data, then your ability to use it to innovate new digital products is increased. So, that's where the optimization comes from, and AI makes this so much more true than it was five years ago.

Alan Kaplinsky:

Okay. Let's crystal ball. Let's get out our crystal ball, Amy, and let's look ahead over the next five years or so. What developments in privacy, cybersecurity, and AI governance concern you the most? What developments make you optimistic?

Amy Worley:

I'm always optimistic. It is my nature.

Alan Kaplinsky:

Good.

Amy Worley:

What I think is hard and is causing a lot of us to feel a certain level of anxiety about is there's just a tremendous amount of uncertainty. I don't mean to answer a crystal ball question with, well, it's uncertain, because that would indicate that I went to law school. But it is uncertain. Especially on the AI front, we're just seeing different geographies take different approaches.

The Brussels Effect, there's the EU AI Act, they're trying to create a proactive strategy. The US at the federal level has taken the exact opposite approach. We want to be hands-off and allow for more innovation. In Asia, you see some kind of hybrids. China's definitely been very regulation forward.

I'm writing about this a lot in this second book. I really think what this means for business is it's going to be private to private for a while. We're going to see things like ISO 42001, the NIST AI Risk Management Framework, or people aligning to the EU AI Act, although it's not all that specific, to create a private set of standards that will govern business. Because ultimately, even while this space is pretty uncertain, businesses still have to work.

Greg, I'd be interested to hear what you're seeing, but what I'm seeing is the companies are saying, okay, we're all going to align to this standard, even though it may not be required by Congress or legislatively mandated, because we need something we can audit and test against, and this is how we can go forward.

I think we're going to see a lot of private management of things that you would typically think of as regulated because we're in this liminal space, and there's just uncertainty right now.

Greg Szewczyk:

It honestly depends on the industry for what I'm seeing a bit. Especially with the Colorado AI Act coming online at the end of the year, we're seeing some pretty big shifts in the financial services industry in particular.

Amy Worley:

I think that's definitely-

Greg Szewczyk:

Because we're now going to have a state law that's going to apply to the underwriting and major tools that are used in underwriting. So, I think there's been, what I've seen across a lot of clients, a lot of kind of wait and see over the last couple years as to what was going to happen with that law.

As to other industries, I have seen a fair amount of that for the more domestic ones that aren't subject to the EU AI Act. A little bit of watching what was going on with the CCPA, ADMT regs and a little bit of... Maybe we'll peg against NIST, maybe we'll peg against some other private standard, but still kind of figuring it out, like you've been saying.

It's a little bit of private, what can we do on a defensible level if we're going to be coming down against some kind of a negligence standard or some other kind of a reasonableness standard that we're likely going to see in private litigation is how we're going to manage this.

Amy Worley:

I do think that's where it's going. We just have seen in the past month, a bunch of state attorneys general bringing claims. Right now, they're specifically against frontier model developers, but we're seeing those under unfair and deceptive trade practices.

Unfortunately, I'm a little concerned that AI will sort of go the way of data breaches in the US. And that in the absence of a federal standard, it will be, I don't want to say death by a thousand cuts because I don't want to be skeptical of the plan as far, but there will be a, can we tell a reasonably defensible story?

This goes back to the explainability, transparency. Are we making claims that we can defend? A lot of the state AI laws right now are about transparency. Are we telling people when they are engaging with an AI? Are we giving them an opportunity not to if they don't want to?

But for people who have practiced, I think about my husband who's a commercial real estate attorney. The law doesn't change a lot in his land. This is not a space for people who are not really comfortable with change because it changes. I have a regulatory agent actually that runs a regulatory update for me every week just on the Delta over the week.

It's amazing the changes that'll come in just week one to week two. This state has amended this little thing. So, you have to kind of be ready to surf the waves a little bit and understand-

Alan Kaplinsky:

100%.

Amy Worley:

Yeah. It's not going to calm down anytime soon.

Alan Kaplinsky:

Yeah.

Greg Szewczyk:

No.

Alan Kaplinsky:

Yeah. Amy, if our listeners remember only one thing, if there's one takeaway they can have from the message in your book that you've discussed today, what would you want that message to be?

Amy Worley:

It's the confidence in your digital trust as a part of your product, whether you know it is or not. So, I really encourage organizations to be thinking about it. There's research from Harvard Business School, from MIT, from Stanford, from all the big four consulting firms that it is a market differentiator.

So, I think the easiest way to think about it is it's just like the nuts and bolts... Or in the services, in our QC process. It's a part of what you sell and you need to be doing it right to create positive sum outcomes for your customers.

