

The Risks of Using AI for Legal Clients

Sarah Sawyer: Welcome to this week's OK at Work with myself, Sarah Sawyer, my colleague Russell Berger. Both attorneys at Offit Kurman. And today we are talking about AI use, which we talk about often on OK at Work as it is a relevant topic that's always evolving and changing. But today we'll be focusing on the client use of AI.

So often, no surprise to probably anyone who's listening, our clients may, put something into AI to look it up before they call us or while they're working with us, and I completely understand the temptation to do that, obviously, right? It's nice and easy on your desktop or ChatGPT, and you can just quickly say, like, "Well, help me understand this concept, what's going on."

"What would you think about this?" And it feels probably pretty good to do those things when you're just like anything else you're using AI for. However, there are some [00:01:00] unique things as it relates to the attorney and client relationship, which we've talked about on OK at Work before, related to privilege and confidentiality and, shielding of the information that you express to attorneys versus things you might tell somebody at a bar or some, friend or over dinner, and there's some special protections there.

And that applies as it relates to communications. And so when you are putting something into AI, that is a communication with that AI bot and that program. And so we're starting to see some issues with clients' use of AI. So what are some things, Russell, that, business owners and individuals should be thinking about as it relates to putting that burning legal question into AI and getting AI to help you out?

Russell Berger: Yeah. So you kind of alluded to it. We've got these long-running concepts of attorney-client privilege and work product performed at the direction of counsel. [00:02:00] And by and large, what courts are doing is they're not rewriting these concepts for AI, they're applying them to AI. And so what that means is if you're engaging with AI particularly if it is in a public AI, which we would recommend against anyway and already have probably here and it's not being done at your attorney's direction, which it probably isn't.

You risk waiving this. That's actually you're gonna lose privilege, you're gonna lose work product and it exposes what your AI chat history is, particularly on a given subject, to opposing counsel, to the other side if you get into litigation. And obviously if you're in litigation, that's a very obvious risk.

If you are in a transactional matter it's not an obvious risk 'cause you're not having litigation right then, but if things don't go right, you might. So something really, really critical to think about and, the general advice on this is that you shouldn't be using it for these legal purposes because you risk waiving these privileges and these [00:03:00] protections, and you could just give the other side the playbook.

So, for example, like the worst thing to do is to take a detailed strategic privileged email from your counsel and put it into AI and say, "Hey, I..." "Tell me what this..." "Shorten this. Tell me what this- really means". Explain this to me like I'm a business person." What I think makes more sense is if you have those questions, to talk to your lawyer about them and put that burden on your lawyer, who can also use the same AI tools to help you, but make sure it's coming through a privileged protected channel.

'Cause when it's not, you risk exposing whatever you're putting into the AI, not just your comments, not just your chats, but whatever you're uploading into the AI to opposing counsel.

Sarah Sawyer: Yeah, and I think a lot of times that people are trying to take a shortcut or save some money or be more efficient or, like you said, Russell, like be- have a better understanding, and often, even if you do all of that, you're still gonna end up wanting to go to your attorney and get that clarification.

So a lot of times AI will spit out an answer, and you [00:04:00] still want that clarification from your attorney because they're the professional and they actually can give you the real advice. And so you might as well skip that step that's exposing you to all of that risk, because you're gonna go to your attorney anyway especially for things that are more detailed and involved.

And so it's really not saving you the time that you're thinking in that moment, and it also is exposing you to the risk that you describe. It's something to be really mindful of. I think privilege, confidentiality, work product, like these are things that even before AI can be really challenging for people to kinda keep in mind, 'cause we're all moving so fast and it's so easy, like you mentioned, dropping an email into AI.

We've said the same thing before as it relates to forwarding an email, right? With more modern technology, even before AI, we've dealt with these issues where it's just so easy for a communication that's protected and a strategy that's protected to all of a sudden become not protected because it gets routed somewhere else.

So those same principles that you're thinking about when you're thinking about forwarding that email to someone [00:05:00] that is, not within your company or that is, where it could destroy the privilege, like those same concepts are applying here, and it's really just good to stop, think. Don't forward, don't in the middle of the night when you're up thinking about this issue, don't just start dropping stuff into ChatGPT so you can sleep.

Write your attorney an email. They may not answer you until the morning, but that might be a better thing than getting your direct response from a chatbot in the middle of the night.

Russell Berger: Yeah, absolutely, and, if there's a pain point, if there's something you're struggling with that should be something you should address with your attorney, and your attorney should be asking about that too.

I think the best place to solve those pain points is within the protections of that relationship. And it does remind me too, the other point here is because these things are discoverable, that also creates a litigation hold obligation. So if you've litigated at all, you probably got a litigation hold letter.

That's going to cover chat histories as well. Obviously some of these things have auto-delete features [00:06:00] and, they could all be wired a different way and set up a different way. But, and your hold obligations are gonna extend to your AI usage as well.

Sarah Sawyer: Yeah, really great points. Well, thanks Russell, and we'll see you next time.

Russell Berger: Thanks, Sarah.