Reema Moussa 0:00
Hey everyone, welcome back to the Tech Policy Grind. I'm here with the wonderful Lama Mohammed, and we're gonna get into some tech policy news of the week before we dig into our episode for this week which features Foundry Fellow Rebecca Kilberg in conversation with Jeremy Avnet. And it's a really fascinating conversation. They're both technologists deeply steeped in the technical side of this tech policy world. Before we get into that, let's talk about some news. And now is probably a good time to add that neither Lama or I are lawyers. I am in fact in law school, but not yet an attorney. So none of this obviously is legal advice. We're just covering our understanding and take on what is going on in the world of tech policy.

So Lama what's going on in the world of tech policy this week?

Lama Mohammed 1:25
The big "L" lots of lawsuits to say the least. I'm so looking back from last week, we see that the state of Texas has sued Google for allegedly capturing biometric data for millions of Texans without their consent. So essentially, Texas filed a suit against Google for collecting biometric data of Texans without obtaining their consent. The Attorney General filed that suit last Thursday, basically saying that Texans have been barred for more than a decade from collecting people's faces, other biometric data known relating to like their hand features, I think the specific technologies that Texas is suing is related to Google's Nest, Google Voice and Google Photos. So let's get into it. What are your thoughts? What does this mean for the future of lawsuits in regards to cracking down on big tech?

Reema Moussa 2:29
Yeah, this biometric angle is really fascinating, because I think this is the first or one of the first times that we're seeing a biometric suit from a state attorney general without a biometric law, specifically in place like we see in Illinois with BIPA. So it'll be interesting to see the outcome of this lawsuit. And if it inspires any legislation that could create a private right of action, or to what extent various Attorney General's or other enforcement agencies are going to start prioritizing biometrics, but we've seen already that there have been a variety of lawsuits against big tech from Texas and a couple of other states earlier this year. So seems like the trend is just intensifying. And it's gonna be really interesting to watch.

Lama Mohammed 3:40
Yeah, I totally agree. And I also think something that I appreciated in this lawsuit is that the attorney general isn't just talking about the private rights of people that was violated, but also non users, because non users have almost no way to actually opt into consent, because they don't know that their information is being tracked. So you walk past the Google Nest video on the street, technically, your privacy rights violated, you're a non user. And so the extension of

rights is now being given to general society, which I think is really interesting about how this idea of consent and compliance will be interpreted in the future. But I digress. Moving on, sort of similar to the use of ads and tech companies, the state of Pennsylvania just had a resident I believe her name was Ashley Popa, she filed a lawsuit against NaviStone and the Harriet Carter gifts over technology that allegedly enabled online retailers to arrange and send postal mail to anonymous web users after she visited the website. So this was filed under a federal appellate court and not as the attorney general. So how does this sort of differ? And what is the sort of mean for the future of ad tracking companies because their entire business model is reliant on on data, all kinds of data and a lot of it?

Reema Moussa 5:09
Yeah, so this suit is really interesting in that seems to carve out an acceptance for individuals to bring suits against ad tech companies within the scope of Pennsylvania's wiretap law. So we'll see the sort of precedential effect this has for other private right of action suits that come forward in the state of Pennsylvania or within the Third Circuit, more generally.

Lama Mohammed 5:50
Precedent for the future of digital digital advertising, because I think a trend, especially the apple headset with the ability to turn off ad tracking, will greatly affect several major technology platforms, and change the course of the of the entire ad tracking industry. So this is very interesting. Well, we'll see what happens. And lastly, the FTC has taken a very rare and unique step in bringing individual sanctions against the CEO of the alcohol delivery company Drizly, for data privacy abuses, their allegations that the company's security has failed under his watch, and that its expose the data of over 2.5 million customers.

Reema Moussa 6:40
Interesting here that Drizly is actually a subsidiary of Uber, which is mentioned by different FTC officials in their their comments or responses to this lawsuit, and as we know it from just a few weeks ago, the CSO of Uber was held personally liable for his obstruction of justice, with investigations into Ubers security practices, among a couple of other a couple of other allegations. And so it's interesting here how the relationship between Drizly and Uber could be one aspect of why Drizly in particular is coming under fire. But it's also interesting to see that both the Uber case and this case, seem to have pretty extreme disregard for for security, best practices. And I think there's a lot of conversation within the security community of what does this mean for us if we can be, you know, as security professionals held personally liable, because we know that security is not a flawless endeavor are always loopholes, everything is hackable in the end. So how do we how do we deal with the difficulties that that arises? But I mean, it's just interesting to see that from our

tapping around Google can't find any info about the existence of a security team or CSO at Drizly. I mean, could be totally wrong. But that's my guess as to why the CEO is is currently being put under the microscope, in his personal capacity for for failing to prevent the various security incidents that that Drizly has encountered.

