March 2019

Daily Journal • California LAWYER

Roundtable Series

CYBERSECURITY

Experts weigh in on this year's significant cyber developments.

SARAH BRUNO
Arent Fox

DAVE WATTS
Chief Information Security Officer
Inovo InfoSec

SA JASON G. WEISS
FBI Los Angeles – Cyber and Forensics Branch

DONNA L. WILSON
Manatt, Phelps & Phillips, LLP

An update on emerging cyber threats, cyber risk mitigation policies, and the California Consumer Privacy Act of 2018.

Sponsored Supplement to the Los Angeles and San Francisco Daily Journals, The Daily Recorder, Orange County Reporter and The Daily Transcript

Cybersecurity

Cybersecurity practice is evolving rapidly to keep up with an increasingly sophisticated cyber threat environment. Practitioners are advising clients on emerging threats and litigation over data breaches, on working with law enforcement following an incident, and on improving and implementing cyber risk mitigation policies. On the regulatory front, businesses large and small are navigating the California Consumer Privacy Act of 2018 and its array of compliance requirements.

Participating in the discussion are Sarah L. Bruno of Arent Fox; Dave Watts of Inovo InfoSec; Jason G. Weiss of the Federal Bureau of Investigation; and Donna L. Wilson of Manatt, Phelps & Phillips. The roundtable was moderated by Rye Murphy of Goldfarb & Lipman.

Participants' comments do not represent the views of their clients or firms.

Participants

SARAH BRUNO
Arent Fox

DAVE WATTS
Inovo InfoSec

SA JASON G. WEISS
FBI Los Angeles –
Cyber and Forensics Branch

DONNA L. WILSON
Manatt, Phelps & Phillips, LLP

Moderated by
DAILY JOURNAL
• CALIFORNIA LAWYER

DISCUSSION

MODERATOR: What are the most common threats and techniques we're seeing cyber criminals use today?

JASON G. WEISS: The risks of cybercrime are growing. Obviously, the oldies and goodies are social engineering techniques that have been used for years such as phishing and whaling.

The problem is many people set up technology, but they don't understand how to operate the technology's security features—how to turn them on or how to configure them.

So our job is to work with the community and inform them of what the risks are. We want to work with corporations; we want to work with lawyers; we want to work with anyone who will allow us to be a partner in trying to secure people's cyber information.

DAVE WATTS: I agree. The oldies and goodies still work for getting into the system. It's the combination of human error and improperly configured systems or incorrect permissions given. It's also a person's curiosity, coupled with them having too many rights and permissions; either that or the networks themselves are not properly configured. You can buy the same piece of equipment or same piece of software and configure them differently and have radically different security results.

I do find, though, that once you get in the door with the oldies but goodies, then some of the landscape has changed. In the old days, ransomware would encrypt whatever it could see but there was some possibility of decrypting it. Now, it often double-encrypts making it much harder to

SARAH BRUNO leads Arent Fox's Privacy, Cybersecurity & Data Protection group and is a partner in the Intellectual Property and Advertising & Promotions practices. Sarah advises businesses on privacy and data security, advertising, trademark, and copyright issues. Her clients come from a variety of industries, including technology, entertainment, retail, and automotive. Sarah's practice has been recognized by *Legal 500* and the *Daily Journal*.

decrypt. It also spreads faster and encrypts your backups better than it used to so you cannot always restore your data from backups. Another common threat I see is that a lot of firms still allow BYOD: Bring your own device.

WEISS: Yes.

WATTS: Firms will allow employees to bring their own laptops, phones, or tablets to work but these devices are usually not properly managed or vetted. Frequently, the networks don't have any method for detecting that there's an unknown or new device on the network.

DONNA L. WILSON: From a legal practitioner perspective, it's really about basic blocking and tackling. People get really focused on the sexier scenarios: the guy in Romania in his basement trying to hack into U.S. companies for purposes of espionage or his own fraud. But every study has shown, and in our experience, the more serious data security incidents oftentimes involve failures of basic blocking and tackling. So, whether it's social engineering—the e-mail to the finance office at the company saying, "Please send me all the W2s," or situations where you have phishing incidents or spear phishing—the basic issues are the most serious security risks.

I think the risk with respect to remote access, especially with the use of mobile devices, is great. You have situations where there's no multifactorial authentication and no network structure to identify whether there's any type of suspicious remote access. Those are the kinds of issues that go back to the basic blocking and tackling. And, oftentimes, people lose sight of them.

