TABLE of EXPERTS DATA PRIVACY

SPONSORED BY
Bradley
Bradley Arant Boult Cummings LLP

STEVE SNYDER is a board-certified specialist in privacy and information security law and senior attorney at Bradley Arant Boult Cummings LLP. He is a member of the firm's Cybersecurity and Privacy and Financial Services Litigation teams. He leverages his industry experience as a network engineer and cyber risk manager to assist clients in navigating increasingly complex matters related to data protection arising from emerging technologies. Snyder is a thought leader in privacy and data security and routinely writes and speaks on cybersecurity topics. He advises on all aspects of clients' privacy and data security programs and regularly works with technical, legal and business stakeholders to mitigate security and privacy risk. Snyder is an ABA-accredited privacy law specialist by IAPP and treasurer-elect of the privacy and data security section of the North Carolina State Bar Association.

ERIN ILLMAN, a board-certified specialist in privacy and information security law, is a partner at Bradley Arant Boult Cummings LLP. Co-chair of Bradley's Cybersecurity and Privacy Practice Group and leader of the firm's fintech team, Illman is an experienced thought leader in privacy, data security and the integration of technology into business practices. She is a dynamic problem-solver with a strong understanding of U.S. and international private-sector privacy laws and regulations and the legal requirements for the transfer of sensitive personal data to/from the United States, the European Union and other jurisdictions. In addition to providing proactive privacy and information security compliance and legal advice, Illman manages privacy-related enforcement actions and litigation. Her practice includes representing companies in reactive incident response situations, including insider cybersecurity threats, electronic and physical theft of trade secrets, and investigation, analysis, and notification efforts with respect to security incidents and breaches. She was listed in *North Carolina Lawyers Weekly* "Leaders in the Law" in 2018 and in *The Mecklenburg Times* "50 Most Influential Women" in 2019.

LISA LAVIGNE is certified as a privacy law specialist by the American Bar Association and was the first Tennessee-licensed attorney to earn the privacy legal specialist designation. She also holds the CIPP/US and CIPM designations. She has been a practicing attorney since 2005 and has worked primarily in government, financial services and health care. As in-house counsel, LaVigne assists lines of business in new projects, daily operational issues, litigation and transactional work. She has served on the board of directors for the Memphis Bar Association, as a hearing officer for the Tennessee Board of Professional Responsibility, and is currently serving on the Charlotte Chapter of the Association of Corporate Counsel Women's Committee. She is active in the Leadership Counsel on Legal Diversity. LaVigne has been published in the *Specialty Pharmacy Times* and served as speaker for Global Advocaten and the Association of Corporate Counsel. She serves her community through the Junior League of Charlotte and has earned an award for her work with the Ronald McDonald House.

SCOTT MICKLE is the global privacy leader for Red Ventures, responsible for the development and implementation of the enterprise-wide data privacy program. He advises on compliance with various privacy laws and regulations and develops and maintains procedures related to the collection, use, sharing and disposal of personal information. Mickle leverages his experience in sales, marketing and entrepreneurship to guide business teams operating in an increasingly complex regulatory environment. Prior to joining Red Ventures, Mickle served clients as part of a "Big Four" consultancy helping companies evaluate, prepare and enhance their privacy programs. He earned his Master's Degree from Wake Forest University and is a certified privacy professional in the U.S. and Europe (CIPP US/E) by the International Association of Privacy Professionals (IAPP).

(left to right) Lisa LaVigne, corporate counsel, Premier Inc.; Scott Mickle, global privacy leader, Red Ventures; Erin Illman, co-chair of Cybersecurity and Privacy Practice Group, Bradley Arant Boult Cummings LLP; and Steve Snyder, senior attorney and privacy law specialist, Bradley Arant Boult Cummings LLP.

photos GRANT BALDWIN

Companies must navigate public sentiment and ever-changing laws to in order to keep growing

The nation's toughest data privacy law takes effect in California in January, giving that state's residents new rights to have a say in what big businesses do with their personal data.

