



**Barclay Damon Live Presents Cyber Sip™**  
**Episode 40: “Does Anybody Really Care About Privacy?,” With Michelle Merola**  
Speakers: Kevin Szczepanski, Barclay Damon,  
and Michelle Merola, Hodgson Russ

**[Kevin Szczepanski]:** Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I’m your host, Kevin Szczepanski. Let’s talk.

**[Kevin]:** Welcome back, everyone. Today, Michelle Merola joins us. Michelle is a partner and the associate general counsel of Hodgson Russ, where she is the leader of the firm’s cybersecurity and privacy practice. Welcome to Cyber Sip, Michelle.

**[Michelle Merola]:** Thank you, Kevin. It’s good to be here.

**[Kevin]:** It’s great to have you. I’ve been wanting to have you on for so long. I’m glad we could finally make it work.

**[Michelle]:** Yeah. I was thinking about this this morning. I really enjoy talking about this. And what’s really interesting about these topics is there aren’t “tried and true” answers yet, so it’s good to talk to other folks. Everyone’s had different perspectives on the issues, and I’m looking forward to hearing your perspective as well.

**[Kevin]:** Oh, well, thank you. Yeah, I think you’re exactly right. Anyone who tells you they know what’s going on in the world of privacy is probably kidding. So let’s start with that.

**[Michelle]:** Okay.

**[Kevin]:** What is privacy and why do we seem to be hearing so much more about it these days?

**[Michelle]:** So when I hear people talking about privacy, I, you know, I think often at least lay people are talking about a different concept. They’re referring to the right to lead a life free from interference and particularly government interference and frequently personal space. Those are concepts that have been around for a long time, and I think they arise out of the US Constitution, sort of Fourth Amendment concepts where, you know, you should be free from unreasonable search and seizure. So people talk about privacy in that context, and that’s not really what we’re talking about these days for the modern concept of “privacy.” That is different. That’s the right to protect your personal information, your personal data. So that is a field that’s been emerging over the past, I’d say, know, five to 10 years. It’s different than, you know, the other concept because it doesn’t have its bearings or didn’t arise out of a great document like the Constitution. You know, it really started emerging with the rise of the Internet. So as the Internet grew, people started to realize they have all this personal data that can be transferred just so easily. And concerns did start to arise in legislation; has just begun to arise out of that concept. So the privacy that I am talking about and, you know, we’ll talk about over the course of the next few minutes, is that second type of privacy; the right to be, you know, protected in the personal data that you put out there and to



control how it's used. And because of the dangers, I think not only of the Internet, but more particularly social media, it's something that I think people are starting to really focus on.

**[Kevin]:** They are. But let me ask you this: given social media, where people are putting out what they wear, what their exercise routine is, they're taking personal photos of themselves and putting them out there, they're even telling you what they eat—are Americans really concerned about privacy or are we going the other direction? It's the opposite of privacy. And if so, how do you explain the emergence of these privacy laws that seem in some ways to be inconsistent with how Americans, especially younger Americans, view their own personal information?

**[Michelle]:** I think that's a really fascinating question, and I've given it a lot of thought over the course of this practice, and I don't know that I have a clear answer. I think that Americans are definitely late to the game in terms of privacy. I think Europeans do care about it or at least care about it more. I think—it's been about a decade ago that President Obama proposed this privacy bill of rights and he had legislation that was going to back it up. And, you know, they were really pushing it. And it was just dead on the vine. Nobody was interested. I think that, you know, Europeans, for example, for whatever reason, have cared about these concepts a lot longer. They have legislation going back to the '70s where, you know, it was started out as the focus was making sure that your private information wasn't unnecessarily interfered with by government. But over the years, they've started to focus on business. We haven't quite gotten to that standpoint. So I'm guessing a little bit with respect to the American mindset, but I think Americans did get very wooed by social media. We like the connections that we feel on social media and, you know, feeling like you've been heard and, you know, feeling like you make the connections with friends. And because we've been so interested and sort of smitten with that technology, the other parts of it, the dangers of social media have not seemed to come to roost in the same way.

**[Kevin]:** Right.

**[Michelle]:** So I think, you know, social media started and it's been more of an American concept, although obviously at this point everyone's involved in social media. But it started, you know, back in the late '90s, not that long ago. Facebook didn't, you know, launch until 2004 and didn't really gain traction until later. So if you have folks still enjoying that new technology, it's taken, I think, a long time for Americans to care at all about privacy. As you say, they want to tell folks what they're doing. I think it's shifting, but that's something that's...as you said, I think there's some generational issues around it. I...you know, I have a young daughter who is itching to get on social media, and I'm...

