TECHNOLOGY
POLICY
INSTITUTE

TPI SPECTRUM SERIES 2024

Growing Threats to Wireless Communications and How to Address Them

2001 L Street NW ● Suite 500 ● Washington, DC 20036
Tel: (202) 828-4405 ● Email: info@techpolicyinstitute.org ● www.techpolicyinstitute.org

Scott Wallsten:
I'm Scott Wallsten, president of TPI. I'll be moderating this fireside chat, which is part of TPI Winter Spectrum Series. Our guest, Dale Hatfield, needs no introduction, but I'm going to give one anyway. Dale has a storied career over his more than 70 years of experience in telecom policy and regulation, spectrum management and related areas. He's currently executive fellow at the Silicon Flatirons Center for Law, Technology and Entrepreneurship and an Adjunct Professor in the Interdisciplinary Telecommunications Program, both at the University of Colorado at Boulder. But before that, he did almost everything else you can possibly imagine in this field. He was the chief of the Office of Engineering and Technology and chief technologist at the FCC. Before that, he founded and ran Hatfield Associates, a multidisciplinary telecommunications consulting firm, and before that he was acting assistant secretary of Commerce for Communications and Information and acting administrator of NTIA. And before that he was chief of the Office of Plans and Policy at the FCC. He was also the founding executive director of the Broadband Internet Technical Advisory Group.

Scott Wallsten:
He's currently serving on the FCC's Technology Advisory Council and on the Commerce Department's Spectrum Management Advisory Committee. So to summarize all that quickly, in case you weren't paying attention, he's been at OET and OPP at the FCC, AAS, and CCIA at NTIA and DOC, as well as the ED at BiTAG, FCC, TAC, and CMAC. So I think he's got all the acronyms that you could possibly have. But what that really means is that for more than half a century, Dale has been the reliable, thoughtful connection between policy and engineering, helping generations of people understand what spectrum is, how wireless technologies work, and how policies interact with those. Dale, thank you so much for joining us.

Dale Hatfield:
Thank you very much, Scott, for the very kind, generous introduction. And thank you also for asking me to address the topic of growing threats to wireless communications and how to address them. If you would permit me being at my age or voice like to tell a story. So if you would allow me, I'll tell a story here quickly of how long I’ve been involved.

Dale Hatfield:

I was a ham radio operator 70 years ago. Some of you may know the amateur six-meter band is directly adjacent to television channel two. And so when I got my license and went on the air immediately almost our neighbor called and said to my parents, your son is disrupting our TV. Now, this is back in the over-the-air days. And the problem was that I had a high-powered transmitter and some of my energy was spilling over into channel two. And I'll try to use kind words here. The receiver manufacturers had really skimped on the performance of the receivers, so they were receiving a lot of my energy outside the band that they were trying to receive, which was channel two. The kind of funny part of it is there were solutions. You could buy a filter that went on a TV set that filtered out the signals that I was transmitting, and that was a fairly cheap small device.

Dale Hatfield:

But since I was operating high power, I had to have a great big filter that prevented me from slopping over in there. And when I sit and listen to discussions today, boy, we still got some of those same discussions where we want to pack more people into the spectrum. But you got these sort of adjacent band or adjacent channel issues. So thank you for allowing me to divert to–

Scott Wallsten:

Could I ask a follow-up question on that? In that example, did you end up with a Coasian solution where the two of you were able to come to some agreement, or was there an external government, like your parents? .

Dale Hatfield:

Yeah. They said get it fixed. And no uncertain terms. So I think I used some of my grass mowing money or something to buy the parts necessary for them and for my transmitter.

Scott Wallsten:

Well, early, early policy interventions.

Scott Wallsten:
Okay. So let's move to what our actual topic is. Tell us, you know, wireless wise, what keeps you up at night.

Dale Hatfield:
Well and preparing I, I picked a total of eight threats and some potential solutions. And we can talk about them more or less as you may see fit in time allowed. But my first concern is the jamming, spoofing, sniffing, and unauthorized interception of radio frequency or RF signals. That's what really keeps me up at night. I could give you some recent examples, but people do not appreciate as much as they should, that wireless is inherently open, and we can explore that a little bit if there's time and energy. The second area that I'm particularly concerned about is RF pollution, when the spectrum is becoming polluted from a whole host of different sources. I'm concerned about one particular type, which is the use of what's called switch mode power supplies. But if you look at it in my mind, the fundamental role of the FCC, of course, is to protect—kind of an original environmental protection agency.

