Spring 2015


Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol31/iss4/5

This Conference Proceeding is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
SESSION ONE:

DUAL-USE DEVICES IN THE WORKPLACE

MODERATOR:

DAVID SORKIN
PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PANELISTS:

EUGUENE GORYUNOV
PARTNER, KIRKLAND & ELLIS LLP

GREG POLINS
ASSOCIATE, KIRKLAND & ELLIS LLP

RYAN HUBBARD
ASSOCIATE, KIRKLAND & ELLIS LLP
PROFESSOR DAVID SORKIN: My name is David Sorkin. I'm a professor here at John Marshall, I teach in the areas of IT and privacy law, among others. My five-second plug is this summer I'll be teaching an online seminar on cyber-space law, sort of an afternoon at law, and I believe registrations are still open.

It's my pleasure to introduce the first panel. Speaking on dual-use devices in the workplace, from the law firm of Kirkland & Ellis LLP, Eugene Goryunov, Greg Polins, and Ryan Hubbard.

(Applause.)

MR. RYAN HUBBARD: Good morning, everyone. So what we want to talk about today is dual-use devices in the workplace. Eugene, Greg, and I, are all actually patent guys, normally. We do a lot of patent litigation. But, we all had prior lives as engineers before we became attorneys, so we've actually encountered dual-use devices or, I might sometimes say, bring-your-own-device policies, in three different arenas.

We've encountered them as employees of tech companies or companies with tech focuses. We've encountered them in our daily lives as attorneys who are tied to them or chained to them, or glued/chained/padlocked, and otherwise bonded to, and also on the back end, when things have gone wrong, when there's litigation, when we need to be collecting and preserving and reviewing all this wonderful data that everyone is creating on a daily basis.

So we -- in doing so, we came up with some concerns that are -- need to be balanced when you're considering these policies, things like what they mean for your employees, privacy concerns for those employees, security of the company's data, the complexity of the back-end system and the IT that you're going to have to be looking at, depending on which sort of policy you implement, and also the size of your company.

So I guess I am speaking with the assumption that everyone knows what we're talking about when we say dual-use devices, also known as a bring your own device policy. Basically, this means that instead of the company providing its employees, or in addition to the company providing all of its employees with a Smartphone or their personal device, iPad, the employee can bring their own. Usually there is a short list of acceptable hardware, because we want to have some control. That would include both the work e-mail account, work data accounts, perhaps some work-related apps, and also the employee's personal information, their personal e-mail account, and their personal phone number. Depending on policy strength, maybe some personal applications. This is something that's becoming much more common and some things that a lot of employees at least think they want. Whether or not when they actually see how easily reachable they are outside of work, they ac-
tually do want it.

There can be a lot of overlap. You have people merging their calendars together, people with multiple e-mail accounts all on one device. You know, most of these devices only have -- and this is where the security concern comes in -- most of these devices only have one memory partition. So all of that data, even though when the employee sees it and when it's perhaps being transmitted over the various services, it looks like it's separate, but at the end of the day, it all sits on one physical device. Although some of the more recent iPhones and Android devices I understand can actually start doing a complete partition of one set of apps and software and one goes to the one and one to the other.

So we're going to address all these issues from three different perspectives; one being the employer's perspective. How do I manage my data, keep my data safe, and also my employees. One by the employee's perspective, what do I actually think about all this? I think about my privacy and my convenience in my everyday life. Finally, Eugene is going to sum up on sort of the balancing act.

So starting with the employer perspective. And each of these segments is going to kind of go the same way, what are the advantages of some of the policies that you can implement, what are the disadvantages of some the potential policies, and then what's the scope of control and intrusiveness into an employee's daily life.

So the first policy we want to talk about is: employee brings their own device or is provided a device by the company; but, regardless, they are allowed to put their own e-mail account on there, they're allowed to use it for texting, they're allowed to take both personal calls and work calls off of the same number, and they're allowed to install at least some apps.

Now the advantages here for an employee, this is very convenient, because they only have to carry around one thing. If they want -- you know, they only have to give out one number to friends. They only have to keep track of updating and the expense of one device, and when they're off working or something, if they want to go play Angry Birds, or whatever the latest game is, they can do that too. Maybe that's not so great for an employer; for employees, this is something they kind of want.

For the employer advantage, when you have the ability to contact people by their work phone and it's also a personal phone, you have a high degree of access to your employees. You know you're basically going to reach them everywhere, because the same phone they are using to text their friends to go meet at the bar later, is the same phone that you are using to send them an e-mail saying, don't go to the bar, get back to work, there's something important happening right now.

The other advantage, although this comes with some cautions, as
we'll see later, is that you're not as -- you don't need to be as strict, at least from a general sense of what your policies are, and this is a slippery slope. Basically you're saying, go ahead and use the device for whatever, but there's going to need to be a whole bunch of conditions: we're giving you a lot of trust here; don't go installing malware on your phone; don't click on stupid links; do not take confidential information you got from your work e-mail and then send it back out over your personal e-mail, etc. So from a technological perspective and from a policy perspective up-front, it doesn't appear like there is some overhead, although as we'll see later, some of that kind of creeps up.

So then the next policy we want to talk about is, we have separate accounts allowed but no text messaging. It's not that there is no technical capability for text messaging, there's just a policy against doing it. This is sort of an example of a lot of ways that, even if you're not controlling the actual tech, you are still setting a policy of no text messages, or don't install any apps. We're not going to technologically prevent you from doing it, but just don't put any extra applications on your device.