The legislation is the latest development in a rapidly evolving area of law that forces companies to comply with new standards after years of doing as they please with customer data. Starting in 2020, all California residents will have the right to ask retailers, restaurants, banks and other companies to provide them with any personal information they may have, ask those companies to delete their personal information or opt out of allowing it to be sold.

"There used to be this adage to run fast and break things. Get your market share and don't worry if you are 100% within the letter of the law," says Steve Snyder, senior attorney and privacy law specialist with the law firm Bradley Arant Boult Cummings LLP. "That is increasingly hard to do in this data privacy realm. Even if you get there, if you have practices that don't fit into the regulations, you won't get to the next step if you want to get acquired or get funding. Five years ago it was a free-for-all for data."

Snyder made his comments as part of a panel discussion of data privacy experts convened by the *Charlotte Business Journal*. Attorneys and in-house data experts surveyed the financial, operational and reputational risks businesses face if they ignore shifting sentiment on data privacy. Joining Snyder on the panel were Lisa LaVigne, corporate counsel for Charlotte-based health care company Premier Inc., Scott Mickle, global privacy leader for tech firm Red Ventures, and Erin Illman, co-chair of Cybersecurity and Privacy Practice Group at Bradley. *CBJ* publisher T.J. McCullough moderated the discussion.

Panelists discussed how companies must navigate the new fundamentals of data privacy, the changing landscape for regulation and compliance, and the potential that legislation first passed in California may spread throughout the country, creating a patchwork of disparate regulations. Finally, the panelists offered their best practices for getting ahead of the increasing risk.

Why is privacy an important area for businesses to focus on?

Illman: Data has always been an asset for businesses, particularly as technology advances and the use of data diversifies. Within the last several years, however, with high-profile data breaches in the news, consumers are paying more attention to how businesses use personal information. Now, data has become a liability. Privacy is critical for any business strategy. In fact, we are beginning to see privacy as a tool to obtain a competitive advantage and to strengthen a brand. For example, Google just purchased Fitbit, and Google's privacy reputation may come into play as people consider whether to continue to use Fitbit or to go to a competitor.