**[Kevin]:** Right. And mine are already there.

**[Michelle]:** I bet that's true. And I think over time, Americans generally are caring. But I think it's, you know, first and foremost, an older generation that cares, the legislators care. And I think they are spurred on by what the Europeans are doing. It's my sense of it.

**[Kevin]:** And I think my question was a little misleading, right as I'm thinking of it is: we may want to post our Halloween costumes and our favorite dinner, and where we went last night. But when we're talking about privacy, we're talking about certain specific types of information you don't want people to know, like government IDs, financial information, and in many cases, race, gender, union membership. And it's not so much the risk—I know we're going to talk about the intersection of cybersecurity and privacy. It's not so much the risk that someone's going to hack into your computer system or that of your employer and steal this information. It's that we are increasingly providing this information to big businesses who then turn around and make it available to others so that they can... ostensibly so they can better serve consumers by knowing what we want and when we want it. But really what you've got in the end is a whole lot of very personal, sensitive data out there. And I think we're going to talk about the CCPA on a different episode, but you've got



the federal government and a lot of states trying to wrestle with how we limit the ability of these third parties to use our personal information. So I guess in that sense, it really isn't a dichotomy between social media and privacy. Those two things live together.

**[Michelle]:** They can live together. I think you're dead on with that. I think, you know, whether or not the information that you share about the events that you've been going to, whether those things are private, is a different issue. But I do think that as a society, we become a little desensitized to giving out information. And I think that carries over into the other context that you're talking about when you have to provide your Social Security number, your home address, your email, bank account information. I think sometimes people are just used to sharing. And I think it's that... that we're trying to reel that back in, you know, an atmosphere where we share a lot of other information en masse.

**[Kevin]:** Right? We're used to sharing. And we may think, you know, I do... speaking only for myself, we think, well, my data's out there anyway, so why not provide it to this particular third party? But that's not necessarily the case. Or if it is, you can, as a consumer, control your data or at least have some control over how it's used, and stored, and shared with others.

**[Michelle]:** Yeah, there's a lot of danger... that having personal data of another individual comes with a lot of power. There's a lot of danger that can flow from it getting into the wrong hands. So I know you spend a lot of time in your day job doing cybersecurity work and you know better than anyone, me sharing my information with Company A versus Company B isn't necessarily equal. You can't assure that all the businesses that you interact with have the right levels of cybersecurity protections, and so you should be thoughtful about it. And I'll be the first to admit I've been slow to do that. You should change your passwords. And I think about it all the time, and I don't necessarily get it done.

**[Kevin]:** I know. I don't either. I mean, you should have a separate password for every account you have. Now, I don't; I know I should... I've been preaching about smart passwords, so I think I'm getting better at that. But yeah, I think you can almost tell how concerned someone is with their privacy by how sophisticated their password is. If your password is "password," you're probably not thinking as much as you maybe should about who has your data and what they're doing with it.

**[Michelle]:** Right. And that's another area of dispute, right. I'm sure.

**[Kevin]:** Yes.

**[Michelle]:** Your clients' talking about this, but mine just, you know, what should the password be? And, you know, some of the guidance, is it should be phrases at this point and maybe even up to 64 characters. But that's no good if you're going to post your password on your computer so they can remember it. It's a complicated world and the privacy component of it is what makes the cybersecurity so important I think.

**[Kevin]:** So let's talk about cybersecurity and privacy. That and we're going to delve into an interesting, meaty topic, which is all about what I think is something of a paradigm shift from security to privacy. So when I started in cybersecurity more broadly, data security and technology, we were focused on cybersecurity to protect the integrity of a computer network, to protect, protect data breaches, to guard against, in some ways, the inadvertent breaches. If someone leaves sensitive information out in the open. And I don't think we were thinking as much about the "why." We were doing it to protect the network. We weren't really thinking about protecting the integrity of other individuals' private information. Now there are breach notification laws and they're focused on that aspect of privacy. But what is the intersection between cybersecurity and privacy? Are they the same? Are they different? How do you see it?

**[Michelle]:** Yeah, I think I've mentioned this to you before, but I have, you know, very learned colleagues who see them as being one concept.