There is a better way, the idea here is that we want to let the person use text messages in case of emergencies, some emergency services use SMS. Maybe, if there's -- I'm personally guilty of, if I'm in a meeting and there is a white board, I will scrawl all over that white board, and then I will realize I hadn't been taking notes, so I'll take a picture of it with my phone and then send a message to myself and whoever else I'm working with saying, here are the notes from the meeting. It's a good thing that we have these wonderful devices.

So it allows for a little bit of flexibility, but we have a policy in place saying, you know, we really don't want you doing this. So it's a more flexible policy.

The next level is, again, sort of exemplary. We are still allowing separate e-mail accounts. We are still dual usage. However, technologically we are going to disable text messages, for example, or we're going to put some software on the phone that locks out that user's profile from installing extra applications. So we're being a little more restrictive now. The reasons we're doing that is, we're trying to limit the employees to communication forms that are a little more formal and things that we can control and record a little better.

So, for example, with texts, I think everyone can think of a new story involving at least one politician, if not multiple, or one employee of some department, if not multiple, where they were sending pictures or jokes or things over SMS that they shouldn't have and got into a lot of trouble. It is not that they couldn't send it over e-mail, but for some reason people's brains turn off when they only have to write a few characters, and they don't think about sending a picture of whatever.
The same goes for applications or software. You know, sometimes we just want to avoid the human error, and say we're not going to trust people to only install what is actually business critical or what they really need in their lives. We're just going to shut this off and if we want to put extra software, an extra app on the phone, we'll push it out, either update it ourselves, or give those instructions on how to do that.

The next policy is really not a bring-your-own-device policy anymore. It's -- whatever phone, if you want to bring your personal phone number, whatever, that's fine, but, basically, the phone you're getting is a phone that is totally in control of the company. We control all the applications on it; we control your user profile; all the data on it is ours; your e-mail account is ours; we're not letting you text. The advantages here is that if you still want to be able to reach your employees on a mobile device but you really want to be sensitive about securing your data, this is how you get around that memory problem that would be very easy for someone to take something from their phone and from a work account and push it out on their personal account. Also so that you can be ensuring you're monitoring and, frankly, send a message to the employees that this is not a phone you should be using when you are getting drinks and going to the bar or calling your girlfriend or husband or whatever.

It also helps IT, the IT department of the company a little bit, because now you are really controlling what's on the phone, so you know, or hopefully know, as much as possible about what's on there. So there is a more finite list of bugs and issues and security exploits you need to be worried about.

Finally, the last is simply for some employees or all employees, and this is somewhat common or more common in, say, the finance industry or the banking industry. If you are not a certain level employee, you do not have a work phone. You know, we expect you to be reachable. Maybe we want to have a personal cell phone number, but you're not getting e-mail after hours. You're certainly not sending text messages to a work account. This can be carried to considerable extremes, perhaps, you know you only have a workstation at work; you don't have a laptop you can take home. Your workstation may not have even a USB port on it, again depending on the employee's role in the security has to apply. This, again, reduces the burden on your IT department, because there are just fewer things for them to keep track of. The other thing is that in case of litigation -- and this is something we'll get more into when we get to the disadvantages -- is that by limiting, by excluding this device, it's basically one place we don't have to look when you're doing an investigation. When there is litigation and you are now collecting material, now we know everything is on our servers for the employee's computer at work, so that is the only place we have to look, and it really
cuts down on headaches for things like your litigation preservation. But each of these policies come with disadvantages.

So starting back where we were with the pure dual-device, have everything on one device. The main thing is the security risk, and we actually -- I actually have two anecdotes I want to share on this. One is that we were -- this one is less humorous, but there was an employee who we were aware of and we were tracking as one of our cases, and he disappeared one day. We didn't really know where he went. He was no longer with the company and everyone was uncomfortable telling us why. It later turned out that he had done exactly what I had said. He had taken confidential information from his work device and his work account and e-mailed it out to himself and his wife on his personal account. It's entirely possible there was an innocuous reason for that, that he was just trying to look at it at home and didn't want -- couldn't read it on his phone and wanted to have it on his laptops. Regardless, he was terminated, and it was not a great story for him. So this is not a good thing for either company or employee because you get lulled into this sense of, well, it's my device, I'll do what I want with it. The other, and that leads to the next point, which is, okay, so this is now a possibility.

Do we need to be monitoring the employee's personal account? Is it really a personal account once we start monitoring it? Or do we become accountable for knowing what the employee is doing? If this turns into a sexual harassment suit, if the employee was using his personal account to harass other employees, and we were monitoring that account, again, this is now getting to be more and more data that we have to keep track of and preserve. Then once we get into litigation, when the case starts up, the first thing you do is put a litigation hold in place. We don't want stuff disappearing. You know, we've got all these places that we have to list, and we need to -- and now you've got outside attorneys who have to come in and try and determine where all the locations are that you have extra data lying around that might be sensitive. So that's kind of the downside of this policy, is there's just a lot more data, a lot more to keep track of, and in order for you to feel fully secure about what's going on, you might have to be more intrusive. So the next one is, separate accounts allowed, but we have a policy against texting or apps or things that we don't necessarily want employees doing. The problem here is that if it's a policy without a technological solution, you're kind of setting your employees up to fail. Then if you give them the capability to do it but you tell them not to, you're sort of acknowledging that they can do it sometimes.