Lama Mohammed 9:03
Right. It's it's really interesting, because I'm not even sure the CEO, and I can't imagine is really operating the day to day security endeavors of the company. I'm pretty sure it's a different team. So it's interesting. And I would be curious to see if either this case or the Uber case, do set a precedent for security professionals because as we said, you know, security, it's not a black or white box, and there's no equal equation just to say, Oh, I'm safe. Security is always or really malware ransomware those are really hard things to mitigate and prevent, I think the best thing we can do is try and prevent as much physical harm as possible. For what happened, what's going to happen if security professionals try super hard to mitigate the effects but in the end fail. I think it sort of contrasts this idea of, you know, CISA trying to encourage companies to report as soon as a data breach happens, but then why would they report if they're going to be prosecuted? Like it's all it's very, like the things are on being parallel. And so, you know, that just means that there's more work that needs to be done on the policy level, and really understanding how specific policy affects technologists, which is sort of the overall main theme of our episode today.

Reema Moussa 10:31
Precisely so, with all that news in mind, take a listen to Jeremy and Rebecca's conversation. We hope you enjoy and let us know what you think.

Rebecca Kilberg 10:43
Hello, my name is Rebecca Kilberg, and I'll be your host for this episode. I'm a fellow of the Internet Law and Policy Foundry and a technologist in residence at the Harvard Law Library Innovation Lab. I previously worked for about seven years at a small consultancy, where I worked almost exclusively on federal government software projects as a developer, which is how I met my guest today, the former director of infrastructure at Trust works, Jeremy Avnet. Jeremy has been working in systems and infrastructure for over two decades. Today, we'll be talking about policy from the perspective of technical implementers and diving into examples from our experiences working with federal government agencies. Before I let him introduce himself, I'm going to add a disclaimer: neither Jeremy nor I have a background in law.

Jeremy Avnet 11:57
Hey Rebecca, I've been interested in systems for most of my life, starting with running BBSs as a kid before I could drive and then finding the internet, and eventually discovering the scientific field.

[long pause] Career wise, yeah, for the last 20 years or so I've been doing some version of system administration, which is now called Infrastructure engineering, or DevOps. [long pause] So I've been building and managing systems or building managing teams.

Rebecca Kilberg 12:37
Before we go too much further, can you speak a little bit about what you mean when you're talking?

Jeremy Avnet 12:55
From an industry perspective, most organizations view infrastructure as the creation and management of digital resources. So those are things like computing, storage, networking, and every organization has different needs and requirements around them, some of which are fairly straightforward and some which can be incredibly complex. And healthier organizations, the idea of infrastructure becomes more cultural, as it starts encompassing more roles. It's sort of like going from believing that city infrastructures just about power and water sewer, to realizing it also includes like protective social services, such as firefighting, policing, medicine, if you want a livable city.

Rebecca Kilberg 13:39
So one thing I also wanted to add is you and I have worked a lot in cloud infrastructure, and want to define that term. So people hear about the cloud and it does actually refer to a physical location, or rather many. When people talk about the cloud, they're talking about a large number of machines, also known as computers that users access over the internet. These machines are stored in data centers around the globe. They have software and databases running on them. The differentiating factor in most circumstances between running software on the cloud and running a service locally is that you don't have to be physically responsible for the machine itself. While there are many follow on benefits, such as being able to economize in terms of energies and sharing disk space within machine, the fact is, it's still computers somewhere running code. So when we're talking about cloud infrastructure, that's what we're talking about. Now, let's get a little bit further into how infrastructure developers end up interacting with policy. You can have all sorts of types of policy. There are company policies like at this company we use exe linter are we expect pull requests to be reviewed within 24 hours. That's not what we're talking about. We're talking about government policy, the policies which is sometimes legally binding that you encounter when working in government space. In this context, can you give me some examples of what policy infrastructure policies specifically can look like?