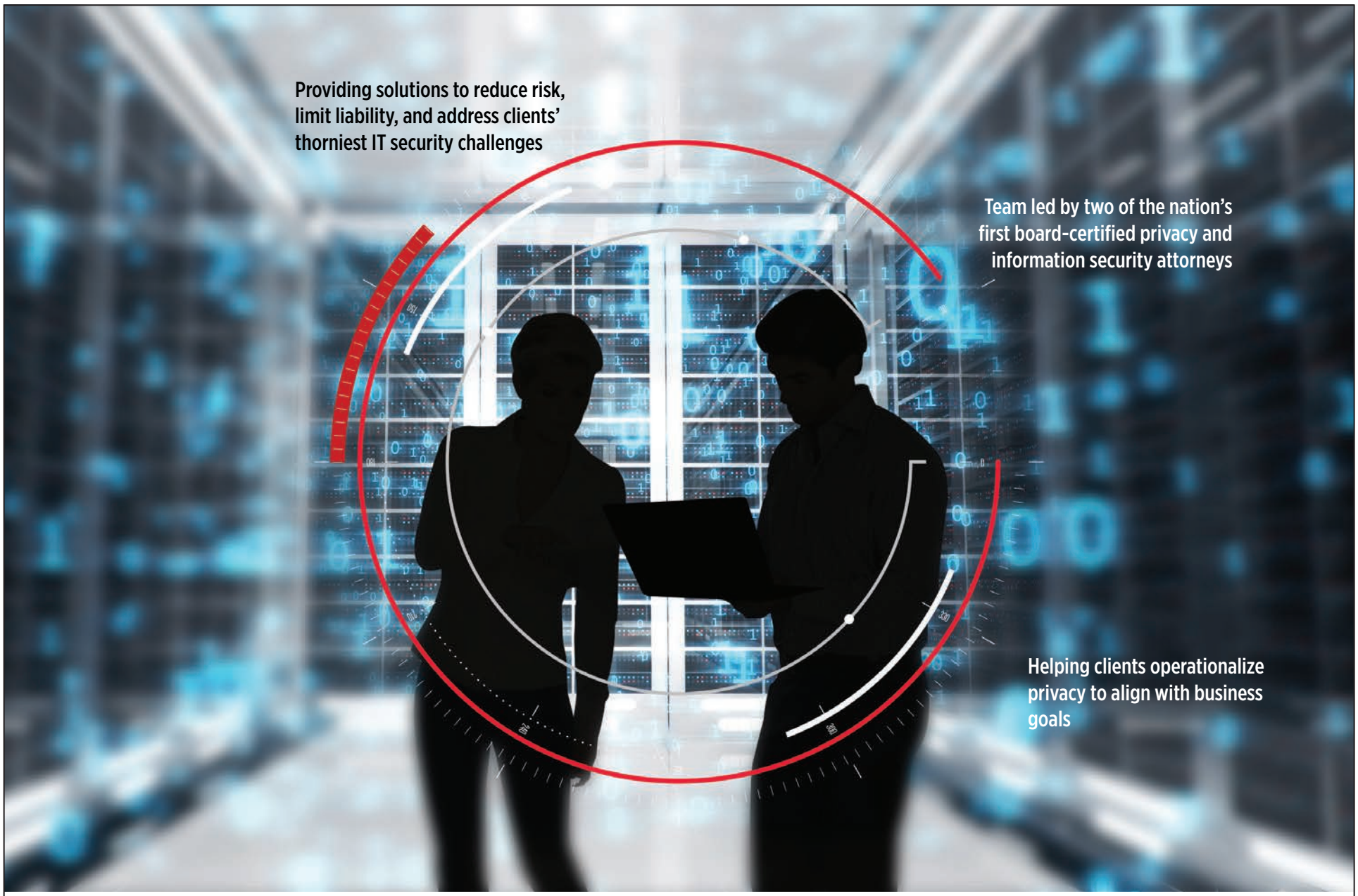
How do you determine where you have privacy risk in your business model?

LaVigne: It's important for every business to look at where they are doing business and what data they are touching as part of that business. To begin to understand a business's data and the associated risk, I recommend mapping out the data within the business model. Generally, this should capture: what data does the business collect/have, from where is the data collected, how is the data used, and what are the data flows. Based on the resulting data map, you can begin the analysis of what laws and regulations apply. This process will help a business begin to understand where its risk lies.

How is the definition of Personal Information changing, and why does this matter?

Mickle: The definition of personal information has changed a lot over the last several years. When you look back at where privacy law started, you were worried about a person's contact information, their name, their address, their phone number, maybe their email address. The (EU's) GDPR (General Data Protection Regulation) along with some of the other laws that have come out have changed that. Now your IP address is personal information. The definition now has gone from everything that is directly linkable an individual to everything that is reasonably linkable an individual. Then when you get out to the inferred area, it really starts to encompass almost anything.

For example, your company has an app and you know the type of transactions a customer is doing on their credit card, and you also have



Focused On You

As business and technology evolve, Bradley knows that ensuring information security to protect business assets is a necessity for companies in today's rapidly changing environment. Composed of experienced attorneys based in 10 offices across six states and D.C., we quickly and efficiently assemble the right multidisciplinary team to provide tailored counsel to clients in various industry sectors and regulatory schemes at each point of the data management life cycle. At Bradley, we're focused on helping you keep pace with and stay ahead of the complex legal world of cybersecurity and privacy.

For more information, visit www.bradley.com or contact Erin Illman, Co-chair of the Cybersecurity and Privacy Practice Group & Board Certified Specialist in Privacy and Information Security Law, at eillman@bradley.com, 704.338.6052

Best Lawyers BEST LAW FIRMS U.S.News & World Report 2020

Bradley®
Bradley Arant Boult Cummings LLP
bradley.com

BIRMINGHAM | CHARLOTTE | DALLAS | HOUSTON | HUNTSVILLE | JACKSON | MONTGOMERY | NASHVILLE | TAMPA | WASHINGTON, D.C.