The other problem is that you have done nothing to solve any of your collection problems. Maybe, if you're in litigation and you have reasonable opposing counsel, you could say, look, we're going to collect and preserve e-mail from their work accounts, but we have a policy
against them using it for personal usage so no personal accounts. In some cases, maybe patent litigation cases, something like that that might be okay. If it's a case against a little more personal relationship, sexual harassment case, workplace discrimination case, maybe that's not going to fly. So we haven't -- we have papered over it and it looks like we've done something, but we still have that human error issue. Next, so now-- if we have the technological solution, now we have increased our security, we have also increased our complexity, and we reduced our convenience for the employees. So now we have this dual-use device, but maybe the employee is starting to bristle a little bit about the burdens being placed on them. Maybe there's some things that, you know, the company would really actually like people to do. So, if there's some app that would be great for everyone's productivity, but we have this lockout placed on all the devices, we have to have IT come up with a solution to make an exception for this app and so on.

The next one is where we have basically banned dual-use devices altogether. I mean, the main problem here is that now-- you have an increased expense on your side, because if you want employees to use a device that is work only, you may have to purchase it for them, it's very likely. Also, employees are going to have a second phone, and based on past experience, if someone has two phones, one that connects them to friends and family and one that connects them to work, and they're in a social setting, their work phone may not be anywhere near them. It was probably left at home unless they're required to keep it. There are some fairly notorious examples of people forgetting their work device. You know, if you've got -- if you are used to only having one device in your pocket and, you know, you got that weight, and then you've got an extra device you are supposed to be keeping track of, it's a little difficult to do, you know, midnight or one o'clock in the morning when you're -- it's a Friday night and you're trying to blow off steam after work. The no device ability provided, you know, that is -- it's the highest security, but, for a lot of employees, it's just not practical. If you need someone to be on call, you basically, in this day and age, need to be able to reach them over e-mail. Greg has a good story about an on-call device that he'll talk about later. In my prior life working for a tech company, I was on the combination of, this is secure enough that we don't want you to take it outside of work, and you are, frankly, important enough that we need you to be on call. So you don't have to have a phone e-mail account. You can just come in, do your work during business hours, leave. If we really need you, we have a contact phone number for you. But that doesn't work for everybody. Certainly, attorneys, basically, have to be on call all the time.

So back to those thematic issues. What's the degree of monitoring that is going to be allowed and what's going to be tolerated by your em-
ployees? It may not always be the same thing. I mean, if you put a policy out there that says we are going to look at everything and you're sending it all over our network and we own the device, you know, there is a lot of control and monitoring you can exert over this. Whether your employees are going to like it, and are going to put up with it, is a different question. Also, whether -- there's also a question of whether people will really understand what all that means until things have gone wrong. So you can say, you know, everything you put over work e-mail is subject to monitoring, and someone works for the company for ten years and never has an issue, so they kind of forget about it. Then all of a sudden they're involved in a suit, maybe against their current employer, and they're still using their work e-mail to communicate with their attorneys about that. That's a problem, because now they're basically revealing privileged information to their opponent. In terms of your security versus responsibility trade-off, you've got -- and you got to keep your data -- some companies more than others -- you got to keep your data safe. Especially if you're a health company, you have to keep the data of your clients, your customers confidential because there are some very strict penalties if you don't. If you are a financial company or a tech company, you need to keep your data secret because your greatest asset is your company's data. But at the same time, you may not want the tech overhead and the responsibility of knowing what all your employees are saying constantly. Finally, this gets into the preservation policy. How long are we going to keep this stuff, and what are we going to do with it? Are we going to archive it? How long are we going to archive it for? When are we going to write over our back-up tapes? Is five years too much? Is six months too little? And I can say from experience, that there's a huge variety of opinions on what people need to do and what companies think they need for their business. Some companies really want the ability just for their own recordkeeping to be able to go back and look at ten-year-old e-mails, because they've got people developing products in real time over a shared site or over e-mail, and that's just the reference they want to have available. Some companies are more risk adverse, and they want to say, look, if it's more than six months old, I don't want to deal with it. I want it just gone forever, and that's their retention policy. So that about sums it up for the employer's perspective. I'll turn it over to Greg who's going to talk about employees.

MR. GREG POLINS: Thanks. So since I'm doing the employee perspective, I figured I'd talk briefly about my own experience as an employee. As Ryan said, we have all worked previously. We all had careers prior to being lawyers. I worked as a computer programmer for a couple companies prior to going to law school, and that was back in -- I worked
in the financial sector back in 2005 or so right about when iPhones were coming out and right about when companies were having to deal with all these issues. The company I worked for started out by only issuing Blackberries to everyone and not allowing any text messages, disabling -- technologically disabling all text messages, all phone calls for most people, but for higher-up employees, VPs and managing directors, people like that, they actually enabled phone calls, text messaging, and stuff like that, because they trusted them a little bit more. So that was their perspective on it. We -- as an employee there, it was pretty frustrating actually to not have to do -- not to be able to text message or anything like that on my phone. We encountered multiple times where it was very annoying, I'll say that. It kind of frustrated, probably frustrating even for the employees -- employer's perspective, rather. For example, I wanted to do work and I can do it better if I had -- if I was able to text or call, but that was the policy they put in place for that. As iPhones came out, I think they started to realize that there might be an issue, and they started to change their policies as more and more people adopted iPhones. Back in the day, if you recall, there was just Blackberries, and that was pretty much it. Nobody had anything else.