Jeremy Avnet 15:04
Yeah, you'll see a lot of policies around cost control and security, as those tend to be the most scary issues for organizations. So that

can translate into things like how long data is stored, who can access, what resources and at its worst, what technologies you're allowed to use. So for example, in the government work we've done, we'll get different data retention policies, you know, 10 years, seven year, five years, depending on the kind of data we'll be asked to use a service called Gov Cloud, which is physical infrastructure that's guaranteed to be managed by US citizens. So those are some of the way policies will show up.

Rebecca Kilberg 15:44
And what are the some of the common pitfalls that you see?

Unknown Speaker 15:48
in general, the technology and methods we use change much faster than the policies can be updated. So the biggest pitfall tends to be getting a heavily prescribed policy where you end, yesterday's best practice becomes today's technical debt, and then you're beholden to it.

Rebecca Kilberg 16:06
So what do you think is unique about the tech ecosystem that makes it prone to these kinds of issues?

Jeremy Avnet 16:12
I'm not sure there's anything specific to tech beyond the speed at which it moves. I think anytime a field changes, how it does its work, you're going to run into that, for better or worse tech changes it's how on a really high cadence.

Rebecca Kilberg 16:27
One of the examples that you and I have talked about in depth is around DNSSEC in web applications. So even if you haven't heard of DNSSEC, you've probably heard of the technology it's built for DNS, which stands for domain naming system. The metaphor often used to describe DNS is that it's like a phonebook that translates the human readable name that we know like, Ilovedogs.com, which is perplexingly nonexistent to an IP address that the computer uses, so 204.74.99.101. So DNSSEC was created to try to cover up a security gap in the system of DNS. Can you tell me roughly what DNSSEC is and how it works?

Jeremy Avnet 17:15
A big problem with DNS is there's no way to ensure that the data you get back is legitimate. So there's no way of knowing that it hasn't been tampered with somewhere between you and the authoritative server that owns those records. DNSSEC provides a way using encryption to check that the records you get are legitimate.

Rebecca Kilberg 17:34
So I did a little research into the history of DNSSEC in the government space and found some interesting threads. It turns out that

DNSSEC is one of a number of solutions to a long standing issue. What you mentioned that DNS fundamentally insecure. In 2008, Dan Kaminsky, a researcher and white hat hacker, popularized a flaw around what was called the time to live or TTL defense. The TTL defense is the idea that you can prevent attacks by setting a variable to a high enough value to slow attackers enough to render the attack toothless. The flaw Kaminsky exposed, was a particularly effective workaround to the TTL defense, which made DNS suddenly appear much less secure than it previously had. And I say appear on purpose because in fact, DNS had been operating at the same level of insecurity the whole time. This issue had first been reported by another researcher in 1999. So Kaminsky alerted the Department of Homeland Security, as well as a number of industry giants like Microsoft, the issue and he then work to patch it with them. The issue went public in July 2008. And in August 2008, the Office of Management and Budget or OMB released a memo saying that the federal government quote "will deploy DNSSEC to the top level.gov domain by January 2009. And urges agencies to have a plan in place by December 2009 to do so." In August 2018, OMB released a memo with the subject, quote "shifting from low value to high value work" that included that the office was rescinding the 2008 memo requiring DNSSEC because, quote, the requirements in this memorandum are outdated, agencies should already have implemented the security protections. So that's kind of amusing because it's unclear to me whether that means that the agencies have implemented these or rather, that the agencies are simply no longer using a technology that is outdated itself. Also amusingly, we first encountered a policy requiring us to use DNSSEC in 2019. So a year after that OMB memo was released and a decade after its planned implementation. Can you tell me about the situation in which we encountered DNSSEC?

Jeremy Avnet 20:06
We were doing work modernizing the cloud infrastructure for a really large government agency. And one of the basic things we needed to do was to play web applications. Of course, that requires creating DNS entries so folks can reach your app. One of the policies this agency had was that DNSSEC was required. Unfortunately, AWS, Amazon Web Services, the cloud provider they were using didn't support DNSSEC and its DNS service. So they were paying another company to host their DNS records. This ended up entailing a lot of extra work to build out our automation, instead of relying on the tight coupling of AWS services and reusing automation tools we'd already built in the past. In particular, the way the agency was updating its DNS records was by creating PDFs and opening customer support tickets with our DNS provider that usually took days instead of seconds. Now, you should know that one of the core tenets of modern cloud infrastructure is to automate everything you can. So by removing manual steps, you're able to create repeatable, testable and audible infrastructure, we ended up being able to get access to the DNS providers API and build the automation we needed. But it took a lot of extra time. And we lost the ability to do something called auto renewing website certificate,

because that required using the DNS service at AWS. And I can't tell you how many outages I've seen due to certs expiring. So losing that auto renewal was a big loss.