SARAH L. BRUNO: I totally agree. I am seeing the same things in my practice. From the tech side, we have these companies that have all of these impressive people and these engineers and programmers and yet, they're moving so quickly that they often aren't, to use Donna's phrase, doing the blocking and tackling. They're thinking four steps ahead and yet they're forgetting things like multifactorial authentication, which many smaller companies are implementing because they're moving much more slowly. The same problems are occurring with large tech companies and little mom-and-pop shops that have one accountant and one HR person and seven employees.

Training is very important, but so is trying to find a way to have a system that you can educate and teach your clients—be it a mom-and-pop shop or a company with 75 programmers just on one product line.

WATTS: That's a really good point. You can have a really fast moving or slow moving system, and you can have the smartest people working for you, but if you don't have the right processes for managing your information security, it's not going to accomplish anything, and, in fact, it could be worse.

One of the things I suggest is that you have a dedicated information security manager who's in charge of and responsible for the information security at a firm. This should be someone at the C suite level or a managing partner. It should not be your IT person. Then, you need to adopt a framework of known cybersecurity controls with which you can align your firm. I highly recommend you adopt the Center for Internet Security's Top 20 Critical Controls. If you do just the top six, you'll prevent around 85% of all known breaches; but if you do all 20, then I think you get to around 98%. Obviously, you can't get to 100. But just

> Regulatory scrutiny can come because of the definition of breach. If you're dealing with a global breach, you may be dealing with different interpretations of whether there was an actual breach, whether data was lost, acquired, or accessed. Your obligations in each of those jurisdictions could be different. You may make a decision that makes you uncomfortable to reveal something to law enforcement in another jurisdiction.
>
> – **SARAH BRUNO**
> **Arent Fox's Privacy, Cybersecurity & Data Protection Practice Leader**

the top six out of the 20 will get you 85 percent of the way there. It's going to be chaotic without a process for managing to a known framework, especially when you have a fast-moving company, like Sarah [Bruno] was referencing.

BRUNO: I agree. I know that we're used to working with organizations that have both a security officer and a chief technological officer: A CTO and CISO. But many of us have been doing this for a long time. It used to be one guy in IT, right? Many of these companies also are now in the habit of having a CISO, as well as a head of IT, which I think is helping with security, but making it difficult to determine who's in charge. Responsibilities need to be laid out and drawn with respect to both areas because I've seen a lot of conflict between the two areas.

WEISS: One thing the FBI has done in Los Angeles is start a new cyber task force, which I helped build, called the Cyberhood Watch, where we are working with industry competitors so that they share technology information about breaches. They're not sharing propriety information because they're still competitors, but, for example, the Port of Los Angeles and the Port of Long Beach are both part of this program, and they share information about hostile actors with each other. If you have a bad actor and an IP address, they're sharing that IP address among the industry, whitelisting all those IP addresses in their system, and working together with the FBI.

One of the things we've done in the Cyberhood Watch is share information with our partners who these actors are, and a lot of our analyst information. It's been a very effective program that's slowly going to spread to become a nationwide program, and it's something that can be done in any industry, even among competitors, even rival law firms, for example.

I know there's a lot of hesitation from private companies and law firms to come to the FBI with problems because they don't want them publicized, but the FBI is not in the business of publicizing people's problems; we're in the business of finding solutions. We have tremendous resources at our disposal, especially in the cyber world. Cyber is becoming the number one single threat on the FBI's list of threat actors. This is a great opportunity to reach out to your FBI partners and let us help you because many of the issues that Dave, Donna, and Sarah have talked about are issues we deal with on a daily basis.

MODERATOR: In terms of these mom and pop places, what kinds of steps can they take from a legal, practical, or liability standpoint?

WILSON: I encourage smaller companies to get cyber insurance and to avail themselves of whatever tools the insurance companies lay out for them. Usually, it's a relatively narrower risk profile. It can be cost-effective. In my experience, the carriers want to minimize the risk and want to assist in all ways possible, and so, they can often offer services relatively inexpensively to help see some of the more glaring deficiencies with respect to cybersecurity.

WATTS: Let's say you can't afford an outsourced information security firm, you can at least choose to actively manage whoever is doing your IT. Ask them which security framework they are using for your company or firm, and if they don't have the answer, maybe they're not the right IT vendor for you. You want to choose a vendor that understands this and has a culture built around aligning you with a particular framework. Again, I would suggest you

align your firm with the CIS Top 20.