You know, I switched companies and I started working for a sports media company. For that company, I was doing programming, and that company had a policy where they didn't actually allow any of the issued work Blackberries, they didn't allow anybody to merge their work e-mail on to your personal device at all, but they did have, as Ryan alluded to earlier, is a little weird issue where they had an on-call system. Everybody in our department had to be on call for a week at a time, three or four weeks a year. And in order to do that system, what they did was, they had one Blackberry, and we just passed around the Blackberry. You know, you get it one week, you get it another week, and you had a Blackberry. That was yours. There was one e-mail address, so everybody knew that if you wanted an on-call problem solved, you e-mail this one e-mail address, and whoever was there was expected to resolve it in an hour or so. That was your -- that was the system they had in place. It was interesting, and I'll say this, I didn't appreciate it at the time, but looking at it from a litigation perspective now, that is an absolute nightmare. I mean, as you can imagine, if something went wrong in that e-mail account, trying to piece together who had that e-mail account and trying to figure out who actually sent that, three or four or five years down the line would just be a disaster. I mean, sometimes you switch days, you know, someone would say, "Hey, I got something tonight, can you take it tonight, I will do it two days the next week," or something like that. And we would do that all the time, no documentation whatsoever. So I don't even know what would happen with that, but that was their solution, because it was a very easy tech-
nical solution. It was very easy to implement; one e-mail address, one Blackberry, easy for everybody in the entire company to know that if you were going to need a problem solved, you e-mailed that one e-mail address, and that was it, you got it handled. So I don’t know what their perspective was, if they thought about it from their legal perspective at all. If I had to guess, I would guess no, to be honest. But that was what they did. On the flip side, because we only had it for that week, and then when I went home, it was great, nobody had ability to contact me, no expectation that I would respond to e-mail. That was spectacular. I wish I had it again.

(Laughter.)

So now we have -- now I am working at Kirkland, and we have two different kinds of policies in place. One would be not really bring your own device, but you can ask for it, and they will give you a Blackberry if you want. You know, all attorneys have to be accessible one way or another. So the one way to do that is to get a Blackberry. It’s configured. Everything is set up. It is similar to what we were talking about before, no phone, and no text. They assume you got that on your own, and you can choose that way. Or you can choose to do the “bring your own device” in. You bring your own phone in, they’ll configure it for you, and it is set up with certain security parameters to make sure that your data is secure on the phone, and that’s the other option you have. I have done both at Kirkland. I just recently switched. I got a new phone. I got everything on one device. Prior to that, I had a Blackberry that was separate. I’ll say I think I like the new phone better from an employee perspective, having everything on one device, actually ended up being better. My wife probably doesn’t think so, but I do.

(Laughter.)

So it’s just like Ryan was talking about. It’s very tough. It’s a convenience for your employee and kind of getting them accessible. I think potentially having the option available for me, for both options, was probably the best policy from my perspective to have. I could choose which way to go, and it worked out both ways. I did one way and didn’t like it, and did the other way and it’s worked out for me. So that’s kind of my perspective as an employee in general and my experience as that. So we’ll talk through the same stuff we were talking about before with Ryan about the advantages, disadvantages, and the scope of monitoring that is involved. I’ll say now with Kirkland, again, I am just trying to go off my perspective, I believe, and I think this is true, but I don’t know it, that because there is a dual-use device, and I had to bring my own de-
vice, I believe they have the ability to monitor everything I do. I pretend that that ability doesn’t exist, as much as I can. I think that it does, and it could happen, and that’s a kind of disturbing possibility. It’s not disturbing, I guess. It’s just not something I would prefer happen because it’s weird, but it exists. So that’s something that you have got to think about. So the separate accounts, allowing no policy, that’s kind of what I have right now; like I said, the one phone, very simple, very easy. I only have one phone. Great to use, quick responses, everything like that, it’s, got its pros and cons. I do like the ability just to send an e-mail where I’m going to say yes, no, you know, a quick e-mail. It’s great. The in-box clog every morning, I remember when I was at ESPN, I came back every morning when I didn’t have a Blackberry, it was tough. You would have to spend your entire 30 minutes, an hour, and every single day going through your in-box every. So it’s good. The policy against text messaging is something I had at Lehman and that was -- it was okay. Like I said, there were instances where I would have preferred to have the ability to do it. Now, when there’s a policy against text messaging, with some flexibility in case of emergency, the employees will inevitably break it. There is no problem -- there is no concern whatsoever. I think if you have a policy against it, you enable it, you are going to do it once or twice, maybe not as often, but they will do it.

I think from an employer perspective, like Ryan said, you got to acknowledge that; and from an employee perspective, it’s how much do you think of monitoring is going on, because I think you end up using it.

Now, with disabling-- technologically disabling, it works. It's okay from an employee perspective. It's not the best, but it's understandable. From a technology perspective, like I said, I worked as a programmer; it is kind of frustrating to do, depending on your devices. It's not the easiest thing to do to disable everything you want to do. There’s inevitably going to be some way around everything. So it’s just a matter of making sure you get that configuration right, making sure everything is set up. From an employee perspective, it’s making sure that that is not frustrating to use.