Rebecca Kilberg 21:34
Given everything that you've just described, why do you think DNSSEC was a requirement for this project?

Jeremy Avnet 21:40
Back in 2008, there was a huge problem that was revealed and DNSSEC was one of the contenders at that time as a way to solve that problem. And I think there was a real kind of reactive process that occurred where they're like, Oh, my God, you know, everything's on fire, this is terrible. Let's require this. Thing is, you know, we're 10 years plus past when that policy went into effect, and the way that we verify that the websites are going to now are legitimate, is through the use of TLS certificates. So that's that little lock icon in your browser, when you visit a web TLS sites are very, very ubiquitous, it's very unusual to actually go to a site that's not encrypted at this point. And one of the things you get with that is authenticity that the site you're visiting is the site you think it is. So it really solves the problem of are you actually where you supposed to be? So there's really nothing you're getting out of DNSSEC at that point, because you're already getting it from TLS.

Rebecca Kilberg 22:40
Why do you think that they didn't make a memo saying we have to use HTTPS and TLS.

Jeremy Avnet 22:47
It's really easy to make policies. I don't know what it takes to go and update a policy, how many people you need to talk to how many signatures you need to get, I'm sure it's a complicated thing. And I'm sure they have a lot of other things to do. So how do you prioritize? It's really easy for her to prioritize creating the policy when everything's on fire. But everything's not on fire anymore. What's the motivator?

Rebecca Kilberg 23:07
Yeah, I agree. One of the things that seems to make it really hard is that with the speed of tech developing as it does, flexibility is kind of the name of the game. And that these two kind of capabilities, policy and technology that are in opposition, kind of in a natural tension. And that part of the struggle is trying to figure out a way to make them just rigid enough, and just flexible enough that you can do what you need to do and be responsive, but also have something that you can rely on that has been vetted.

Jeremy Avnet 23:41
Yeah, I suspect it's, you know, there's nothing special here, per se,

about policy. I think, in general, we're really good at adding things to systems and making new things and not so good about going back and removing the things that are longer in use. I mean, there's all sorts of crazy laws still on the books because we don't go back and vet these things later.

Rebecca Kilberg 24:04
Yeah, absolutely. And maybe you're just seeing them in overdrive, but it's not unique to tech at all.

Reema Moussa 24:12
We'll be right back.

For Cybersecurity Awareness Month, the Internet Law and Policy Foundry, as well as the Women in Cybersecurity, Privacy Law and Policy affiliate are excited to present CYBER CON, the Foundry's first ever virtual cybersecurity convention. CYBER CON will take place on Friday, October 28, starting at 11am eastern, and run until 2:30pm eastern. We have a fantastic agenda planned including a fireside chat with Josephine Wolf, who's an associate professor of cybersecurity policy at The Fletcher School of Law and Diplomacy at Tufts University on her latest book, Cyber Insurance Policy: Rethinking Risk in an Age of Ransomware Computer Fraud Data Breaches and Cyber Attacks. You can register for CYBER CON now on the Foundry's Eventbrite page, or just check out the show notes for the link.

Rebecca Kilberg 25:12
We did want to come up with some examples of policy that worked well, for us. One good example, I thought was a lifecycle policy, which is the method that you might use to define how data advances to the various stages of its life. So you'll start with its creation, you'll then probably have some kind of a storage phase, you might have an archive phase, you might then end with a deletion. And most places, and certainly the government requires some level of oversight into that, and some level of automation so that, you know, after a certain period, that the data will be in a specific place, but they don't tell you how you have to do it. So you get to determine that on your own, which works out pretty well. Another example that I have a lot of experience with is access policies, which you also mentioned earlier, specifically, who is allowed to access what accounts so I have seen them work really well, where you have systems that should be only operated by specific people. And you make sure that those people have the right credentials, and that otherwise the system keeps those people out. It's not too dissimilar from people accessing a building or specific archive. It can be intelligent, it can be flexible. But you also can end up with access policies that are relatively punitive. One example of a attempt to create intelligent access policies that went wrong was a security clearance. That meant only three people on a specific team were allowed to deploy their prod, which is the public facing application. And one of those team members rolled off the team,

one went on a leave of absence. And I was the last one and I broke my hand, which made it extraordinarily difficult for a few months for us to manage that service. When these policies are flexible, and you end up with benefits, but you can also end up getting stuck, and questioning whether the security precautions really outweigh the usability that you were you that are essential to the service running. And I know that both of these, one of the things that you didn't love was that they didn't seem unique to tech, they were kind of similar to analog, okay, a lifecycle policy sure you get a paper in, you preserve it for a few months, on the front page, you know, or front shelf of a library, then it goes into the regular connect collection, then it goes into the archive. That's exactly what we're doing. Why is it specific to tech, but I don't know what you think about them now.

