The Employment Law Counselor Episode 18

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, The Employment Law Counselor. Before we get started, we'd like to remind everyone that the information and opinions expressed by our speakers today are their own and do not necessarily represent the views of their employers or of PLUS. The contents of these materials may not be relied upon as legal advice.

Laura Corvo: Hi everyone. Welcome to the Employment Law Counselor Podcast. I'm your host, Laura Corvo. This podcast is a collaboration between White and Williams LLP and the Professional Liability Underwriting Society, commonly known as PLUS. While our podcast is not legal advice, it is a practical discussion between attorneys that deals with the maze and minefield of labor and employment laws on a daily basis.

If you like what you hear, please give us a five-star review and subscribe so you never have to miss an episode. My cohost, Victoria Fuller, is not here today because she's speaking at the upcoming PLUS webinar, but fortunately she will be back to join us on future episodes. Today we have a hot topic that is ripped [00:01:00] from recent headlines and an amazing guest.

We are going to be discussing what employers can learn from the recent Signal Chat debacle that has been the subject of so many recent headlines. We are going to take the story from a slightly different angle and focus on some best practices for employers as they manage their employees communications over electronic communication forums.

To discuss this topic with me, I am pleased to have my longtime colleague and friend, Andrea Moss. Andrea is a seasoned labor and employment law attorney who practices out of White and Williams' New York City office. Andrea is a skilled labor and employment litigator who has tried countless employment cases and who regularly provides counsel to employers on a host of employment related topics.

Welcome, Andrea. How are you doing today?

Andrea Moss: I'm great, Laura. Thanks. I'm kind of excited to be here to talk about this with you.

Laura Corvo: We're really excited to have you here and so happy that you were able to join us. Let's jump into this hot topic. We have recently seen headlines and news stories about an incident where high [00:02:00] level government officials inadvertently included a journalist on a signal chat, in which they discussed an impending military attack. Now, the politicians and the pundits certainly have had a lot to say about the implications of that incident. As the headlines hit and most people were discussing national security and politics, as I dare say, as nerdy employment attorneys, you and I saw this news story a little differently -- more of it as an opportunity for employers to reflect on how their employees communicate on these informal communication channels, especially as the use of these platforms becomes more commonplace.

Andrea Moss: Yeah, that's right, Laura. I know both of us have seen countless examples of employers who have gotten themselves into trouble because their employees disclosed information on an informal electronic communication platform.

Sometimes they're disclosing information, other times they're just having [00:03:00] inappropriate conversations or using inappropriate language on these communication platforms.

Laura Corvo: That can be dangerous, right? So, can you walk us through some of the dangers that can happen when there are either inadvertent or intentional disclosures on these electronic communication platforms and how that can hurt employers?

Andrea Moss: Well, I mean, there's a number of ways in which it can be really problematic and it can be dangerous for employers. Just backing up, I think we all kind of have the sense that when we are on text or on Slack or on WhatsApp or on any of these platforms, there's kind of this sense that it's a more casual conversation.

There's this way in which people communicate in a much abbreviated way. It's not formal; it’s casual. That always can lead to the problem of people saying things in a manner that's really not professional and not appropriate for the workplace and just getting into conversations that [00:04:00] they think aren't going to be seen by other people.

Just the nature of this type of messaging makes people think that they're having a conversation with somebody, maybe one or two coworkers, and not thinking of it as something that can be seen by everyone. As we've all seen, [this] is what happens with a lot of these things because they last forever.

Even though these messaging platforms are often referred to as ephemeral messaging, they're not ephemeral. They actually last forever. So, one of the dangers is that people say and do things that they wouldn't normally do because they're thinking, as we saw in the signal chat among high level government officials, they think nobody else is ever going to see what they're saying. They're sending emojis and they're saying things that are perhaps not as professional as one might hope, so that's one of the things.

They also can lead people to think that they're erasable or go [00:05:00] away after a certain period of time. They lead to situations where employers sometimes might be required to produce documents that include these texts and employees haven't preserved them, which also can be a big problem.

