PERSONAL DEVICES AND MESSAGING: EVOLVING COMPLIANCE CONCERNS AND BEST PRACTICES
RECORDED 4/19/23

Megan Rahman:

Hi, my name is Megan Rahman, and I'm a partner in the Troutman Pepper White Collar + Government Investigations Practice Group. I want to welcome you to this podcast. I'm here with my colleagues, Abbey Hazlett, Alison Grounds, and Chris Haley. Electronic communications have always played an important role in corporate investigations, but on March 3rd, the Department of Justice issued revised guidance regarding the use of personal devices and the preservation of company communications. The DOJ's concerns about the use of personal devices and third-party messaging applications, they're not new, as issues regarding these applications have been increasingly at the forefront of preservation issues in DOJ and internal investigations for a pretty long time. The revised guidance, which is found in the Evaluation of Corporate Compliance Programs, instructs prosecutors to consider a corporation's approach to the use of personal devices, as well as various communication platforms and messaging applications.

In this podcast, we're going to talk about the guidance and what steps companies can take now in response to these revisions in order to hopefully gain a more favorable resolution in the event of future DOJ action.

Before we do that, we want to tell you a little bit about ourselves. I provide advice and support to individuals and corporations facing regulatory, civil, and criminal investigations. I conduct internal investigations and represent clients in government investigations and federal, civil, and criminal litigation, which relates to a wide variety of criminal enforcement matters, including antitrust, accounting fraud, bank and lending fraud, and violations of the False Claims Act and the Foreign Corrupt Practices Act. Abbey?

Abbey Hazlett:

Thanks, Megan. My name's Abbey Hazlett. I'm a partner in our firm's Government Investigations and White Collar Defense Group as well. My practice is very similar to Megan. I conduct internal investigations for companies regularly, in high-stakes and complicated areas, and also defend companies when they're being investigated by the government for criminal misconduct or potential civil liability in the context of the False Claims Act.

Megan Rahman:

Alison? Chris?

Alison Grounds:

Well, hi, everybody. I'm Alison Grounds, and my practice is focused on all things eDiscovery and data management. I am usually a supporting character, assisting Megan and Abbey when they have investigations or litigation. And our team, which includes Chris Haley, who is our Managing Director of Technology, focuses on the intersection of the legal and technical issues around the preservation, collection, and management of data for legal matters. And in the context of investigations, that is a very large focus and something that we are regularly consulting our clients on. We're excited to talk about the data management implications of this new guidance.

PERSONAL DEVICES AND MESSAGING: EVOLVING COMPLIANCE CONCERNS AND BEST PRACTICES

Chris Haley:

I'm Chris Haley. I'm the Managing Director of Technology here at our firm, and I oversee a team of specialists and technologists that assist our attorneys and our clients with data preservation, data collection, in particular for difficult data sources, like mobile devices, short messaging, those types of things.

Megan Rahman:

Before we jump into the guidance, Abbey, you were at the ABA White Collar Conference in Miami, where this was actually discussed on one of the panels, weren't you?

Abbey Hazlett:

I was. Megan was there with me too, as were a number of our colleagues in beautiful, sunny Miami, Florida. Between standing outside in the sunshine, we heard from a lot of great speakers, including Assistant Attorney General Ken Polite, who talked about changes to DOJ's compliance guidance and the continued focus on electronic communications, and what businesses are doing to govern their employees' use of electronic communications. The top thing about this, which we'll talk about more as we go along, is that there is no one-size-fits-all or prescribed way to do this, and we emphasize that businesses need to consider what their business is, what their risk profile is, and figure out the appropriate policies to make sure that they can preserve and access business communications.

We also emphasize that, when DOJ does come to a company and wants to conduct an investigation, that, when they ask for business communications, they mean everything. They don't just mean email anymore. They know that employees are communicating outside of email, all of the time, these days, particularly coming out of the pandemic. People are texting. They're using Snapchat. They're using WhatsApp. So the DOJ wants companies to be able to respond to requests for business records, by explaining not just what its email systems look like, what its document management systems look like, but how its employees are communicating with each other and what its policies are governing, preserving, and accessing those communications.

Megan Rahman:

So let's talk about the guidance. Does the guidance provide any specific direction to the prosecutors?

Abbey Hazlett:

What the guidance says to prosecutors is that they should look at a few different things. Again, when they're looking at businesses and how they govern electronic communications, they're not looking for a one-size-fits-all approach. There are no hard rules, but you really have to tailor what you are doing to your business, to how your employees work, how your employees operate, the areas within the world that you operate, and what your risk profile is, overall. So there are no hard-and-fast rules, but there are general areas that DOJ says that companies should consider when developing policies on this.