Dale Hatfield:
They need to protect against pollution. And then there's enforcement. This is my third point. Enforcement challenges associated with detecting, classifying, identifying, locating, reporting, mitigating, remediating and reporting interference in the sort of jamming and spoofing examples that I gave a moment ago. I can hear again, I can go through those a little bit more, but just to pick the first one before you can do anything about interference, you have to detect it, and it may be the signal may be of such a design is very difficult to detect, yet causing problems.

Scott Wallsten:
Before you talk in more detail about the ways to to address the threats, could you define what these different threats are because they're different jamming, spoofing RF pollution or, you know, they're not all the same thing and they don't necessarily have the same solutions. And for a lot of us, we just don't know what the difference is between those things.

Dale Hatfield:
Basically, jamming is putting a signal out. Nefariously, a signal out that prevents somebody else from receiving their intended…The example of jamming would be a schoolteacher who says, I don't want my kids operating. I don't want my kids using their phones in class. Therefore, I'll go and you can do a quick Google search and you can find jammers. And then he or she would jam the signals. Well, the problem is of course, that prevents the parents then from calling and checking on their children. The person in the next classroom might be jammed as well. So that would be an example of jamming. And we can go through the list. It can be done for very, very bad reasons. Or it can be young people at university saying, "hey, wouldn't it be fun to jam the parking lot control signals so that you can't open the gates after a football game." And I'll do it for bragging rights.

Dale Hatfield:
So that's the jamming. Spoofing, of course, is pretending you're something else. This happens in GPS. I'll send a signal that looks like a legitimate GPS signal, but it's really not. It's a GPS signal generated by somebody who wants to destroy your ability to find your position, to get precise timing, or for or for navigation. So the GPS, GNSF more broadly, that's an excellent example for spoofing is a problem. Another one that is, when you're using your cell phone, you assume you're talking to the carrier's tower. You may not be. And this is what they call the man in the middle of attack. Somebody is in there between you and the legitimate tower and can then extract certain information if they want you finally sniffing or an unauthorized reception comes about, for example, I can learn a lot by just seeing how you operate your system, I just observe you.

Dale Hatfield:
And when you react to some sort of interference. Because what do you do? So I can learn about your network by just listening to what's going on. And there's other examples too, of where, where you use, sniffing and attempt to learn a similar sort of thing. One of the things, of course, it helps you learn how to do a better job of launching jamming attacks and spoofing attacks, because you've learned a lot about the network by passively listening. And I think I well, I hope I made that point clear.

Scott Wallsten:
So those are those are all on the malicious side of of potential problems. In the previous panel, we had people who disagree on lots of aspects of spectrum, whether unlicensed, exclusive licensed, how to decide what, how much spectrum federal agencies should have as opposed to the private sector.

Scott Wallsten:
But I would think they all agree on the potential problems and harms you're talking about. And you think that they would put a lot of effort into dealing with them. Are you concerned that the efforts have not been sufficient?

Dale Hatfield:
Quickly going back to the seven steps in enforcement that I talked to him. One you've got remediation. You want to stop what's going on. You want to stop it right away. So you need to have action. And then if you're going to remediate, if you're going to, you want to put somebody in jail. Ultimately here these can be bad people. So you need to put them in jail, which means you have trails of evidence issues and so forth to make sure that you can successfully prosecute somebody or if it's a more militarized condition, that you can know more about what the enemy is trying to do. Was I clear on that?

Scott Wallsten:
Yes. I guess I'm wondering, though, if when you when you've talked to people who run these networks and read about examples of where these things happen, if you think that they or, and, and/or the government are not currently doing enough because you think they would worry, they must it must keep them up at night, too.

Dale Hatfield:
Well, I'm not a lawyer. So I don't know, but I don't think Verizon has the authority to tell somebody to turn off their transmitter. I think that ultimately falls upon the FCC’s responsibility. Now, here again, I'm not a national security expert. There may be other things going on here. There are certain volunteer groups, like ham radio operation stuff that do a little bit of this sort of

stuff, but that's the thing. It has to be somebody with the power of government to shut things down. I mean, just think of it here in my house the other day my network went down and trying to figure out, is that something serious? Who did it, where is it located? All that sort of all that sort of thing is a very difficult, time consuming battle.