Laura Corvo: Yeah, and I think you make some great points there, Andrea. One of the things I think we forget, right, is we're operating in a different world. As these electronic communication platforms become more and more commonplace, they're great because they're fast. They do bring people together and build sense of community. They kind of, in some instances, take the place of what we would call the water cooler conversation, right, where people are back and forth having conversations. But at the water cooler, there's not a recording. There's not a permanency, right? You're just having that break room conversation. Now it's out there for the world to see.

Andrea Moss: Right. That's a really good point. I think that especially with so many people [00:06:00] working remotely and people working remotely from around the globe, people aren't having the same interactions with colleagues as they used to. It's kind of become an outlet to be able to get on a message and sort of catch up with a colleague. There's nothing wrong with that. That is great, but it also can lead to informal, inappropriate conversations

Laura Corvo: Getting back to the signal chat incident that happened, the concern there, obviously, was a leak of something that could impact national security. Most employers don't deal in that level of concern, but there are some heightened responsibilities for employers with regard to certain communications, like when we're talking about things like personal health information or salary information [and] social security numbers. I've had the instance where somebody in a human resources group accidentally sends an email [00:07:00] with an attachment containing sensitive salary information to the wrong person, and that gets into the wrong hands.

Employers are handling the height, or even worse, a client or a customer's confidential information that gets out, right. What are some concerns for

employers who have that heightened level of responsibility when it comes to confidential information?

Andrea Moss: Well, the thing is people have the same responsibility. Employers have the same responsibility toward confidential information, whether it's being distributed via email or text, or Slack or any of these other platforms, right? That goes directly to the whole idea of the employer having really clear policies about what people should and should not be able to send around.

One of the things that's great about this type of communication is you can do it from anywhere, right? You can be at the airport. You can get in touch with a client or a colleague and say, "Oh, don't forget to send this." But people have to be mindful when they do that that they might be [00:08:00] sending stuff that's confidential or that could get into other people's hands if it's sent through that channel.

Laura Corvo: I think that brings us to the next point, which is, what are some of the best practices that employers can put into place to avoid these types of inadvertent disclosures, or making sure that their employees are not putting information on these electronic communication forums that will come back and form the basis of a harassment or a discrimination complaint?

You mentioned it probably starts with a written policy. What types of written policies should employers be looking to have in place and to shore up?

Andrea Moss: Of course there's confidentiality policies, right? One of the things that seems really fundamental, but might not be as clear to all employees is what exactly the employer considers confidential.

You have to make really clear, these are the things that you should not be [00:09:00] disclosing. I think a lot of people, for whatever reason, have a lot of knowledge about HIPAA and private health information. [They] know that that shouldn't be disclosed, but there's a lot of other things that shouldn't be disclosed as well, like you were talking about salary. There's also things that have to do with personnel decisions that shouldn't be disclosed. Just letting people know what things they need to make sure are confidential, how your company defines confidential.

Then, of course, there's the policies surrounding the communications you're using. The BYOD, right? The bring your own device policies. [The] expectations the employer has with regards to using your computer to use Slack

or Google Meet or text or any of these other messaging platforms we were talking about.

I think that most employees think that when they're texting people from their own phone, it's private. They need to understand [00:10:00] what their expectation of privacy can be, and that comes through the BYOD policy, right? I mean, we've seen cases where employees think that because it's their private phone that they can have conversations with coworkers that are inappropriate and that nobody will ever know.

In one instance, one of the guys who was involved, one of the employees, had changed the name of the employee on the message to another name, right? So that if anybody ever asked me, "Oh, can I see your text with Laura?" that somehow he will have skirted the issue by having renamed Laura, Tom, in his phone. People need to understand your text messages are going to be retrievable. They're not private if that's what your company policy is.

I think the other thing is that the policy really needs to talk about prohibiting the disclosure of confidential information. It may want to also limit certain [00:11:00] confidential information from being sent through these electronic communication channels.

You may not want your HR person, who's on vacation, sending something through WhatsApp because they suddenly realize they forgot to deal with, for example, a reasonable accommodation request that's going to have medical information and stuff like that. That's stuff that can be really precarious, especially if you're in a situation where, like that example, you may have an employee who is seeking a reasonable accommodation and maybe the company is not going to grant it. Maybe the company is going to create a situation where the employee is not particularly happy that their reasonable accommodation was not granted, but they will then have perhaps exposure. The employer will [then] have exposure because their information was sent through an inappropriate means. Somebody else may have gotten a hold of it through text or chat messages, like I said [in] the example of an HR person using WhatsApp because they're on vacation.