Megan Rahman:

How about any specific factors? Are there specific factors that the prosecutors have to evaluate? Does the guidance address that?

Abbey Hazlett:

It does. So it lists three factors, and I'll talk about each in a little bit more detail. It talks about communication channels, the policy environment, and the risk management processes. And for people who work in compliance, this is all very familiar. It's similar to what you do when you're contemplating a merger, acquisition, or any other policy area that your company is implementing.

So, the communication channel is, "What are you using? What are your employees using? How is that different in one business function versus another business function? How is it different in the United States versus your employees who may sit in India? And how does the company get access to those different channels, so that it can, when necessary, review, preserve, produce those different communications?"

And really importantly, and I think this is important for companies to think about, is prosecutors are looking for companies to articulate the reason why. "Why is your policy in the United States that you cannot use WhatsApp to conduct business, but why, maybe in another part of the world, like Southeast Asia, is that okay? Is there a rationale for that?" And the reasons why are so important for communicating to the Department of Justice. And also, from our standpoint, when we're going in, conducting an internal investigation, and perhaps helping companies train their employees on policies and best practices, explaining the why to employees also becomes really important.

The second piece here is the policy environment. This is really, "What do your policies say? Do you have a bring your own device policy? And then, how are those policies enforced?" Anyone who has been investigated by DOJ or works in a highly regulated industry knows that the worst thing that can happen is that you have great policies on paper and nobody's actually carrying them out. DOJ wants to be able to understand what the policies are, how they're applied, how they're monitored, how they're enforced, and how exceptions are made. It is inevitable that every policy, probably at one time or another, will need an exception for a very good and legitimate reason. But you need to be able to explain that to DOJ, if they're asking questions.

And then, the last area of focus is risk management. "What is the risk to your business? What are the consequences to your employees if they violate the policies? Do you discipline employees? Do you retrain employees? How are you carrying out the monitoring and enforcement piece of this, to make sure that your employees are doing the right thing?"

Megan Rahman:

And it's not just the DOJ that's focused on these issues, is it? There are other regulatory agencies that are talking about these communication and preservation issues, correct?

Abbey Hazlett:

That's right. And everyone is very focused on this issue, because the reality of how people do business today is very different than how they even did business five years ago. It seems to us that our clients and the government finally have their feet under them, when it comes to email preservation and production. But now, there's this whole other category of communication, that everyone is really focused on, so that prosecutors and regulators can do their jobs. FTC and DOJ have a working group. There's a lot of concern around the use of ephemeral communications, so communications that disappear. "How are those being preserved? How are they available to DOJ or FTC, if they're investigating?" And then, everybody read about the SEC settlements with Wall Street firms that paid over 1.1 billion dollars to settle

investigations, that were really focused on how those firms and their employees were using ephemeral communication, when they shouldn't have been.

Megan Rahman:

It's clear the guidance and the remarks at the ABA conference, it just highlights the importance of the development and implementation of clear written policies regarding the preservation of business-related communications. But this sounds like it might be easier said than done. So Alison, Chris, what are some steps companies can take now, in the event of DOJ action in the future?

Alison Grounds:

Well, thanks, Megan. And I would say, this topic is interesting, because the role that we play, typically, in these cases, as I mentioned, can be a supporting role. So once a DOJ investigation ensues, and Abbey mentioned the DOJ requesting information about systems, and that's something we're often helping clients to pull together. They ask very detailed questions about your communication systems and your platforms and your policies and your procedures. So when we're doing that in a reactive way, we can certainly pull that together on the fly and get the information. But systems change constantly. And so, one way that companies can help be prepared is to know the answers to those questions before an investigation ensues, understanding what policies may be implicated and may be requested, as well as not just the policies, but how they come to life, how they're enforced, all the criteria that Abbey mentioned.

Some other work that we tend to do for clients is what we call litigation readiness assessments. Pre-litigation, pre-investigation, let's just see if your house is in order and how you're functioning, what communication platforms your employees are using. One thing our clients should think about when looking at this guidance from the DOJ is, "What policies could be implicated?" We find, when we're dealing with information governance and data management, there are lots of different policies that intersect. So one of the big policies you hear people talking about, in light of this guidance, is bring your own device policies, which are certainly to the forefront here, because people are often using their own devices to use these applications and these communication channels that are offline or off-record or not part of the central IT systems of companies. But they're more than just BYOD policies at play here.