Dale Hatfield:
And it's not clear to me who has those responsibilities, especially when it's nefarious. In other words, it's intended, you know, it's like the example of the kid, hey, I'll take out Hatfield’s Wi-Fi just for the fun of it. So, there has to be ultimately, I think a strong government. And to be provocative, the FCC enforcement equipment, their enforcement network, the sites that they have to be able to track down some of this stuff is very limited. If you have something that happens to the ground communications at DIA Denver airport, you know, they're close by. But if you're up in Wyoming someplace, it takes forever to get up there and try to get it stopped. And meanwhile, there could be bad things happening. So in my opinion, the whole enforcement structure needs to be improved significantly. And, you know, of course, hopefully with the cooperation so forth of the other players, the commercial providers and DoD, etc., you were talking about.

Scott Wallsten:
That's interesting. So enforcement, this kind of enforcement, you think has not kept up with the extent to which wireless has become prevalent.

Dale Hatfield:
They chase pirates up here in the mountain, of course, or pirate radio stations. So they spend a lot of time chasing pirate radio, which is, you know, I'm not saying that's not important. It is important, but it's not the sort of thing that we're talking about here.

Scott Wallsten:
Right? I may or may not have a cousin who ran a pirate radio station. Um, yeah. So.

Dale Hatfield:
But think about it. Just above me here we have Boulder Canyon and the big Dam, Barker Reservoir and Big Dam up here, and that's being controlled, of course, by radio signals. Now, it can be jammed or spoofed or all those sorts of things as well. And that gets into protection of the national infrastructure, the water system and all the other things. Is that being protected adequately? Does the government have the ability to make sure that they can get it stopped or mitigated?

Scott Wallsten:
Let me ask an engineering question, I guess, and I don't know if there is an answer. But we also read about these sort of malicious attacks in war zones in Ukraine and, and so on where drones are misdirected.

Dale Hatfield:
Yes.

Scott Wallsten:
And obviously the FCC can't [do anything]. That's not the kind of thing you can enforce with a law. How do you protect against that sort of thing? How is it possible?

Dale Hatfield:
Well, when you talk about the drone situation. If I have one message, one single message is that wireless systems are inherently open, so you can't get ultimately, you cannot really protect against that. I've lost your question mark.

Scott Wallsten:
That's fine. I mean, I think that that's an answer. I was asking how you would deal with that in a war zone where they're not necessarily rule of law and enforcement, but you have to figure out a technical way. And I think your answer is that it's impossible to completely guard against it.

Dale Hatfield:
There is an example of, in California, there was a guy who deliberately was jamming all the police radio systems and cellular systems from a location and you can get a little bit, even though the local police probably don't have jurisdiction to stop the person you know, showing up at somebody's door with the gun on your hip does have a certain deterrent, a deterrent effect. And that leads to a more serious question, since the interference sometimes occurs at very local levels, should we try to give some sort of enforcement power locally? So you've got help closer to the source of the malicious interference, for example.

Scott Wallsten:
Now there's of course a whole other type of threat, which, innocent might be the wrong word, but not malicious. Talk about those a little bit. Also I should add in the Q&A which people should remember has a rhetorical question, which is how did so much knowledge and wisdom end up in one person? That would be you.

Scott Wallsten:
And then the second question goes, is what should we do about receiver standards?

Dale Hatfield:
So. Well, Preston, thank you for the softball question. Of course, you know, you can have millions of millions of transmitters and they don't interfere with each other when they're out in the ether, so to speak. The problem comes when you put the first receiver out. It has to sort out from all those transmitters signal to get the desired signal that they want. That's where that's where the problem, that's where the problem occurs. And it's just so clear that if we're really going to go to more dynamic spectrum, ways where we are much more dynamic in spectrum, yeah. Just have to do something about the receivers. There's just no question. I have heard very informally recently that the chairwoman is going to maybe step up a little bit at depth looking at the receivers.

Dale Hatfield:
And I think that's a very, very wise step. But I've been saying that for a long time.

Scott Wallsten:
Well, at least since you were a ham radio operator. And your neighbor.

Dale Hatfield:
Exactly. Yeah. Exactly right.

Scott Wallsten:
So but so I interrupted, unfortunately. But you know, talking about the innocent threats.

Dale Hatfield:
The innocent threats, of course, or things like mistuned transmitters. That's an example. Why do people do this sort of stuff? Well, for financial gain, I said pranks. I used the example of teachers or, or theater owners. They put in jammers so people's cell phones don't go off in the middle of an event. So those are sort of non-malignant. Again, there's no bad person. They're not doing it to prevent you from checking, you know, where your child is or something like that cell phone.

Dale Hatfield:
But the result, the extra exposure, I suppose you can say the economic term, there's an externality here.