Alan Kaplinsky:

Okay. Well, thank you, Amy.

Greg, I want to turn to you now. I'm going to say to Amy the same thing that I said to you, Greg, when I had the questions I was posing to Amy. Amy, feel free to chime in after Greg responds.

Greg, from your perspective as outside counsel, are you seeing clients move toward the integrated governance model that Amy advocates?

Greg Szewczyk:

Yeah, we are. I think part of it is by necessity of the AI governance framework really does require a little bit of a cross-disciplinary team. Whereas privacy teams and InfoSec teams have been a little more siloed, what we've seen from clients is that the AI governance team is marrying those teams a bit. I think that's better for privacy and better for InfoSec as well.

So, to the extent that you can integrate all of those teams, you're better off as an organization. But at the very least, at least on the AI governance level, we are seeing more of an integrated governance model. I think that's a good thing.

Alan Kaplinsky:

Yeah. Greg, what are the... I asked this question earlier, Amy. What are the biggest privacy and AI governance challenges that you're currently seeing among financial services companies?

Greg Szewczyk:

I think the biggest challenge for financial services companies is what we just kind of touched on in a bit of the radically-changing legal landscape. I mean, we have been watching. At least we've known that Colorado was the one that was coming online, but we didn't know if there was going to be another law that was going to be passed.

California's still in session. New Jersey's still in session. We could have another law that's passed this year that radically changes the landscape for financial services within the next month and not knowing. So, that lack of certainty as to what your regulatory landscape is going to be poses some pretty big compliance challenges and operational challenges.

We've been fairly lucky so far that although there have been some changes, we've at least had an eye towards from states looking for interoperability. Although there's certainly room to complain and financial services companies would always like to have a little less regulation, we at least have had a somewhat uniform-type approach across privacy, across AI governance.

But there's always that risk out there that one state could pass something that's radically different that's out there and send the entire industry into a tailspin, where you have to change your entire regulatory compliance framework. To me, that's really the wildcard biggest challenge out there, is that unless we went to a full federal peremptory model, there's that risk.

Alan Kaplinsky:

Yeah. Well, you talk about Colorado and the other states that are considering bills to add to the Colorado bill. Also, we did a program recently on our podcast show about a project being undertaken by the American Law Institute that's been ongoing for, I guess, a couple of years now. What they're trying to do is deal with... It's a principles project, not a restatement of law, but they're trying to develop principles of tort liability that should apply to AI, particularly generative AI.

And then, we also had, as guests on our show not very long ago, Professor David Hoffman from University of Pennsylvania Law School, and the chair and president and CEO of AAA. They talked about the impact and the concerns that they have about agentic AI in particular and how you deal with that in the contract law, the common law of contracts that we've all been dealing with ever since we started in law school. That has the potential of being tossed into a cocktail, to put it bluntly.

So, there's so much going on right now, and the currents are just swirling around. I think it's going to take a long time for the law to catch up with the developments. I don't know if you share that view or not.

Greg Szewczyk:

I honestly don't think it ever really will catch up. I mean, I think technology will move quicker than the law will really catch up. So, I think we'll be applying legal principles to technology. I don't think that it is too practical to think that you can write hyperprescriptive laws or regulations to constantly-changing technology.

Alan Kaplinsky:

Yeah.

Amy Worley:

Yeah. To the agent contract question, I read a Substack and I was recently looking at decisions in this space. The interesting ones are not in the US yet, because agents are really only a year old in... Not old school, like deterministic bots, but generative bots.

Companies have been raising arguments, well, the LLM decided. It's like, well, an LLM is not a legal person. So, the accountability under the law so far in a Canadian court, a German court, I believe a Polish court, have said no, it's with the deployer. Whoever deployed the agent maintains accountability.

But there've been some very... I mean, we could do a whole nother podcast on agents gone rogue. It's almost like a reality TV show. When you turn an agent loose-

Alan Kaplinsky:

We know that computers hallucinate LLMs all the time. They just make stuff up. I see it.

Amy Worley:

Well, and they follow their objectives. Sometimes, when you optimize for a particular objective, you can have unintended consequences. We had a client who had a call-in agent, like a customer service agent. One of the metrics for call agents was how many calls are you turning over in a certain amount of time. Well, the bots started hanging up on people and having them call back to increase its call metrics.

Sometimes, it's a question of... They're very literal beast agents. So, thinking about what you're optimizing for is just one of the myriad challenges. But courts are really going to be pressed. I took a course in Sweden several years ago about law and AI. I think really just to emphasize Greg's point, what I took away from that was we are going to end up applying old school legal principles to new technologies. You simply can't go fast enough. Frankly, the lawmakers are not technical enough.