No representation is made that the quality of the legal services to be performed is greater than the quality of legal services performed by other lawyers. ATTORNEY ADVERTISING.
Contact: Christopher C. Lam Esq., 704.338.6059, clam@bradley.com, Bradley Arant Boult Cummings LLP, Hearst Tower, 214 North Tryon Street, Suite 3700, Charlotte, NC 28202. © 2019

"It's important for every business to look at where they are doing business and what data they are touching as part of that business."

— Lisa LaVigne, corporate counsel, Premier Inc.

"How do we benefit from all of these wonderful technologies but not at the cost of you being afraid to walk down the street because you are being photographed by everybody's house?"

— Scott Mickle, global privacy leader, Red Ventures

their location data. The location data potentially identifies where they attend from a worship perspective and their transactions disclose where their tithings or contributions are going. Combining these two things you can reasonably infer that person's religious affiliation. Now you are into a protected class of personal information. You don't actually have it and you never asked that person those questions, but it's very easy to infer based on the information that you have. That's one of the things I think people in the United States struggle with. I have to answer that question all the time.

Illman: Personal information is not just linked to a person, it now includes that person's device. It's anything that person uses to connect online and any device where information is being collected from. That's another area where the definition of personal information has really expanded.

LaVigne: In health care, there's so much training that goes on around Protected Health Information, PHI. People in my industry tend to focus mainly on the PHI aspect, but you also have to be concerned with the PII, the Personally Identifiable Information. It's an additional level of awareness and training we provide to have a comprehensive privacy mindset within our culture.

Snyder: We run into that as outside counsel, as well. A lot of companies have this historical view of PII, that it's just credit card information or other Social Security numbers. So even if you give them the definition from the California Consumer Privacy Act and say this is what we are concerned about, they often tend to revert to their prior conception when responding.

How would you advise a brand new business to design its data management practices to accommodate present and future trends?

Snyder: The nice thing about a brand new business is that you have a chance to start from scratch. One of the biggest challenges businesses face is reinventing how they manage data with regulations and compliance requirements that are being imposed on them in some cases pretty abruptly. You have practices that you have been using for 10 to 15 years and suddenly, their practices might violate regulations with significant penalties. When you start from scratch, you can build out your data management to be agile to allow you to keep everything discrete and include ways to tag and classify data to allow for options you might not even know right now. It is more compliance by design.

Illman: We get to see both ends of the spectrum, established companies already in the market and startup and fintech companies that are just starting to examine what their business is going to look like and how they are going to collect and use data. We have started to see a trend with startups where they want to build their brand by protecting data and making that part of their marketing strategy. That in some ways puts established companies at a disadvantage because they can't pivot as quickly as small companies.

Mickle: When you talk about designing a data management strategy, it's difficult for smaller companies to have the ability to respond to a request to delete someone's information. Those are not processes that American companies — big, small or indifferent — have thought much about. They have never had to step back and say, "When I store this data, can I go back and delete it, or will I have to have a different solution." Part of the data management strategy isn't just how you collect and protect it, but it's also about operationalizing all these new rights consumers have.

What advice would you give a fintech company or startup to get representation?

Snyder: I don't think they can ignore it. In the past there was an idea that we are going to build our business out and worry about compliance and legal representation later. Now they need to at least educate themselves to understand the high-risk areas or avail themselves of incubators where they might get some guidance that will guide them away from the pitfalls.

Illlman: From a cost perspective, creating a data management and privacy plan is not as expensive as companies presume it's going to be. It will save them so much more money in the long run. It's a great investment if it means your business is going to be acquired because your data practices are inline with industry standards or you get funding because you are in compliance with privacy and cybersecurity requirements. As advisors, we can help issue-spot and make recommendations on how to pivot your business model to meet regulatory expectations.