So the other policy that we already talked about, and we are going to talk about is separate accounts not allowed at all. That’s what I did at Kirkland for a while. When you have a separate account with the separate device, it’s a little bit nice in the terms of, you can put one account down and just I’m not looking at this for the rest of the night and go on with your life. So that works. It’s a little bit easier to distinguish between the two, and that’s kind of a nice advantage for employees to have to be able to leave it at home. Whether you want that from an employer perspective is debatable, but from an employee perspective, it’s nice.
The no device option is great; they can't expect you to answer if they don't give it to you. That being said, sometimes you do want to answer.

So now the disadvantage for the separate accounts allowed, no policy, we trust you with everything, you're a high-value employee, we trust your judgment. It's like I said, the work life blends into personal life, and it's difficult to get away from. You also have -- when litigation gets involved, a very difficult situation that you have to been involved with. Like Ryan mentioned, when you get involved in litigation, how much are you accessing, how much are you making available to the other side when they say, we want all the e-mails from this employee. Now do you have to give them personal e-mails because you are allowing separate devices?

One thing that happened in a case I was on, --we have been generally speaking about the phones so far, but laptops can also be dual-use devices, as well. You can have a laptop that you bring it for personal use or bring it to your workplace to do a little bit of work or maybe at home, you do a little bit of work on your personal computer, and then, you know, you send it into work, then you work continue working on it, from your work computer. Again, when you get involved in litigation, if you allow that, and you're doing that the question is: how much is discoverable, how much are you preserving, are you making sure you're preserving it? The more personal the device feels, the more employees are likely to have potentially embarrassing information on there.

I have encountered multiple instances where an employee just wasn't thinking about what they were doing and then we ended up forensically imaging the hard drive, and, they come to us and say, hey, just so you know, I've got this on there, and it doesn't look the best for me. But this is that reason and you have got to deal with this, it's a situation, and you will argue about it. You'll get involved in trying to exclude it, making sure it is not used against you, but as you have the shared device, totally shared devices that is an issue that we need to go into. From an employee perspective, you just kind of don't think about litigation at all, which is bad in general when litigation happens it kind of comes back to bite you.

I guess employees are going to break the policy, I think that's just inevitable. So the question is, what you do about employees when they break the policy and how much do you care? I think there is an understanding from an employee perspective, generally speaking, that as long as you're pretty reasonable about what you're doing, as long as you're not egregiously abusing the policy, you're probably okay, but that's not necessarily always true. Because, it can be used against you. I know there's always an issue for employees that are a little bit concerned, maybe I am breaking this policy, and I know all my co-workers
have never gotten in trouble for it, but maybe I will, you never have that guarantee. So it is always a little disturbing to do that.

For the separate accounts, disabling texting, it's just frustrating. Both with separate accounts not allowed and separate accounts allowed but disabling stuff, you need two devices. They are always split between what you're doing. If you go out, you have to -- just put them both in your pocket, which is really annoying. When you're developing policies, thinking about that from an employee perspective, it's really helpful to understand what your employees want to do.

When you have no device ability provided whatsoever, sometimes, like I said, when I had that, there were very few instances, but there were instances where I really wanted to actually work or be available. When I did that, I needed to stay at home. That was the only way to do it. So that was kind of frustrating for me, I wasn't really sure how to deal with that. I didn't like it, but, you know, you give it up a little bit for the advantages.

Now, inevitably, the scope of monitoring is an issue, and like we talked about, the degree of monitoring, can depend on the policy in place. Obviously, the less you have of dual-use devices, the less dual-use you allow, the less monitoring you probably need to do, but when you have policies against certain usages, you know, how much monitoring are we doing, and from an employee, how does that make me feel if I know that they are doing auditing, for example, every month or two of my data or what I'm doing. I can't say that I would like that. You know, I deal with it, but I can't say that I like it. It is just a very sketchy line, and employees feel like you're trusted and responsible, you know what's going on, and, you know, big brother is kind of looking over you at all times. And I think from an employer perspective of a reasonable expectation no personal use, it is just -- I don't know how much people actually obey that. So it's something that you need to take into account when developing policies like this; and, of course, the line between personal use and work use is a very fine line. This is particularly true if you've ever been involved with sales or anything like that. Their business is essentially making personal connections. And so, sending an e-mail about meeting up at a golf course or doing something like that, or meeting up at a bar later, that might be a work e-mail, even though you wouldn't think of it normally like that. So differentiating between the two and figuring out if you have a policy against personal usage, but then they start doing that, what does that mean? How is that even feasible from an employee perspective to even do that? It's tough. So those are just kind of questions to think about as we go forward, and Eugene will kind of give a little bit of view of how to balance between the two, the employer and employee perspective.
MR. GORYUNOV: Good morning, everyone. Thank you for having us here. I do want to leave some time for questions and answers, so I will do my best to somewhat reduce how much talking I do and then just leave the floor open to everyone here. But before I start, Greg, something that you mentioned, Kirkland does -- well, can and does monitor everything you do on your device, including the apps that you install.

(Laughter.)

One of the reasons I know is because I had an app installed on my device. It’s called Talk-a-Ton. It basically allows you to read forums. I read forums about various collectors, you know, things that -- one of my passions is watch collecting, and I always like to read forums about what things are out there, what things are coming out and so forth. Then one of the times that I was having my device upgraded, one of the techs mentioned to me that technically the app is against policy because it allows the user an opportunity to read forums that have more illicit topics. I will leave it at that.