Laura Corvo: [00:12:00] One of the things when I've drafted these policies [that] I've always tried to do is bring together both HR and your IT departments, right? Because you need to understand, I think when you're talking about confidential information, how these electronic communication platforms work. I'm not an IT person, but I think there are some protections that you can build into these policies for that heightened information where you have heightened

responsibility, like the personal health information or the salary information, or the disclosure of DA accommodation, or just the internal communications that you don't want out there.

You may want to have certain systems in place where those types of communications can only be used through different channels as you said, Andrea. I think a lot of times when you get together with your IT people, they'll have a lot of tools available for you which may help protect that information. It's really always, I [00:13:00] think, a good idea, as I'm sure you do, to get that input so that when you're drafting the policy, you're drafting it not only from the HR perspective or the legal perspective, but also with an IT input to say, "Hey, we actually have a tool here that would require a password protection on anything coming from the HR department."

Andrea Moss: Right. Yeah, that's a really good point. I think that one of the things that's really great about this signal scandal, from our perspective at least, is that signal is supposed to be encrypted, right? Signal is supposed to be the top level of secure messaging, and this incident showed us that even the highest levels of the government cannot rely upon encrypted messaging.

You're exactly right, getting the IT person in there to say, "If you're away and you don't have access to your email and you need to send something that's in these categories, this is how you go about doing it." [00:14:00] You don't do it via text. You don't do it by any of these messaging platforms. You have some workaround so that people understand, even if you think it's encrypted, we've all learned that doesn't really mean very much.

Laura Corvo: Exactly. You mentioned earlier that you have a concern about employees who look at these things as informal and who put things up there that they otherwise shouldn't and then that suddenly becomes discoverable in a lawsuit or exhibit A to a complaint.

What should employers include in their harassment and discrimination policies to address the concern over that type of disclosure?

Andrea Moss: That's a really good question. I think that one of the most important things that can be included is a clear statement that the anti-discrimination, anti-harassment policies also apply to electronic [00:15:00] communications.

I think that this is almost our modern day version of like the after work party, where twenty years ago people thought if you were at an after work party, the

policies of the workplace didn't apply. Right? Everyone would be out, they'd be at a convention or whatever. Now we've evolved to a point where most people recognize that [at] after work events you are guided by the same policies that are in the workplace because of the training that we've been doing, hopefully, has gotten through to people over the years that after work is still covered by the same policies.

Now what companies need to do is make sure that that extends to all electronic communications too because we've all seen situations where people are texting coworkers and using these messaging systems after hours. There just really is never an employee harassment or discrimination case that doesn't include text messages. It's always [00:16:00] going to be part of it.

It's interesting because even now people don't really seem to appreciate that they don't go away. I recently had a situation where the discrimination complaint was largely based upon text messages. In representing the employer, we obtained all the text messages from the employee who had been accused of engaging in inappropriate behavior. It turned out that the employee had selectively provided us with messages because he took out the ones where he thought he didn't sound as professional as he wished he had. That, of course, puts you in the position where you produce the messages and then the other person you're texting has the messages that you sent them. Then the other side produces the messages that include all of the one part that the employee on our side deleted. That puts you in a [00:17:00] terrible position.

Having people understand this stuff exists, you can't just selectively delete things and expect it's going to go away. It will be found somewhere, and employers have obligations to produce them if they are found.

Laura Corvo: I think it's also important to include in the policy that employees do not have any expectation of privacy in anything they send, receive [and] store on any communication system and that [they are] also seeing that you're monitoring it, right? You're able to see it. You're able to download it after the employee has left. You're able to view it. This is not a private conversation for the employee, and I think that's an important statement that has to be made in all of these types of policies.

Andrea, in addition to the written policies that we discussed, the strong communications policies, the technology policies, the confidentiality policies, the harassment policies, what else should employers be doing?

Andrea Moss: I was just going to ask you [00:18:00] about this because I think that I don't have a lot of familiarity with all of these messaging systems, but I know some of them give you the opportunity to set it so that it automatically deletes. I think Slack you can delete after five days or ten days or you can set it for whatever.