We also look at acceptable use policies and the guidance our companies are telling their employees about how they should use the communication platforms that they have through the company, appropriate use of them, language tone, what you're supposed to be saying and not saying in them, as well as what you should be using your mobile device for, and any personal devices, or in most cases, what you should not be using it for. Those intersect very closely. We also look at information governance policies around data security and privacy, which can overlap. And the final category that typically has guidance around these issues is a company's litigation response plan or discovery documentation, how they suspend their regular retention policies when there is a need to preserve, because there's an investigation or litigation that's ensued. So all of those policies working together, and what we find, in many cases, is those policies are owned by different stakeholders.

Maybe the legal hold policy and suspension policy is owned by legal, but the records retention, acceptable use, the privacy security could be owned by the privacy team or the information governance team. Or there could be different business units that have different policies, that could conflict with one another. So depending on the profile of the client, their regulatory profile, their business profile, their risk profile, we see the full gamut there. So really just taking the time to do a little self-check, a little

assessment, "What policies do you have? How are they being enforced? What are the technology implementation tools to make sure that people are complying with them so that you have some guardrails around that?"

And then, the last thing I'll say, and I would love for Chris to kind of comment on some of the technical challenges we see, as you said, Megan, it's easier said than done in these SEC enforcement actions that Abbey mentioned, those were fun nerdy reading for an eDiscovery lawyer, because what they did, in those actions, was, and I think someone else had mentioned this previously, the government kind of becomes spoiled by being able to get all your communications.

"We request emails, and we can see the whole conversation. And now, we want to see that when we do an investigation." And they were getting frustrated because they weren't seeing the communications. They knew people were talking, but they weren't seeing them in the productions that were being made. And so, they did a serious audit of offline communication channels in those investigations. And the way that they assessed and discovered a treasure trove of communications that were business-related transactional communications that these heavily regulated entities were required to retain in a location that could be preserved and produced when required, the way they found out about these was by doing some audits, imaging devices, doing some collections, and finding these communications.

And what I found very interesting, these were very sophisticated Wall Street firms that had robust policies, robust training programs, and documentation confirming. The problem here was the managers instilled with the authority to enforce these compliance programs and to make sure that the messaging and communication was being appropriately channeled were some of the very custodians who were using these offline channels to communicate. And it was rampant. So you see those fines being so high, I think because of just the full scale of that. When we're advising clients, it's not just about the policies, it's not just about the training, it's not just about the implementation, it's "How can you ensure that's happening?" And that's certainly easier said than done.

Chris Haley:

I don't think anything that we're talking about, frankly, the challenges themselves, are anything new. We had these challenges for a long time. In particular, if you think about just using personal computers or personal email, but the certainly bring the heightened awareness to it in the challenges that are compounded by mobile devices, where everyone has one, it's convenient, there's a desire to want to use it, because it's easy. It's there, these ephemeral or short message applications that make it easy to communicate in a way that is not centrally managed or centrally controlled or preserved or collectible. And so, those challenges are really what is at the heart, from the technical perspective, of this. This is a tremendous wake-up call and opportunity for corporations who may not have a good relationship or collaborative work environment between different departments, in particular legal, IT, information governance, and security.

This is a time to get together as a group and to talk through these challenging issues because there's a stakeholder in every one of those groups that can build momentum for change within an organization. Obviously, data security is critically important, and having data out on mobile devices and business records there is a challenge from security. Data privacy is a big concern nowadays. And then, obviously, the legal concerns and the legal requirements have always been there. But with this as a heightened alert for us and a wake-up call where we could take action before there's an urgent need to deal with it, because collecting and preserving data on mobile devices and these new applications that are popping up every day are really, really challenging. So if you are permitting business records and business

communications that need to be preserved and collected, to be done on mobile devices or personal devices or applications that are not centrally managed, you're introducing a lot of risk into your legal practice and matters.

Alison Grounds:

And it's interesting too. We talked about ephemeral messaging, and I think that was mentioned in the guidance as well, which was originally intended to be something that went away very quickly, like the conversation and the air that we're having. We're recording this intentionally, but most of the time, we don't record every word that we speak. But you're seeing a lot of these applications, at least in our practice, which were developed for that use. But because people liked them so much and they adopted them for business applications, they had to modify their functionality to be able to preserve that information, when appropriate. A lot of the collaboration tools that have expanded over the course of the pandemic, they're rolling out sort of the business-friendly models of those applications and allowing for more tools for that. It's an interesting challenge to me, and I think, Megan and Abbey, you guys do this for a living.