So before we dive into this, let’s kind of set the scene, right. We have a dual-use device. We have a dual-use device policy, and let’s say the policy is more expansive than some of the policies that Ryan discussed. So let’s say we’re not really limiting the particular features that a person can use, but we have the same concerns that Greg talked about where a device may have both a personal and a work e-mail, and a user can use both and essentially comingle the information.

Let’s say somebody sends you a work e-mail. You pick it up. You try to respond. Lo and behold, your work server is down. You cannot respond to the e-mail. Unfortunately, that has happened to me in the middle of trial. The Kirkland e-mail server was down for over 45 minutes, and the issue was, “what do you do?” Lucky for me, I was able to reach out to the various people I work with, and we were able to exchange the information that we needed, and the issue was resolved by the time we actually needed to exchange any documents.

But the question I pose to everyone here is, what if the issue is more -- has a much longer duration? What if the server was down for many hours? What happens then? Is it appropriate for an employee to then use their dual-use device to send a piece of work product using their personal Gmail or Yahoo! or Hotmail account to their colleagues? Again, if a corporation is monitoring the activities that an employee does on their device, the question is, would a corporation, law firm, what have you, sanction that kind of conduct; and does that essentially make your personal e-mail account a work account rather than a strictly personal? I think both of my colleagues have discussed that issue.
I mean, at the end of the day, any time that a corporation permits a dual-use policy, the employees and the corporation need to understand and come to terms with some very basic concepts. If an employee - employees have privacy in the content of their personal information. The question, though, is, if a device is used for both work and personal information that privacy significantly reduces.

Now, the flip side, a corporation then allows dual-use devices, they have to make sure that devices are not used for illicit or illegal purposes. In order to prevent that from happening, corporations need to be able to monitor and reduce possibly some of the features that the employees have access to. So one of the biggest concerns that corporations have is that a work device may be used for corporate espionage, or looking at certain illicit materials. The only way to prevent that is from implementing certain controls on a software level, rather than handing out policy to your employees and hoping that they will abide. A corporate, as I believe Greg mentioned, if you have a personal device that is being used for more -- I think the example was harassment-type situations, well, if an employee is using their device to harass fellow employees but they're originating the e-mails from their personal accounts, I think the corporation who allowed the dual-use policy still have the burden to monitor and curb that kind of conduct. I would also say there is a question here whether or not the corporation, by allowing the dual-use devices, now has the responsibility for monitoring what their employees do. In the case of harassment, taking affirmative action, actually controlling and getting involved trying to prevent the harassment from continuing.

Now, I appreciate the circumstances are different than if you were to have a work-to-work, employee-to-employee live conversation where various people could start speaking and exchanging information in the office that is inappropriate; however, once you get into the personal device policy -- and, again, all of this takes place on a dual-use device -- the question is what is the level of corporate responsibility? Based on all of the cases that we have seen and all the dual-use policies that we have encountered, the corporation who allows dual-use devices actually has a much higher burden to make sure that their employees use it for the right purposes.

Greg mentioned one example that I would love to follow up on. He spoke about sharing a Blackberry device. When I was a programmer, we shared a laptop for support purposes and we shared a cell phone. Every couple of days for -- I think we had 18 members, and we had a requirement that each team member carried the laptop and the cell phone for eight days out of the month. We had a very interesting scheduling policy. Of course, nothing was ever written down. The policy changed and the days that we gave ourselves changed all the time, as
well, and what makes it even more egregious than the policy Greg spoke about, is not only were we exchanging a device that gives you the ability to send e-mails, but we could also provide support from this laptop. We had access to all the corporate resources. We had access to all the servers, and so forth. Now, granted all of us ended up being straight shooters, so this was never an issue for any of us, but you can see the issues that this presents. If you were in a situation where an employee was not a straight shooter and caused certain issues in the company’s servers, for example, or company resources by using this kind of technology to wreak havoc on the back end.

Now, both Greg and Ryan spoke about various elements of a bring-your-own-device policy and what elements it could restrict. And one thing I should mention is that all the examples that Ryan and Greg spoke about on dual-use policies, those are just things that we came up with in order to present this to you. Those are either things that we’ve dealt with directly in our careers as engineers or things that we’ve dealt with or seen other colleagues deal with in the context of document preservation and dual-use device policies. And what I tried to do here is I tried to summarize what various issues can be controlled, texting, personal accounts and so forth. When I first started using a Blackberry for Kirkland, for example, we had a policy against installing the Google Gmail app on the devices. That has since changed. I believe that all three of us have iPhones; is that right?

MR. HUBBARD: Yep.

MR. GORYUNOV: And I will speak for myself. I have Gmail, Yahoo!, Hotmail, and Kirkland on my device, but the benefit of the iPhone is it actually does a really good job with compartmentalizing all of your apps, which is why a lot of corporations prefer the iPhone as opposed to Android devices. While the new Android devices really do have several partitions on the hard drive, the iPhone won’t allow you to attach a document that comes to you within your mail app as an attachment to an e-mail you send out of your Gmail app. That’s the good news. It really makes it very difficult to comingle information. That said, if an employee is very determined, I’m sure there’s a way around that.

So this is something always to keep in mind. And at the end of day, a corporation can control anything and everything that occurs on an employee’s device if they permit dual-use and if the employee takes advantage of the dual-use policy.