LaVigne: With the changing privacy landscape, it's hard to envision a business taking off and being successful if they haven't invested in the right resources to develop their product and their structure. Just like you would invest in good office equipment, you also have to invest in the right privacy resources. You can't do it on your own. Find a law firm that specializes in data privacy for your industry. When you hire the right outside counsel, they generally spend less time researching because they are already knowledgeable in the law and can focus on how the current laws impact your specific model.

Mickle: As someone who works at an organization that has done a fair amount of M&A, we (privacy and security) are at the table early. We have an entire section of due diligence just on these topics. As a buyer your privacy and security processes are not

something we are going to wait to find out after the deal. As a seller, it should be part of the pitch for why the buyer should pay the premium.

What does the future hold for data privacy regulation and data privacy more generally?

LaVigne: What we are seeing now is privacy regulation at the state level. Everyone is aware of California's new privacy law. I don't think it's the last state privacy law we will see. State AGs are starting to take more of an interest in privacy and build out departments to look at privacy issues. I predict we will see states putting legislation forward that would be similar to or even more robust than California's Consumer Privacy Act. I am hopeful we will see federal legislation that will control and offer more certainly in this space for companies transacting business in multiple states.

Snyder: We are going to see more and more privacy regulation. Data privacy is tied to technical innovation. You see it in examples like facial recognition, which is feasible now from 1,000 feet away. Things like that could not have been regulated 10 years ago because they didn't exist. We get regulations in place but it's very temporary because suddenly there are innovations that lead to everyone scratching their heads on how do we manage this? Innovation outpaces regulation, and regulation plays catch up. Even if we get comprehensive regulation at the federal level, we'll get a brief reprieve before we have new issues raised by technical innovation that they will have to figure out.

Illman: Over the next couple of years, I expect to see more certifications that incorporate best practices and regulatory requirements and become the gold standard for what a company needs to do to hit privacy requirements under U.S. and global law.

Mickle: Tagging on to what Steve said, I was watching TV the other night and one of the home security companies had an ad for a new product that was using Artificial Intelligence (AI) and facial recognition. It can recognize and alert you if it sees a car or a person show up in your driveway. It's like when Amazon bought Ring and started partnering with local law enforcement. I'm not saying these are bad. They have a great safety component. But where is that line between the data that your doorbell has with your neighbor just walking by with their dog being shared with the local sheriff's department? How do companies look to monetize that information in the future, if at all? This isn't about limiting or stifling innovation or making people less safe, but how do we blend these things? How do we benefit from all of these wonderful technologies but not at the cost of you being afraid to walk down the street because you are being photographed by everybody's house?

LaVigne: When I was working for a Registered Investment Adivsor/Broker Dealer, the idea was that you could generate business by cross-selling. Now companies are having to rethink that model because once you collect that data, you have to give notice of how you intend to use it. The whole idea of cross-selling between business units has a layered-on component now. Many times, there are simple solutions to overcome the concerns. Provide notices that cover all of your uses. Provide notices at the point of collection that anticipate future uses. On the other side of the equation, don't retain customer data that is outdated or is no longer useful. That data that's sitting there becomes less of an asset and more of a liability in the event of a privacy incident or breach.

Illman: With all of the conversations around privacy and innovation, I've heard people push for an FDA for data. The concept would be that when a new technology comes out, it would have to be approved for that purpose and the data collection and use would be vetted by an organization at the federal level. While we do have an issue of legislation lagging behind technology, there is a valid fear that this kind of oversight would stifle innovation.