**[Kevin]:** Mm hmm.

**[Michelle]:** And I understand why, but I don't. I think they're different. And I think you're touching on the very reason that they're different. There is a symbiotic relationship between the two, but one is, you know, looking towards the consumer. It's providing the consumer with a right to control the use of their personal data. The other, cybersecurity, is looking towards the business and imposing obligations on that business to maintain, you know, the confidentiality and integrity of that personal data and other types of regulated data, like PHI. And, you know, there are banking information that's non-public, those kinds of sensitive data, but that's looking at the business and imposing those obligations on businesses and a way to bolster or operationalize the privacy rights of individuals. So they work together. Well, you know, when you think about the privacy laws that are, you know, coming through from the various states, they each strike a different balance. One might be more focused on the privacy rights of individuals, and one might be a little more focused on the cyber obligations or lack thereof so as not to interfere with business unnecessarily. So it's a really interesting mix, and I do think the two concepts are different. They work together. But you know, what happens with a business is they have to really focus on the cybersecurity, make sure they have reasonable, "commercially reasonable" is the standard. We like to talk about checks and balances in place, and if they don't, they risk violating the privacy rights of individuals.

**[Kevin]:** Right. So they are symbiotic. One does lead to another in the sense that, yes, the stronger your physical, electronic, and legal safeguards are, the more you may be protecting your customers' or consumer privacy. But on the flip side, having strong security controls and protecting the integrity of your network doesn't necessarily have anything to do with whether you know what data you have. You're informing consumers that you're collecting it and you're giving them an opportunity to opt out from the sharing of that information. So I guess that the high-level takeaway is: if you think that in securing your network, you are complying with the panoply of state and in the healthcare realm, federal privacy laws, you're not ... they're two different things.

**[Michelle]:** No, no. You would have teams that may focus on the cyber piece and teams that might focus on the privacy and they will have to work together, but it's not there. You know, cybersecurity is not going to satisfy the state laws that come up.

**[Kevin]:** Right. So I guess one way to summarize it is they're not the same thing, but you do need to focus on both.

**[Michelle]:** Yes.

**[Kevin]:** Now, having said that, we talked a little bit about this paradigm shift, and it's not my idea. It's my good friend Brian Dusek at Mosaic Insurance introduced this concept to me, and I've been thinking about it ever since, and I wanted your take on it. So Brian essentially has said, and we can you can click on the link that may appear in your screen, we'll put it up for you so you can go to that episode with Brian to check out his thoughts. But the idea is that we were focused obsessively and appropriately on security, but there's a shift in our world from security. Not that we're no longer focused on security, but that we're increasingly focused on privacy. What do you make of that? And assuming you agree, why do you think that is?

**[Michelle]:** I think that I do agree. What's interesting, though, is at least for me, one of the hallmark pieces of legislation where these issues came up is HIPAA. And I do a little bit of work with HIPAA. So HIPAA is such an interesting piece of legislation to me because it's both privacy and cybersecurity.

**[Kevin]:** Yes.



**[Michelle]:** And I'm not sure that, you know, everyone thinks of it that way, but the legislators working on that piece of legislation were talking about privacy, but they have both a privacy piece of it and a security piece of it. And they felt that they should work together. And I think that makes sense with protected health information. But for some reason, that concept didn't bleed into other areas where there's sensitive data. I think the cybersecurity pieces that came out of HIPAA, Gramm-Leach-Bliley Act in the financial realm, those became just really critical. People do recognize that they were there to protect data, but they weren't...I don't think people have thought about, you know, their rights in that data. They've just thought about a more general concept of securing data. But you have a right in your data and, you know, that right is borne of the concern that something malicious might occur with respect to it. But I think, you know, those concepts weren't on the forefront, at least of, you know, the average consumer. As these breaches have taken place—and they're taking place daily, especially in healthcare—I think that that's causing a bit of a shift where we start to think about the privacy, my data, I want my data protected, and then the combination of the EU legislation, the GDPR, which really is more privacy focused, it has cybersecurity in it, but they're foremost concept was... it's a consumer rights statute, human rights statute. And I think a number of these concepts have come into play that caused that shift you're talking about. But it doesn't necessarily make complete sense to me when I think about, you know, HIPAA as being the genesis for some of this stuff, but...

**[Kevin]:** I think you may have touched on it. HIPAA happens to address health information, which many Americans may hold most sacred. And so that may have been part of it. But I think you've really hit on it. It's not just data, it's my data. And we're thinking more about the rights we have in our data. And I think one of the effects that we will see, although I never underestimate the creativity and zealotry of our friends in the tort law realm, I think that's one of the reasons that we're seeing a proliferation of these privacy-based suits. People are representing classes and bringing lawsuits sometimes very quickly after a data breach is reported to a regulator. And the concept there is that I have a right to my data, and I have been violated because my data is now theoretically, if not literally, sometimes it's not known. But the feeling is that if I even have to think about my personal data being in the hands of a threat actor and that that data could be misused, I've suffered an injury, whether I've experienced a loss or not. And frankly, as someone who, in the interest of full disclosure, defends those data breach class actions, I'm on one side and not the other. But I do get it because as you said earlier, we're both consumers and we've both been victims of these breaches over the years. So what do you make of that, Michelle, and what do you... what should we be looking out for, not just in lawsuits but over the next five years? How if you were to put your crystal ball on the table and anticipate the changes that we're going to see, what do you see?