So, copyright and IP law will continue to be hotly litigated. Privacy will be litigated in the context of the existing privacy laws. I think AI, it'll be depending on the type of harm. Is it a consumer financial harm? If so, then we would be looking at that set of laws. Is it a personal safety harm? Then, I think we're looking at product safety. It's never boring over here.

Alan Kaplinsky:

That's for sure.

Greg, one of the other things, a question I asked to Amy was what role should boards of directors and senior management play in overseeing privacy, cybersecurity, and AI risks. I want to ask you what you're witnessing. Are you seeing boards and senior management actually becoming more engaged in these issues? Or do you think that organizations still have a lot of work to do in order to get [inaudible 00:45:08]?

Greg Szewczyk:

I think yes to both of your questions there. It depends on the client. But if you take what we saw happen with cybersecurity from the various laws and regulations and in privacy, we will see it be imposed through laws and regulations, that there will be a requirement for board level involvement for AI regulation or in AI oversight. It's just how it will eventually be.

So, the more advanced and more on top of things boards will get involved before they have to from a legal standpoint. That's what we're seeing already. It's not universal. It's not across all clients, but it will get there eventually.

Alan Kaplinsky:

Yeah. Yeah.

Amy Worley:

Also, there's AI insurance now, which is a new thing. With the AI insurance, you're seeing board level involvement requirements there too.

Alan Kaplinsky:

Final question for you, Greg, before we wrap things up. What practical advice would you give companies that are just beginning to develop AI governance programs?

Greg Szewczyk:

I mean, if you're just beginning to develop an AI governance program, you're behind. Not to sound overly pessimistic, but you are behind. If you're thinking that we don't use AI, you're wrong. Your employees are using AI probably a lot more than you know, both officially and unofficially.

When we work through with in-house counsel, we typically find both sponsored ways that they are using it, both in ways that are likely going to be subject to ADMT regulations in the US and through just the everyday employee uses that they probably want to try to get their arms around and confine. So, it is a little too late to be getting into the game, but it needs to be done.

Alan Kaplinsky:

Right. As our special outside guest, Amy, I'm going to give you the last word other than what I'm-

Do you have anything you think that we overlooked or anything in addition to the message you've already imparted to our audience?

Amy Worley:

I'll just say this from the consulting point of view, since I think Greg gave you such good advice from the leg al point of view. One of the things that is often underestimated is the implementation complexity. Getting from great policies and procedures

and great legal advice down into systems is hard and it takes time. Some organizations are equipped. They've got great internal teams who can really turn this into requirements documents and build it into the technologies. Sometimes, people need outside help.

But just don't underestimate if you have your AI principles of transparency, explainability, observability, accountability, all that has to get pulled down into the tools. Having a program that is making sure that you do that can be the difference between defensibility or what we call compliance on paper.

Alan Kaplinsky:

Right. Okay. Well, Amy and Greg, my thanks to both of you for a very interesting discussion today. Amy, good luck on the second book that you're drafting.

Amy Worley:

Thank you.

Alan Kaplinsky:

Let me see if I can summarize for our listeners what I learned today and what I would consider to be the major takeaways from the discussion. Hopefully, I get this right. Let me run through it. There are only a few things, but very important.

First, privacy, cybersecurity, and AI governance can no longer be viewed as separate compliance functions operating in organizational silos. They're increasingly interconnected and they require an integrated governance framework.

Second, organizations should not regard governance merely as a cost center or regulatory obligation. Companies that establish robust governance programs and demonstrate responsible stewardship of data and AI can actually strengthen customer relationships, enhance their reputations, reduce risk, and create meaningful competitive advantages.

Third, as organizations increasingly adopt AI, effective governance must be built into systems from the very beginning. Governance cannot be an afterthought or something that's bolted on after deployment.

Finally, digital trust, or as Amy describes it, confidence grounded in evidence, transparency, and accountability will become increasingly important as customers, regulators, investors, and business partners demand greater assurance regarding how organizations use data and AI.

For our listeners who want to learn more, I encourage you to read Amy's book, The Confidence Advantage: Optimizing Privacy, Cybersecurity, and AI Governance for Growth, available for purchase on Amazon. I want to thank our audience for listening to today's program. Please visit us at consumerfinancemonitor.com for daily updates on developments affecting the consumer finance industry, and be sure to subscribe to our podcast so that you don't miss any future episodes.

Well, until next time, this is Alan Kaplinsky for the Consumer Finance Monitor podcast. Hoping that you enjoy the rest of your day. Thank you.