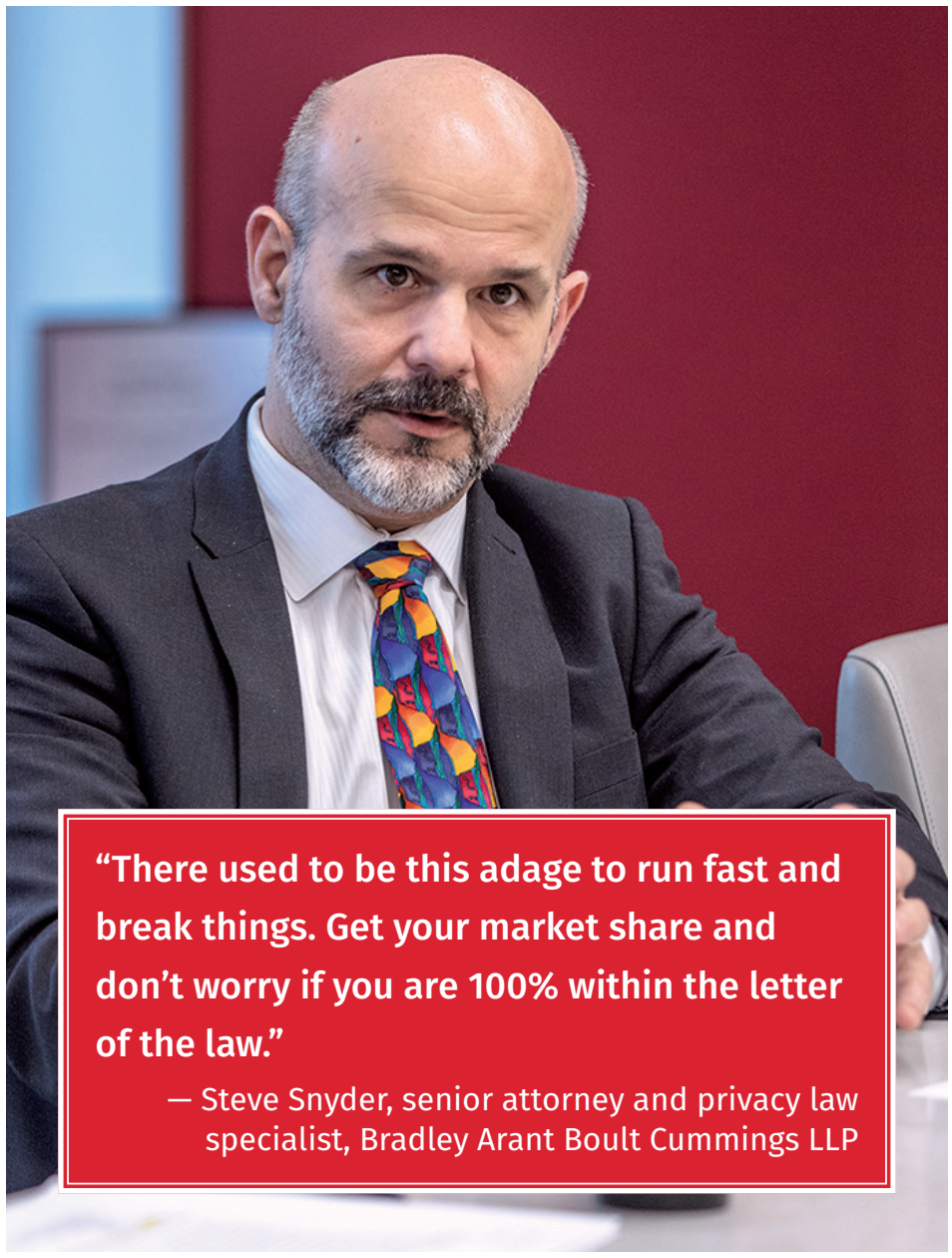
Mickle: It's one of those tough lines. The Federal Trade Commission has about 40 people who have something to do with enforcing privacy. Forty! The primary federal agency that is charged with monitoring these things has less employees than a startup. Then look at the state level and it's same thing. It's hard to figure out what that balance is between innovation and regulation. Take as an example how long it takes to get a drug to market. It takes decades. You are going to do that with technology? That seems like bad idea. But without oversight, people have no awareness of what the risks are and where their data is going.

Illman: Businesses are looking out a decade and thinking this could be a completely different enforcement mechanism if you've got a data privacy regulator at the state level and one at the federal level. I agree that having to go through the process that a drug goes through to get approved would not be good for business.