If someone is intentionally trying to avoid having a conversation being recorded, you can still go to a parking garage. It's going to be hard to stop people from doing that. And I think what we are trying to look at for clients is that there's no one size that fits all. "What's your regulatory profile? What's your risk profile?" You're not going to be able to stop individuals from doing certain things, unless you have, again, if there's a motivation to do that. And I think part of the problem with these SEC fines were it was a rampant business practice to communicate on these offline channels.

And so, just really looking at that and understanding, when is that happening? Why is it happening? How can we ensure and limit that in a meaningful way? In some cases, it's an innocent reason. It's happening because it's a more user-friendly communication platform. So should we start reconsidering the tools that we are giving to our company employees for communication to make sure that those tools are appropriately controlled, can be preserved, and produced when necessary? So again, just evaluating the why behind some of these offline discussions to be able to make informed decisions about how to comply with this guidance.

Abbey Hazlett:

And I think, from our standpoint, I think back to when I was first starting as a lawyer and emails were really coming into use, and one of the things we always said to our clients was, "Oftentimes, tone is lost on email." That is infinitely worse in text message, and you lose context too. So I think employees need to understand that companies aren't just trying to make their lives more difficult, but that we're trying to protect them from saying boneheaded things on text message and having to explain that five years later to an aggressive prosecutor in whatever jurisdiction you're getting dragged into. I think if employees think about that, take a step back and say, "This is not just an off the cuff one time joke, but something that I might need to explain, 2, 3, 4 years from now," that helps companies get everybody on board and think twice about how they're communicating and what tools they're using.

Alison Grounds:

I don't know if you read this, but I think that false confidence of assuming the tool you're using is not recording or is safe or is secure and nobody's going to see what you're saying, I believe a government agency outside of the US just hacked into one of these supposedly secure environments that the crime

syndicates were using and just discovered a treasure trove. Because they were speaking so freely, they weren't even trying to hide what they were doing. And I think that's a similar mindset of you get this false confidence in using some of these applications, that it's never going to see the light of day and that it's going to go away.

And so, Abbey, that's a really good point, and we certainly see that. I think all of us on this podcast see this when we do these collections and start to analyze the information in response to investigations. We often find the communications being a little loose and colorful and not maybe the sender or recipient expecting that to have lasted or to have been available to us. So the same speeches we gave about email, moons ago, then we started talking about text messaging. Now we're talking about these other applications as well.

Megan Rahman:

And I think that just highlights, Alison, the importance of training. Training and communication on these policies. We've been talking about the policies, and we've been talking about a review and update to the policies, but they've got to be communicated and the employees have to be trained on them. And to Abbey's point, the employees have to understand why these policies are in place.

Alison Grounds:

Absolutely. And I know we've all done those trainings, where we've shown, on the big screen, the communication that we collected as an example, so people know the kinds of information that's out there. Because it's easy to say it in the abstract. It's another more frightening experience to see an example from your own company or on a particular incident, where something's gone wrong. You never want to be the star of that show.

Megan Rahman:

No. So we're going to tell all of our clients to go back to fountain pens. That's how we're going to communicate going forward.

Abbey Hazlett:

And phone calls, everything.

Megan Rahman:

Phone calls and fountain pens.

Alison Grounds:

What's funny, we laugh about it, but the technology's existing now where we could record every phone call that we ever have. And so, part of my reaction when I hear the DOJ with some of these guidances is like, "Well, just because you can doesn't mean you should have to. And just because it's frustrating that everything's not recorded..." My understanding is, and this is what you guys have explained as well is you can have a record retention policy, a communication is not necessarily a record. While there are regulations that require certain types of business communications for heavily regulated entities to be maintained, this is that balance. Not every client is in that category. So understanding your regulatory profile and then, understanding what kinds of communications may need to be kept and retained and

recorded, because there's a line here where you could be recording every meeting and every discussion and every thought that you ever have, which is obviously not going to be sustainable for anybody.