Scott Wallsten:
I assume it’s always illegal though, right.

Dale Hatfield:
Yes, yes. That's very, very clear I think statutorily jammers. But there's been some challenge, not challenge like prisons because prisoners were using cell phones to coordinate drug trading activities outside. So there was a proceeding regarding the use of jammers by law enforcement people for the limited purposes of. But here again, how the law gets waived in that case and so forth, I hasten to add, that I'm not, not, not a lawyer. If you, you know, go ahead. I'm sorry.

Scott Wallsten:
No, go. Go ahead. Continue. Especially you talked about switched mode power supplies. And again, that's something that, you know, you need to explain that a little bit. Yes.

Dale Hatfield:
By the way, if you're sitting near a computer you can just type in into Google the advantages and disadvantages of switch mode versus linear power supplies. But the thing to keep in mind, the basic sort of kernel here is when you, when you change the direction of—let me say—radio waves are generated by moving electrons, by electricity, moving very fast back and forth. And what we're talking about here is the switch-mode power supplies. The switch mode power supplies essentially chop up the signal that you're trying to send and convert into a very, very broadband signal. And you would say, why the heck would you do that? Well, it turns out that they're much more efficient. They have much better control circuitry, so you don't overcharge your whatever device it is. And to bring this home to be personal about it, my wife is disabled and uses a scooter. Electric scooter. And the latest one we bought, what did it say we're using we're using this modern switch mode power supply. So what they're doing, they're chopping up.

Dale Hatfield:
They're chopping up this voltage from the batteries. And they got much more powerful. So it doesn't overcharge at night. So it makes sure it's charged in the morning and does all of that. But the price of it is the tradeoff that I don't think is being recognized is that that pollutes that causes serious pollution of the in my mind at least, the potential for even worse. Even worse is the EV charging stations. Now, you're not just turning on and off a little bit of electricity like my wife's wheelchair. You're turning on and off at very high speed, if you will. Very, very high if you're trying to charge a truck, for example. These are huge things that are generating interference. And I don't think we've seen the worst of it. For example, the studies in California that I've seen so far, where people pull up to a charging station and it says not in service. Well, my feeling is in some of those locations anyway what it is, they are essentially blasting out huge amounts of this very rapidly changing voltage.

Dale Hatfield:

A colleague of mine wrote a paper essentially saying VHF is dead. And you say, well, who cares about VHF? Well, you look at it, there's all kinds of very important military, state police. There's all kinds of people in this VHF range that can be affected. And as we add, keep adding, you know, you have an EV station that has ten places to park today, tomorrow it may have 30 or so. And then you get into the issue of accumulated interference. People told me, well, there's rules against incidental radiation. And I say that's true, but that doesn't mean that they're adequate. When you have, you know, thousands of them or hundreds of them contributing to it. So there's that, that issue as well.

Scott Wallsten:

So if I understand it's the constant on and off of the power that creates RF interference. And the higher the power levels, the greater the interference. Um, and so is this something that you can, if you take your phone or you're trying to use a Wi-Fi signal near, let's say, a Tesla Supercharger. It's noticeable. You can see interference.

Dale Hatfield:

Well, the evidence is largely anecdotal. And that goes to a point of the FCC, in my opinion, should be taking a look at this because some of these systems coordinate the chargers using Wi-Fi, for example, that's unlicensed or not entitled to any protection. Wi-Fi, as we know, was never intended for that sort of serious use. So right now, when things are out of service, it may be because of this issue. More to the point, it's crying out here for the FCC to have more capabilities working with DOT or whoever it is to see what the facts are before it becomes so bad that it becomes almost impossible to handle.

Scott Wallsten:

So your point is, isn't that we don’t know that this is necessarily a big problem, but it could be. And they're ignoring the possibility and it needs study.

Dale Hatfield:

I would go beyond that. I would put my engineering reputation on the line and say that some of the problems we're having at these charging stations are due to interference to Bluetooth or whatever. Now, some of course, connect to their ISP. I don't know, maybe Tesla uses a fiber optic cable to connect, in which case they don't have the problem, right? Somebody else can't afford to put in fiber everywhere and instead uses radio. They're going to they're going to be subject to the sort of contamination I'm talking about.

Scott Wallsten:

And I'm sorry if this is a silly question, but, you know, often the problem, as you said, or implied, is with the receivers. In this case, the power is acting as a transmitter. Is that so? But so, so in this case, though, it's the transmitter that needs some kind of filters or I don't know, how do you like, what's the what's the answer?