Jeremy Avnet 28:03
I think the I think it all feels very similar to an issue that I've heard from a lot of consultants, particularly designers in how they experience some of their client relationships. So often a client will come to you with a solution to build. And what you really want to be hearing is the problem they have, because that ensures the best chance that you're going to actually solve the problem in the best possible way. And I'd love if tech policies were more about sharing the problems to be solved and letting implementers figure out the best way to do that. So I mean, lifecycle policies are a good example of that because they are problem focused, right? They're like, this data needs to be retained for this amount of time. But there's nothing about the mechanism or implementation and how to do that. So like to take the DNSSEC thing again, it would have been, I think, a lot better and you know, hindsights always 2020. But it wouldn't would have been a lot better if the policy was more about authenticating resources, which is the problem they were trying to solve, rather than, hey, use DNSSEC. And that way over time, as technology evolves, you could use the best solutions to solve the authentication problem, which is what TLS is doing for us today with the web.

Rebecca Kilberg 29:16
It sounds like what you're describing is the difference between descriptive and prescriptive policy. And I'm wondering what you think it would look like for that kind of policy to get developed? Where do you think that pilot policy would would originate? Do you think it's possible in our current system to get it?

Jeremy Avnet 29:34
I suspect there's already examples of this. So like the lifecycle policy, right, like, that's a policy that sounds like it's being done kind of the right way. So I bet there's other examples like that, that are perhaps not as simple as a data retention policy. That one might be a little bit of a cop out because it is pretty straightforward, but I think you know, it comes I think it requires, that the policy maker works closely with someone who can understand the demand space. Right?

So, I mean, here's really talking, talking like out there, right? It would be like get a policymaker to work with a designer, like designers know how to ask these questions. They know how to think about how to frame things, sorry, how to frame the problem space to begin with. And it's not clear that a policymaker has that skill set.

Rebecca Kilberg 30:26
Yeah, that seems reasonable to me. And yet, I would suspect that there were folks in the room for the DNSSEC decision, because why else would you end up with something so specific? There's why you create the policy. And it's either you're reacting something, as you said, it's reactive, or it's trying to anticipate something you're like, Okay, we've seen this already, where could this possibly end up? And we don't really necessarily understand, we understand parts of it. And we have this person here who's representing parts of it. But of course, it's incredibly complex, and gets only more complex as the internet grows. And we have to try to figure out something that's smart enough to keep us in like a safe box. But the reality is, we're not going to be able to stay in that box. And so what we should be thinking about is what the path looks like that we want to walk down with this kind of thing. And what are really important pieces that have to stay fundamentally secure. And I don't mean secure as in like security, I mean, secure as in stable. And what are the pieces that we can be loose on that we can try to use our imagination for?

Jeremy Avnet 31:36
I think that way of thinking is not it's not easy. It's hard, right? Not everyone has that skill set? For sure. Right, in some ways, using an intermediary would be great. I don't know how reasonable that is. But there are people trained right to think about the bigger picture, right? And to think about how, like the ramifications of the solutions. I mean, again, like the DNSSEC thing also might be suffering from the everything's on fire, quick put it out problem, right. Like when that when that came out. It was big, it was big news and front page of, you know, mainstream news sources which is very unusual for anything like a technical discussion about like internet underpinnings, right? So I think is a very particular thing. And so it was, I think, was extremely reactive process that probably went through and who knows who was involved, someone's butt was on the line is how it feels right. And so choices and decisions were made. And the policy was put out, and the checkbox was checked. Right, which is, I think one of the biggest problems we see in a lot of government work with a lot of government policies is it's become over time, or maybe even at the beginning, right, it becomes a lot less about doing the thing, or achieving the goal and a lot more about checking the box.