Chris Haley:

Well, and you have pressures of clients who want to use a particular messaging capability and you want to be responsive to your client and responding that way. I think, your culture, your business, your clients, the regulatory requirements are all going to be factors in determining how you approach this and the risk that you're willing to take or not take and the solutions that you might put in place. Because allowing individuals to use their personal devices to communicate, business communications, and to store business records or create business records can be a huge challenge, because there aren't great technology tools to allow us to easily preserve and collect, in a particular parse out, what's personal from what's business. So there's a lot of overlap, a lot of discomfort from clients, who, when we show up to image there and take all the data from their phone, especially the battle between privacy and compliance, Apple and Android actually intentionally make it difficult to get data from devices and to parse out work from personal information, because of privacy concerns.

And so, they're fighting to lock down. And every day, every update, and every upgrade to their hardware and software is intended to make it more difficult, for privacy reasons, to be able to collect from those and to carve that data out. So it's a challenge that you're facing, if you are going to allow that to occur. Then questions start come up. "Do we need to get a more comprehensive, if I'm in a regulatory space, a more comprehensive archiving solution, like Smarsh or Proofpoint?" Not endorsing anything, those are just two of the more popular ones. "Or do we need to issue corporate devices, so that employees who have a need to create business records on their devices are using a corporate device and can separate their personal from private information?"

Alison Grounds:

I'd also add that this is one of those things that isn't a one and done, because the technology is constantly evolving and people's preferences are evolving, and the business case is evolving. This is something that we have standing meetings with our clients on. We help them assess these policies, and then, on an annual basis, we're revisiting them. We're looking at them. We're seeing with changes to make sure we're adapting to that. And the other thing that Chris mentioned that I thought was a great point is there was a swing toward everyone using BYOD. We're definitely seeing a shift towards more company-issued devices and/or company-issued and authorized communication tools on personal devices, that are in a sandbox and isolated and can be centrally controlled. And again, testing the compliance for that can be challenging because a lot of these policies do limit the company's ability to go outside of those designated zones.

Really balancing that is an important part of this analysis. We're also seeing, when we look at bring your own device policies and acceptable use policies, companies used to use language, and we used to advise language that was very clear about the separation of what was the company data versus the personal data. But it's really hard to have that happen in practice. So if you've got policies that are very strongly worded, that say "Every word you ever utter on your device, while you're in office hours, belongs to the company," you could be saying that you have control over that data and be obligating yourself to do that. And it may be that you need to because of your regulatory profile. It may also be that you need to draw a clearer line where there are certain things you don't control and the things you don't control should not be places where information generated for the course of business is stored or transmitted.

But again, much easier said than done. And the technology here is constantly evolving, and we're constantly having to evaluate new tools for preservation and collection.

Megan Rahman:

And the guidance, I think, is going to change too. I think you will see constant revisions to the guidance, but the DOJ's new update to its guidance, as we talked about, is a good reason now, for companies to consider reviewing and updating their policies on their business-related communications. These revisions to the guidance are a sign that a company's approach to preserving and accessing these electronic communications it's going to be an important piece of any DOJ compliance evaluation and not just the DOJ. We talked about SEC, we talked about other regulatory agencies. So I think taking some of the steps we discussed today will really ensure a more favorable resolution in the event of a future DOJ investigation.

Chris Haley:

And not just the policies themselves but the verification that the policy is being followed. The testing may a random sampling. We do this in a lot of different areas of businesses to verify that things are being done properly. Just in the normal course of your business, you want to make sure you have high quality for your clients, so you probably sample whatever your product is. But I think what this is saying is that considering that you need to have some verification, it's not enough just to trust and train. You have to verify that you have some process. You don't need to do a hundred devices a year maybe, but I guess it depends on your risk tolerance and risk profile, the exact number, or how you sample your sampling methodology. But not doing anything seems to be a bit concerning, depending on what you're allowing or wanting business records to be created any sources.

Abbey Hazlett:

Chris, that's a great point.

Megan Rahman:

Well, thank you for joining us today for the podcast. Collaboration, whether on a podcast or on a case, it's a hallmark of our firm, and we appreciate this opportunity to offer insights that address the full spectrum of issues facing our clients. Troutman Pepper's service offerings span transactional, regulatory, and litigation practices, allowing our attorneys to draw upon the expertise and insights of colleagues across the firm to develop holistic, comprehensive solutions to complex legal and regulatory issues.

For additional insights, please head over to troutman.com/podcasts, and listen to other podcasts currently offered by our colleagues, all subject matter experts in their respective practices. These podcasts are insightful, entertaining, and dedicated to interesting and evolving areas of the law. Each of our podcasts is also available for download on popular streaming platforms like Spotify, Apple Podcasts, and more. Thanks for listening.