LaVigne: Small and midsize businesses have a great concern that states are standing up their own data privacy laws. The question I get often is whether they can align policies to the most restrictive state laws. The concern with this practice is that just because a law is more restrictive does not mean that it will capture all of the requirements of other state laws. Also, you may implement policies that become too challenging for compliance and put your company at risk for a regulator to cite you for not complying with your own procedures. This means you are still required to do the state-by-state analysis, which again drives up costs for business.

"Creating a data management and privacy plan is not as expensive as companies presume it's going to be. It will save them so much more money in the long run."

— Erin Illman, co-chair of Cybersecurity and Privacy Practice Group, Bradley Arant Boult Cummings LLP



"There used to be this adage to run fast and break things. Get your market share and don't worry if you are 100% within the letter of the law."

— Steve Snyder, senior attorney and privacy law specialist, Bradley Arant Boult Cummings LLP

Mickle: It's not only states. There are actually cities looking at their own privacy regulations. How are you going to operationalize the fact that if you are in city A I've got to get a different type of consent from you. That's the worst case scenario if there's such a decentralized regulatory environment, that you are dealing with federal law, state law and municipal law. You will have hamstrung business and stifled innovation. Right now there's nothing stopping it.

How is CCPA impacting business? Online versus brick and mortar?

Mickle: A lot of people think about data privacy, and they only think about the online world. For people who run stores, if you meet thresholds for these laws, you are going to have to put notice of your privacy policy and practices on display in the store. No one really knows what that means. Is the store staff going to hand you a copy of their privacy policy? If I walk into a store and I want my data, the customer service desk is going to have to be able to handle that request. It's not just an online issue. It is also a brick and mortar issue.

Snyder: Businesses are collecting a lot of data in brick and mortar. There's becoming less of a demarcation between online and off line. We are all basically all online anyway, and it's going to trend that way more, especially with the roll out of 5G wireless technology.

As in-house counsel, what are some resources you use to help you manage privacy issues and understand the changing landscape?

LaVigne: My best advice to other in-house counsel is to build relationships with the business teams you support. Being effective in-house counsel means cultivating a relationship of trust. Because of my investment in the relationships, my business partners tend to come to me at the beginning stages of issues which allows me to help them get ahead of issues and engage the right players for the conversation. Privacy is a team sport. I have to have the right resources at table to have the right conversation. My company has done a great job of recruiting top talent in this area, and I am grateful to have such amazing resources in my colleagues.

What are the factors to consider in advising clients in an area of law that is rapidly evolving and where organizations possibly face conflicting obligations?

Snyder: For CCPA, some people say this is a law that no one can comply with 100 percent. Everyone wants a black-and-white answer to every question. But these questions have to be viewed from a risk perspective. Companies should view these problems in that lens and consider regulatory compliance as a risk that is dramatically growing compared to other business risks. There are entire industries that are threatened by something like CCPA.

What about the data analytics companies that are going into businesses and trying to mine that data?

LaVigne: We are responsible for every company we engage. If we open our door and let them in, we better have done our due diligence on that company to ensure they are compliant because we own that risk. Really, it's our reputation at stake. We have to hold those we do business with to the same standards we hold ourselves.

Mickle: It takes making sure your privacy teams are working with those analytics teams on what pieces of data are going in that algorithm. I think there is a model where you can do this safely and compliantly. But what you can't do anymore is what happened five years ago when a big data company came in and sold it to a technology officer who gave it to some data scientists and they started to spit out findings and the marketing team reacted to them. This can't happen anymore.

Snyder: For many of these companies, it was the Wild West. "We'll give you this for free, but we are going to take your data and add it to ours." They had no limits on what they could do. The technology officer would think it was a really neat product but not realize they were giving away their customer data. We still see vestiges of that.

Where are the areas that are most likely to get a business into trouble?