I know one of the things that came up in the signal controversy with the government was the idea of how much time they had their messages preserved for. I remember somebody was joking that he has his signal messages with his dog groomers set to erase after twenty-four hours, and the signal messages with the government were sent to race only after thirty days or something like that. So, he's like, I have [more] heightened security with my dog groomer than they had with the war plans.

I was wondering whether you think employers should have a policy where they tell employees that they cannot or should not set their Slack messages or their whatever messaging system they're using in the course of their employment to delete automatically?

Laura Corvo: Yeah. I think that [00:19:00] there should be some control over that, certainly when we get into litigation claims. As you know, when an employer is sued or a claim is made against employer, there's a preservation obligation, so the employer has to control that deletion time. That should not be done by the employee. That should be set by the employer. If the employer has a thirty day retention policy that's company-wide and consistent, that should be done.

Again, I think that has to remain in control with the employer and the policies, the procedures all have to tell that employee that this is your company business. This isn't your playground. This is our information system. We're in control of this, right? So absolutely I don't think employees should have that ability to control the timeframe in which those messages are deleted. That should always remain in control of the employer.

Andrea Moss: Right. Of course, one of the most important things the employer can do is not just [00:20:00] have these policies but enforce them. Even if they're just doing a verbal or a quick email to somebody, letting people know when the policies are violated [is important]. As we know, all of the bigger problems usually start off with smaller problems, and the bigger ones could have been avoided had the smaller ones been addressed.

Laura Corvo: Absolutely. That enforcement should be consistent across the board and, like you said, address it when it's small. When you see an employee putting something on a Slack that might be borderline and inappropriate, you want to talk to that employee right away.

I also think training is important, right? We have all these policies and sometimes they'll go on for pages and pages or be on page thirty-five of a handbook. Just having the written policy in place doesn't mean the employees read it or understood it. Actually taking the time to train the employees [and] remind them frequently that, "Hey, these policies are in place and here's what you need to do" goes a long way as [00:21:00] well. Especially specialized training when you're dealing with that heightened confidential information like HIPAA or social security numbers, salary information [and] things like that.

Andrea Moss: Yeah, you're absolutely right. Again, that's what we started this with. That's one of the things that's really interesting about the Signal controversy is that the people in that group obviously weren't properly trained in the use of that platform and whether it should be used in the way they were using it.

People have a very different response to reading page thirty-five of the handbook than they do to even being talked to for a minute and being told some things that can go wrong if they don't follow the policies. The policies are there for a reason. I mean, they look really dry. As well as we can draft them, they still come across pretty dry on paper. When people understand the real-world concerns and the real-world ramifications of not following them, [this is] usually through training.

Laura Corvo: Absolutely. I always tell [00:22:00] employers when you're implementing a new software program, you're not going to just throw an instruction booklet at the employee and tell them to figure it out. You're going to actually sit there and tell them what to do and what you want to do with it. It goes the same for all employment policies, but especially these policies where they're really protecting the most valuable assets of your company, your confidential information. If that's important to you, take that time to actually train the employees.

Also, as you said before, enforce it. Make sure that we're nipping things in the bud.

Andrea Moss: Right.

Laura Corvo: Andrea, this has been an amazing discussion. I think we are out of time, but I really want to thank you for joining us and giving us your insight on this great topic. It's been a pleasure.

Andrea Moss: Thank you so much for having me.

Laura Corvo: Well, we would also like to thank all of our listeners for joining us here on The Employment Law Counselor Podcast. I will be back next time along with my cohost, Victoria Fuller, to try to make sense of our ever-changing world of labor and employment law. If you enjoy this [00:23:00] episode, please leave us a five-star review, tell your friends and subscribe to the podcast.

For more information on this and many other topics, please visit the White and Williams website at www.whiteandwilliams.com, or you can visit our blog and learn more about the firm. Until next time, stay safe and stay compliant.

PLUS Staff: Thank you for listening to this episode of The Employment Law Counselor. If you haven't checked out the previous episodes, make sure to give those a listen and check back in in the next few weeks for the next episode. If you have an idea for a future PLUS podcast, you can visit the plus website and complete the content idea form.