**[Michelle]:** I do think there's going to continue to be that kind of shift that you're talking about. You do see consumers becoming much more concerned about data breach activity. What you don't see is a number of these laws create rights to access information that businesses hold on them, to ask questions about how it's being used, to restrict the way their data is being used. I know my law firm and many of my clients have started to put in place these programs around privacy and data subject access requests. So you have the right to... you can, you know, reach out to my firm and I would, you know, start this process of answering questions. We haven't, you know, we've had this in place for quite some time and haven't had questions around the data that we hold. So I don't see Americans, you know, have not yet reached that phase where they want to actively or maybe proactively manage their data. I think that that will start to happen. In the meantime, for businesses, I think things are really going to get worse before they get better, because what we've seen happening is, you know, this patchwork of different obligations, legal obligations through law. So now we're at present we're at seven states with privacy laws that are, you know, more like GDPR and focused on privacy more than cybersecurity. In addition, we still have the industry-specific laws, mostly at the federal level, in the healthcare, banking, credit reporting areas. So we've got those and sometimes they can conflict and that creates some confusion. And then we also have legislation, again more in the federal arena, but some state as well that deals with certain segments of the population, so primarily children. And who else do we have, drawing a blank...oh students, FERPA. Right. So, you know, so children through Children's Online Privacy



Protection Act and FURBO, which deals with educational records. So we've got those three types of laws that are all interacting on the same concepts. I think that that's going to be incredibly onerous. Like you said, I'm part of my office of general counsel and I have to operationalize, you know, the, the procedures for dealing with all of those. I think that's going to be a huge burden. And the problem is we're all sitting around waiting for federal legislation to cure this problem. There is a leading bill out there, the American Data Protection Privacy Act that was in committee and made it out of committee. But then we are in a new Congress so it has to start all over again. And but there's a lot of controversy about a number of the provisions, including the preemption provision, which, as you know, is will the state laws preempt the federal legislation in any way? And I think it's going to take a long time to sort that out. So I see, you know, it being a difficult time for businesses, particularly in states that are California, like, you know, have an approach, sort of like California, which is very pro-consumer. And New York will be...when New York gets its act together, which I think will be soon, I think we're going to look at something similar to California. So I think that means, you know, in particular for businesses that you're going to need to have folks who deal with privacy. It's... you have a new department that you have to put in place. You've got, you know, accounting and human resources and IT, and now you have a privacy department, I think, and especially if you're in multi-state business. So I think there is all of that to look forward to while we, meanwhile educate consumers about, you know, their rights and their data and theoretically, they may show more interest in it.

**[Kevin]:** Right. I... we've got a few minutes, a couple of minutes left.

**[Michelle]:** Okay.

**[Kevin]:** But I was going to ask you if you had a business coming in today and you had to give some specific advice. You could tell them one thing about the privacy landscape today and what they need to be thinking about. What would it be? And I guess one of them would be: you need to be thinking about privacy as the new HR. You need to be focused on this and have a dedicated team with the experience to handle it. What other advice? If you could just say one more thing to a client that came in the door and said, "Michelle, what do I ... What do I do? How do I grapple with all of this?"

**[Michelle]:** I think it's primarily those things and having someone, you know, as we touched on at the beginning of this, there aren't people that have all the answers but have people that are sensitive to it. And then I think having good disclosures—that always makes the regulators happy, as if, you know, you have a privacy policy that's clear and accessible on your website. I think disclosures go a long way to satisfying regulators and consumers. So those are the things that I would focus on. But I think you want to put a team in place, like you said, that has sensitivity to these issues and some experience.

**[Kevin]:** Right. Well, that's great advice. We're going to have to leave it there. I think that's a good place to leave it. Thank you so much for coming on.

**[Michelle]:** Thank you. And I enjoyed talking to you.

**[Kevin]:** Oh, I enjoyed it, too, was a great conversation. And I would love to have you come on another time to talk about the changes to the California privacy laws, because I think those are laws that we are looking to as bellwethers in places like New York, but really around the country.

**[Michelle]:** Agree. Thanks so much, Kevin.

**[Kevin]:** Thank you, Michelle. Michelle Merola joining us on Cyber Sip. We hope to have her back soon—and we will be back soon with another episode.



**[Kevin]:** The *Cyber Sip* podcast is available on [barclaydamon.com](http://barclaydamon.com), YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

*This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.*

*Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.*

*Thanks for listening.*