Mickle: There are a lot ways to potentially get in trouble, but in my mind there are really two main areas. One is third parties. It's not a day that we don't read a data breach article that points a finger at a third party vendor. It's not that those third parties are bad at data privacy, per se. It's that companies don't always understand where their data is and they don't understand who are all the people who are connected to their system. The other is individual rights. Consumers have been given a set of rights, and if you are not able to meet a minimum standard, that is the most high-profile thing that will get people to complain. If I'm a California resident and I'm not getting back what I want, that's an easy email to the state attorney general. You get enough of those and that's a phone call coming from the state AG.

Snyder: The CCPA has a lot of requirements that are public facing that you can easily test. We are going to find out January 1 who puts the "do not sell" button on their website and who doesn't. And who puts a statement in their privacy policy saying they do not sell your personal information. Because you have to do one or the other. They are basically forcing companies into some form of affirmative representation. Which representation a company makes will be public record, whereas many other historical compliance decisions are behind the scenes and not readily visible to the public.

What are some of the challenges that businesses face in implementing privacy compliance programs?

Illman: Historically businesses have been able to collect as much data as they can possibly get their hands on and retain it forever. They are now having to change that mindset and ask, what data do we really need? And how are we going to use it? Another change in mindset is having a master list of all of your vendors. Traditionally business lines have been siloed with each manager entering into their own contractual relationships. CCPA is forcing companies to rethink how they not only collect data, but with whom the data is shared, and for what purpose. The other challenge is that the privacy landscape is changing so quickly, there is something new coming out daily. We're operating in a regulatory landscape where we don't even have the final law on CCPA, as the comment period runs through December 6. It is certainly a challenge to not only keep up to date, but to anticipate what privacy changes we should be prepared for six months, two years, or five years from now.

Mickle: I left out the most obvious one, which is the financial risk, which is potentially as high as $7,500 per incident. That can be defined as you have information on 1,000 individuals and you email them a hundred times. That's potentially $7,500 times 1,000. These numbers get really big, really quick. That's the extreme case. We talk about the operational risk, but there is a clear financial risk if you thumb your nose to this environment. There is a group of people who will be looking to test things.

What are some of the best practices for implementing data privacy compliance?

Snyder: I heard something recently that I really liked. It's abstracting above the level of compliance to create a corporate policy. It is almost like an ethical or moral outlook on how we treat data. You define these guiding principles, and if you run into situations where there are conflicting laws or you can't quite comply, you can look at these principals to determine what the best course of action is that's defensible. When we do start to see a lot of regulation scrutiny, the really flagrant bad actors that have bad intentions are hopefully the ones that get penalized and not those who did the next best thing from perfect compliance. Maybe they get cut some slack.

Illman: In addition to guiding principals, companies should strive for transparency. That's a big area where you can avoid a lot of conflicts in the law by being transparent on your data practices. That gets you a long way toward compliance.

How do you educate employees about privacy at your organization?

Mickle: There are a variety of ways in which you can go about doing it. At Red Ventures, we have our annual privacy training that gets common themes across for everybody. But we have been looking at the International Association of Privacy Professionals (IAPP) training program for more specific training for specific teams. This can get a small subset of people a little deeper so they can issue-spot. The whole point of training is doing enough with our people so their "Spidey sense" will go off and they will say something about this just seems like I should go ask a question. That's a lot of what our training is about.

LaVigne: Privacy has to be a culture within your organization. It has to be from the top down. It has to be messaged as a high priority for business as a whole. You must develop privacy as a mindset that is part of every decision. We tend to get so embedded in all of the technology and the deep laws, but really it just takes one employee who prints off some PII and dumps in the trash bin and your whole privacy program is blown. You constantly have to send a message out to remind employees that this is everyone's responsibility. If you are an organization that implements a culture of compliance and you have an incident, you can point to all things you did right. Those will weigh in your favor.

"Five years ago a big data company could come in and sell it to a technology officer who gave it to a data scientist and they spit out findings that the marketing team reacted to. This can't happen anymore."

— Scott Mickle, global privacy leader, Red Ventures