Dale Hatfield:

Do you remember? I think probably in some of the movies the radio operator was called Sparks? Why was he called sparks? Because he generated rapid changes in electricity. The very first transmitters were the spark gap transmitters that generated sparks. And that's what we're, doing here. Can you filter some of it? You can improve. But here again it's wireless. Remember this is a wireless system. You can't make it entirely. You can't get all the results—from an economics term. We may know what the solution is but can you afford to do it? And we haven't talked about LOT devices and very small devices that don't have, you know, intelligent capabilities to try to avoid interference. So this is a tough problem.

Scott Wallsten:

Well, also on M*A*S*H, Klinger and Radar were always calling Sparky to set up the telephone connection back home. I never knew why [he was called Sparky] until now.

Scott Wallsten:

So what are possible solutions to this? It sounds almost intractable.

Dale Hatfield:
I try not, in my old age, to press, but. There is one thing I haven't mentioned on the enforcement side that could be helpful. Now, this is not a panacea. It's actually rather narrow. And that's called RF fingerprinting. It turns out that every transmitter, every transmitter built by whoever has a unique signature. In other words, I can identify the transmitter by the fact that no two transmitters are exactly the same, just as no two people's fingerprints are the same. This is based upon manufacturing variations. Manufacturing variation. So if I have, for example, a whole bunch of drones coming in may want to attack or cause all kinds of problems, I can, in advance, put in the devices that I know should be there and if there is one fingerprint that doesn't match, then that's one we better go after. And we talk then about going back to jamming or something about some way of taking out that, taking out that particular device.

Dale Hatfield:
And there's a lot of other uses for that here. Again, going back to the remediation phase of enforcement, I want to put the person in jail. Now, I don't know whether before I didn't know, I couldn't prove in court necessarily that it was you actually doing it with your transmitter. Now, I could say this is Scott Wallsten's cell phone that did this.

Dale Hatfield:
So, so anyway, it's a powerful tool, but it's it's rather narrow, but, and there's quite a bit of research in fairness, there's an awful lot of research going on in this area because the identification of because of the identification of the actual device is important. Now, of course, my students would immediately put their hands up. Well, professor, Professor Hatfield, that has all kinds of privacy implications, doesn’t it? And indeed, indeed it does. Interesting. Another trade-off? Yes. Another trade-off. Exactly, exactly.

Scott Wallsten:
I was going to say that this is a good place to talk about where you see reasons for optimism because you sounded like you started down that track and until you pointed out the downsides, the privacy implications. Do you see reasons for progress or optimism in these issues? I mean, you mentioned one. And so that's I mean, the research is good.

Dale Hatfield:
Yeah, what Scott are you saying? The answer is money. What's the question? Right.

Scott Wallsten:
Yeah, exactly.

Dale Hatfield:
And, they're saying it's the periphery. Periphery? One thing is, I don't think we do enough risk assessment. Scott, you may know much more about risk assessment than I do. We have. We have risk-informed interference analysis where we can't solve all of these problems. But what you do is try to go after the problems, like opening the floodgates up here on the dam and letting the water, and you go for the really big hits.

Dale Hatfield:
And if it's just the kid interrupting my Wi-Fi, you kind of let it go. And by coming up with a list of the types of attacks and their impact, then you can do a much better job of taking a society's scarce resources and devoting them to where and devoting them to where they can do the most damage, build in the most resilience.

Scott Wallsten:
And so where would you like to see? Um, what would you hope to see in the next 5 to 10 years? These issues.

Dale Hatfield:
Well, one of the things is more information to help researchers like me being self-serving. I would like to. And I realize there's reasons, you know, you don't want people to. As the last panel says, some people to know certain things and so forth, but we don't report well enough incidents like the incident in California with the Walnut Creek, where the guy was deliberately. We don't have, in my opinion, a good now on GPS and GNSS. There you can find lots of reports on that,

but in general, it's very difficult to get the research information to be able to do the sort of risk informed interference analysis and so forth that I, that I'm talking about.

Dale Hatfield:
So I think reporting is so critical. So did I. Am I ducking your question? I don't mean to be ducking it.

Scott Wallsten:
No, I don't think so. It's hard to study something without having any data for it. So that does seem like a good place to start by getting it.

Dale Hatfield:
I don't know what your protocol is, but I would invite questions or challenges to things that I've said. So what's the process for doing that? But I would love to have people say, Hatfield, you're all wet, you know?