Rebecca Kilberg 33:00
One of the hurdles that we often faced was this question of compliance or security, there was a huge compliance element to a lot of work that was claimed to be security work. And what that meant was typically,

these very prescriptive policies of your logging needs to look like this. It needs to use these tools. It needs to be queryable in this specific way. When we were going well, really what the underlying question is around logging is, can I see who's in my system? Can I see who's done what, and that could end up looking at any number of ways, but having to do it, according to these specific rubrics really hamstrung us and sometimes forced us into making decisions that we often would not have otherwise made.

Jeremy Avnet 33:48
We have examples of being asked to make the system less secure or more insecure, in order to follow security compliance rules that did not make any sense in the modern infrastructure landscape anymore. One of the policies that we started to deal with was around software that was installed on computing instances, like things to do like virus scanning or checking about, like what is running on the system—

Rebecca Kilberg 34:20
Just to clarify briefly before Jeremy goes any farther. So when he's talking about a competing instance, you can just think about it as a computer, just some machine that we run things on.

Jeremy Avnet 34:29
Yeah. So one of one of the things that's changed in the industry over time is, you know, it used to be that we would run these computers for long periods of time, right? They would stay up for days or weeks or months or whatnot. And what has happened is we've moved to a much lighter weight computers, we could barely even call it a computer where it's only running a single piece of software with very few libraries and other things running with it. And they only run for hours or even minutes before they're thrown away and a new one is spun up. It's it's a completely different model of how we think about computing resources. And so being asked to add things into these, like virus scanners or things checking for, you know, what other kinds of running processes were there, starts making a lot less sense, and in fact, starts to reduce the security of these things.

Rebecca Kilberg 35:22
One particularly egregious example that I remember was, we were experimenting with making these containers where no one could get in, they couldn't be accessed by anyone or anything. And one of the things that we were asked to do was to make them accessible in order to add these things in order that we could check that they weren't accessible. And it was like, the whole point is that they're not accessible, we're being forced to make them accessible in order for you to check this. And it was completely antithetical to what as you say, the architecture achieved itself.

Jeremy Avnet 35:57
This also made me think a little bit about something else, I'm

realizing about the DNSSEC issue that I have questions I have big questions about, I think it came out of a very reactive, you know, place, right. But I think something might even reveal that more is the thing about DNSSEC, which we didn't get into, right, is DNSSEC is you can't just like, implement it. Right? It requires two sides, both sides to be using it. Right. So it wouldn't matter if the entire government used DNSSEC, and all of its records, if none of the clients are using DNSSEC to actually verify those records, right, that you've gained zero, you've done all the work and gotten nothing, which is a lot of the issue today is is most people aren't using DNS resolvers that actually check DNSSEC records. What's wild to me, then it given that and they knew that back then I mean, that's that's part of the system, there was nothing to check in on it, right? It's just like, here have a policy to do all the work. But there's like there was never anything about checking in to see whether it was effective, whether or not the client side ever reached a place where the DNS records were actually being checked. Like, like, there was a huge missing piece of the puzzle. Right, which I think is very revealing. I don't know if it's revealing about this particular instance, or revealing about policy in general, right. Like how often and this is, this is a thing that I feel like we're only recently coming to in general in our modern era, right. But the idea of like measuring the results of the things you've decided to do, right? Is there is that ever happen? Like? Like, do we ever see laws or policies where part of the policy is about like, the effectiveness? Yeah, I mean, there's maybe this is like an incredible example, right? There's so many problems here, or there's so many question marks around this policy.

Rebecca Kilberg 38:06
And I mean, it's sad, because there's all this effort and money, that the whole point, the whole intent is, we want you to feel safe using our services. It's important there are government services, you are you have right to access them you have right for this information about you to be saved, you have right to know that this is a trustworthy source that you can enter in information like your social security number and not have it be blasted across the internet.

Jeremy Avnet 38:35
And we do because we use TLS certs like we have it. We have solved this problem.

Rebecca Kilberg 38:44
Well, Jeremy, thank you so much for joining me today for this very interesting conversation.

Jeremy Avnet 38:50
Thanks, Rebecca for having me.

Rebecca Kilberg 38:53
Bye bye!

Jeremy Avnet 38:53
Bye! [laughter]

Reema Moussa 38:59
That's it for this episode. Hope you enjoyed and we'll catch you next time. Huge thank you to Lama Mohammed, our Social Coordinator, and Allyson McReynolds, our Accessibility Coordinator. for all their help in making this episode happen.

Transcribed by https://otter.ai