This is the last slide. At the end of the day, and what I would like to open the floor up with, is corporations need to have a good balance between the policies that they instill when it comes to dual-use. On the one hand, they need to allow their employees to perform their job func-
tions, whether that be on-call, to be able to respond to e-mails or perform electronic support, like Greg was doing at Lehman and ESPN, as opposed to employees performing illicit acts, getting involved in corporate espionage, and so forth. I think that what is important for all of us to walk away with is that the more expansive a corporation’s dual-use policy, the more responsibility the corporation takes upon itself.

If it allows employees to use their devices for any and all purposes, then the corporation needs to, at least as we have seen, needs to be a lot more involved in controlling the content and the information that is being exchanged using these dual-use devices.

We only have seven minutes or so, so I leave the floor open to questions.

FROM THE FLOOR: In litigation, how do you handle identification of attorney work product -- and I’m thinking of, hiring private investigators and their work product; and if you build a Chinese wall somewhere, all of a sudden three or four years down the road, something you discovered through attorney work product becomes an exhibit or somebody that you want to depose? How do you handle identifying that early in litigation?

MR. GORYUNOV: Well, I think that we can probably all take turns responding and go down the line. In my view, any time that you’re in litigation and you’re looking for documents from a particular individual. Let’s imagine that the person who has the work product or attorney-client information is one of the tactical employees. You would always want to run search terms on their e-mail to identify and all of their documents to identify anything that contains work product. Then once you identify those documents, you will most likely schedule them on a privilege log. Now, all other documents from that custodian are going to be ultimately reviewed by someone. Now, we would never be in a situation where you would just produce the documents without any level of review. So we would have an opportunity to see what work product is and attorney-client privilege and it are highly unlikely that those documents will be produced in the first place.

MR. HUBBARD: So one of the things I think we have seen some companies do -- and actually if done right, I think it can be very effective -- is that some of the policies change a little bit once there is anticipation of litigation. For example, one policy we’ve seen is that certain levels of employees have access to text messages, whatever; but when they are put on litigation hold, technologically that is stripped from their device. So, you know, there’s nothing to be done about documents that existed previously, but now we are at least preventing some of the
key employees who were involved in discussions with attorneys from accidentally creating documents that contain privileged information. Then also admonishing all those employees that e-mail is fine with the attorneys, but, really, you should be mostly having phone conversations at this point. Let’s cut down on the total amount of data we’re actually creating.

Again, this is all once the outside attorneys become involved or if you got a good in-house counsel department, once in-house counsel is getting involved. Ideally before in-house counsel gets involved, there shouldn’t be any work product, because the employee should be going about their daily lives and shouldn’t be doing anything to prepare for litigation if he has some attorneys.

That being said, how do you identify all those things beforehand? Mostly we are relying on the employees who left us clues that there is some instructions to them saying, if you’re working on this for this litigation because we think there’s litigation coming and you’re working with us as a consultant or because you are the subject matter expert for this, all that work has to be done over in this folder so we know it’s there. Or if you’re sending an e-mail that is in any way related to this litigation or copying an attorney on it then that is very easy for us to pick up on the back end. Also you are putting in the subject line as the first line of the e-mail, "This is done pursuant to attorney instruction. Please do not forward ever, ever, ever."

(Laughter.)

"And we mean ever."

Then even -- and, unfortunately, we have both perspectives, so then we sit there and five years later, after litigation has been ongoing, we sit there and go, this guy forwarded my e-mail to ten different people trying to dig up this information. Now what do I do with it; I got to redact parts of it and not others; what part of my instructions was not clear, never forward this ever? Before you know it, ten people see it. So it's tough.

There is a lot of different ways to do it. I think, it’s mostly trying to get in right away and figure out where all of that would be and then a little bit of hoping that it’s in places that are easily accessed and controlled.

FROM THE FLOOR: Have any of you dealt with the health care industry, whether a health care provider, health plan, or their business associates, because if there’s a breach, they carry a much stiffer fine, into multimillion dollars, and I would think those policies would have to be reviewed differently in that context? Do you think even if the use set
today would be different if they had to apply to a health care provider, say?

MR. GORYUNOV: I think that any dual-use policy, especially in the health care context, carries a certain corporate responsibility. As I mentioned at the very end, if a corporation allows a dual-use device and allows its employees to use it, it bears -- it carries a pretty significant burden to make sure that its devices are not being used for improper purposes. It sounds like in the health care context, that burden would be much higher and the policies would actually be open to outside scrutiny. That's something that both Greg and Ryan spoke about. These policies are not set in stone. They're very fluid, and they have to adjust based on circumstances as you learn more about your employees' use cases of the devices.

MR. HUBBARD: In addition, HIPAA is terrifying.

(Laughter.)

I don't think there's a way to sugar coat it. HIPAA is just terrifying, both because of the requirements, the penalties, and also the pure number of people that are employees involved in that organization where things could just go so wrong so fast.

Even a simple "reply all," and all of a sudden every customer is seeing each customer's personal information and you've got a serious problem. So I think the policy would have to be ramped up. You would just have to adjust up. HIPAA is certainly not the only area. There is the financial sector. You got Sarbanes-Oxley and related regulations that really puts some controls on what you have to preserve and where information can go. Really, for some tech companies, you have ITAR and U.S. Export control laws, where if an employee sends the wrong file to even another employee in a different country, everyone is going to jail for years.