Scott Wallsten:
Well, people can type that into the Q&A if they want to right now. And we had some questions that we answered. People should feel free.

Scott Wallsten:
But if not, you know, I guess I assume you're open to emails. Absolutely.

Dale Hatfield:
Absolutely, absolutely. There are people that Dale.Hatfield@colorado.edu.

Scott Wallsten:
Preston raised his hand again. I'm not sure how to call on people. Maybe you could type his question in. Wait. No. I can allow him to talk. Hold on. Let me see. Okay, Preston, I believe I think you're on.

Preston Padden:
Can you hear me?

Scott Wallsten:
Yes. Yes we can.

Preston Padden:
My question to the great Professor Hatfield is. Demand for wireless data is going up like a hockey stick. And I sometimes worry about what we do when there just is no more spectrum to allocate for, for that demand. But in particular, we often use our scarce wireless spectrum for the carriers to send millions of duplicating streams of the same content or same data to millions of people simultaneously. And are there more efficient ways that we can? For example, I'm out.

Preston Padden:
Take the most extreme example, the Super Bowl. I mean, probably more than 100 million identical streams eating up spectrum with the same content at the same time. It just doesn't seem very efficient. And I'll stop there. Thank you, Scott and Dale.

Scott Wallsten:
Thanks, Preston. Dale, do you want to reply?

Dale Hatfield:
Well, this is an art. This is an area that's here again. Been around forever. If you're for example the police. You may want to send a message to everybody, all the police on the beat. Or you can send it to just one. And there's always trade offs. There are trade-offs here depending upon the traffic, some traffic you do want to express, and was saying some you do want to send simultaneously the same information. Others you want to be selective about it. So I guess my only point is this. This is not a new issue, and it's the sort of thinking we have to be doing to cut down on the cuts, to cut down, to be able to do more of the dynamic spectrum sharing that we've, that we've talked about.

Scott Wallsten:
So we have another question from Tim Brennan, who has been chief economist at the FCC. He says, “hi, Dale, with the current administration's considerable effort to encourage EV adoption and build more charging stations. How aggressive do you think the current FCC will investigate the problems with EV charging that you described?”

Dale Hatfield:
I think first of all, they don't plan just don't have the resources, the technical resources, the equipment needed to make the and these people are very highly paid people. So it's also there's probably issues on the on the hiring side. There is some encouragement. I think DOT is looking at some of this. But I go back to the inherent sort of thing. Jurisdiction seems to me to lie with the FCC. So DOT I think should be cooperating, that they should be making some of these studies at these very high, high power charging stations. But the Commission ought to have the or somebody it maybe we need oh my gosh, a new agency or something to try to.

Dale Hatfield:
[Laughter] I didn't really mean that. I take that back to look at, but I think, I think genuinely it's my professional opinion that the, that the, that this is one of the externalities of our conversion to renewables.

Scott Wallsten:
So let me put you in the impossible position that Chairwoman Rosenworcel would be in if she wanted to do this. Congress isn't allocating any additional money to the FCC because, well, they can't do much of anything, even if they wanted to. What would you have the FCC do less of in order to do this? And I know that's an impossible question. It's impossible in reality. And hypothetically. But still, what do you think?

Dale Hatfield:
Yes. A little bit too deep into the real politics. And I'm willing to go here of what? You give up my choices, not necessarily politically popular and so forth.

Dale Hatfield:
So I don't want to really go there, but.

Scott Wallsten:
Probably why they're right.

Dale Hatfield:
But there is one, this is a little bit self-serving. You have the Technical Advisory Council, which is supposed to be giving the commission advice on very difficult technical problems. So one of the things that I would recommend that she do or, other commissioners support, is to seek the advice of people that serve on the task force. And, you know, excluding myself, there's some really smart people on the TAC that I think could be a great, great help. So that's one kind of free. It's already kind of free. It's already existing, but that's a little bit, like I say, self-serving.

Scott Wallsten:
It seems like a good place to start, though. Okay, I think without any additional questions. Then we'll wrap it up. Dale, again, thanks so much. Really, really a pleasure talking with you.

Dale Hatfield (00:42:34) - Thank you again.

Dale Hatfield:
Thank you for having me. And I, like I say, I do invite people to reach out to me if there's things they'd like to challenge and what I've said.

Scott Wallsten:
Or I would. I don't want to inundate you with email, but I would encourage that because I always, I always learn things with our exchanges, email or otherwise. So all right. Thanks so much. Take care. Bye.