(Laughter.)

MR. GORYUNOV: No joke.

MR. HUBBARD: Or even if someone -- and this is even worse -- even if someone had -- even if they never look at it, even if they have access, if you've got an employee in China and an employee in the United States and the employee in China can see certain information, it's related to arms trafficking, but it also applies a lot to computer security technology. If you have an employee in China who can see the confiden-
tial ITAR information in the United States that can be a breach and this can be a huge, huge problem.

So when you're dealing with these more stringent regulations, you're going to need to have detailed policy figuring out what this particular information is and controlling how it's handled, and probably where it's stored and technologically how that can even be accessed.

FROM THE FLOOR: As a follow-up for those industries, would you advocate against bringing your own device policy, whether it's ramped up or not, or against using one device for example, iPhone.

MR. GORYUNOV: So my experience is actually in health -- my pre-law engineering experience is in the context of a health care company. I will tell you that the company was very much against dual-use devices. We all had Blackberry's for our e-mail, but all other features were completely disabled at the server end, not at the actual device side. So while the device arguably could have all these different capabilities, none of them were usable. In a Blackberry, you can set certain policies, which will essentially disable all or some of the features. So, in my experience, the company was extremely against it. We, as I mentioned, shared a laptop, because there was one computer. Everyone knew who would access the system because you have to use a log-in password to get in. Every person had their unique user name and password. We had a separate cell phone that we shared and again, no dual-use policy. So all of the resources were provided to us, and we could take advantage and access the system when we needed to, however, only if it was your turn and -- your turn on the support and if you were in possession of the actual devices. You couldn't do it otherwise.

PROFESSOR DAVID SORKIN: I have a quick question and maybe we will be able to get another one. Both of you mentioned, or at least Greg mentioned that he wasn't sure if Kirkland was monitoring his personal e-mail. Wouldn't there be some disclosure required to the employee if they are or are not doing that?

MR. POLINS: So to clarify, I think they have the ability to do it. The question in my mind is whether they actually do it. I mean, I think it's really difficult -- any policy for a big corporation is, it's difficult to monitor all employees all the time and, really, no company is dedicating the resources to do that. I don't think it makes sense to do that. But, I know they retain the ability to do it.

MR. GORYUNOV: So one thing I will clarify about that. The ability is 100% there. No one actually logs the e-mails.
No one logs the traffic, but any time -- I remember myself when I first had all of my profiles installed in my iPhone for Kirkland use, it was made very clear to me, here's how we encourage you to use your device, here is how you may not use your device. If we feel that there are any questions about your use, we have access, keep that in mind.

FROM THE FLOOR: As a follow-up to that, don’t you need acknowledgment from the employee to say that you know that is happening so that you know that it is being monitored?

MR. HUBBARD: Oh, yes.

MR. GORYUNOV: Absolutely.

FROM THE FLOOR: Isn’t it an invasion of privacy, otherwise?

MR. GORYUNOV: Well, that’s something that I was talking about at the very end. Any time that a corporation creates a dual-use policy, there’s always an amount of disclosure that they make to their employees. If you wish to take use of our dual-use device program, you hereby acknowledge that we have the following controls.

FROM THE FLOOR: Don’t you need like a –

MR. HUBBARD: Signature.

MR. POLINS: Yeah, that happens.

MR. HUBBARD: We all signed our lives away. That is beyond question. The question is, whether or not, as a practical matter, anyone is actually going through and doing that?

One concern for a large company is, you’ve just got so much data that no one is looking through this, or you’ve got some automated system in place that will look for certain things, like a blacklist set of websites or something like that, but we are not reading everyone’s e-mail; and, although, I have to say, the technology is starting to emerge, where even if a person isn’t reading everybody’s e-mail, there could be a very smart computer reading everyone’s e-mail.

MR. GORYUNOV: I will also note that most corporations have policies where you sign an employee policy when you started, and they supplement -- and the corporation may supplement the employee agreement as various other policies are created, and they do not require a separate acknowledgement, as long as the employee is made aware. It's
FROM THE FLOOR: Have you seen any case law out there that relates to an employer's responsibilities when it comes to monitoring a bring your own device?

MR. GORYUNOV: Yeah, it depends on the context; most of the case law that we've seen is in the context of employee harassment. The question becomes, if a company permitted the dual-use device policy, what liability and what duty did the corporation have to identify the harassing activity and then stop it before it became an issue? There's, unfortunately, no consistency between various circuits, though.

MR. HUBBARD: The other place you run into it is spoliation case law, where you should have known that your employees were using their personal information. This is going to be very fact dependent. There was a valid source of documents. It's gone, and so we don't care what the merits of the case were. This is the ultimate worst-case scenario. You got some critical e-mail that an employee sent out using his personal account. It wasn't tracked. It wasn't logged. It was lost. Now we have an adverse inference, and we are going to lose some portion of the case or some issue, because we weren't thinking through tracking down this data.

PROFESSOR SORKIN: I'm afraid we are going to have to stop here to keep this on schedule.

Please join me in thanking our wonderful panel.

(Applause.)

I have to say, I was reminded of a case that happened last week at another law school, where a professor apparently inadvertently used a dual-use device to send a porn link to her students, and the law school investigated. It's pretty clear it was inadvertent, but that hits a little close to home.

We are going to take a brief break. I think we're down to about 11 minutes now for you to check your dual-use devices.

We will resume at 10:45.