BRUNO: I totally agree. Having it in the budget, having an attorney look at that agreement with a forensics company is extremely important. If they can budget for it, it's important to make sure that they have the appropriate indemnity language, and the limitation of liability with respect to data incidents because it's surprising how many of those agreements have vague language that doesn't give much coverage to the company that has the incident.

MODERATOR: Dave had mentioned mobile devices. Have you run into mobile-specific problems recently?

BRUNO: One of the issues that I recently dealt with was business e-mail compromise, in which an individual received an e-mail that looked exactly like his CEO's e-mail. The issue was that it came through the mobile device. It was briefly written to this person in payroll, and it was, like, "Hey, I hear you're the guy that's responsible for the payment stubs. I need the payment stubs for five different individuals. I heard you're really quick. Appreciate your prompt response." So, the guy on his phone felt great about himself, responded by phone, "I am the guy. As soon as I get to my desk, I'll send it to you." Luckily, he had been trained, so the training worked out, but because it came through on his mobile phone, he didn't see that it was different. When he got to the computer, he saw the one character different in the e-mail address, and so he could pick up on it.

So, this is another example of big companies sometimes not having the appropriate mechanisms in place to protect from a phishing incident like that. Many of the incidents that we work on are related to employees sending information to individuals they believe are authorized.

WATTS: That hits on another point: we do phishing training, but we don't specifically change it for mobile devices. So, now, I want to do that. That's smart. Because people get in a hurry. And, also, we have this culture that you have to respond immediately. "Why did someone not respond to my e-mail for 30 minutes? What's wrong with them?" Also, in an e-mail on your computer, you can hover over the link and see where it's going to take you. It's not the same on a mobile phone. So, I'm actually going to adjust our phishing training to include mobile devices. Thank you. That's a great idea.

WILSON: In my soon-to-be new leadership role, I actually have had experience with what was just described. I was on my mobile phone, and someone asked if I sent a particular email. Fortunately, we had warned people that with the change in leadership at the firm, think carefully and don't respond immediately, if something comes out, "Donna Wilson"—for these very same reasons. This e-mail was so close to looking real. Because I was on my cell phone, literally, I got it and I almost responded, "Yeah, I think I may have sent this." It was that good. Fortunately, I looked at it again, and I said, "Oh, no, no. Do not respond to this." But it even gave *me* a moment's pause as to whether, in an average day, I just would have sent that out and not thought about it.

So, people look for it. They look for changes in leadership. They look at LinkedIn. They like to mine to see what they could do with respect to social engineering. It's a very low investment with potentially significant rewards. Again, it's the basic blocking and tackling that companies need to think about, including social media and how much information they share.

Professional services firms and small-to-medium sized businesses alike engage **DAVE WATTS** and the Inovo InfoSec team to reduce cybersecurity risk and exposure and avoid expensive and embarrassing breaches.

Recognized for five consecutive years by the Los Angeles Business Journal as a finalist for CIO of the year, and a regular commentator for California Lawyer and the Los Angeles Daily Journal, Dave and his team use a proprietary, process-driven approach based on industry standards to minimize an organization's cybersecurity risk and identify and fill the security gaps.

Special Agent **JASON G. WEISS** has focused on cyber and computer forensics at the FBI for over 21 years. As a Senior Computer Forensic Examiner, Jason analyzes data and performs forensic recovery for criminal investigations including Cyber, Computer Intrusion, White Collar, Counter-terrorism, Counterintelligence, and Crimes Against Children. Jason has worked over 800 forensic examinations including over 100 cyber investigations. He was instrumental in the creation of three new Cyber and Forensic Task Forces. For this work, he has been nominated for three FBI Director's Award. Jason, who is also an attorney, has also helped create FBI agency-wide policies for maintaining and preserving forensic evidence, including how to identify, seize, and preserve all kinds of digital data. In addition to his work at the FBI, Jason is an Adjunct Faculty instructor at CSU Fullerton.

MODERATOR: And Jason, can you touch on the mobile forensics issues that you're running into right now?

WEISS: Mobile forensics is definitely a growth area, especially as it relates to criminal investigations. Dead-box forensics is slowing down quite a bit because almost everything is being done mobile now. The biggest challenge we have in law enforcement with mobile forensics is encryption. Many companies will have cell phones, but they won't put management software on the cell phones that will allow easy access. So, we probably spend more time breaking into cell phones than we actually spend analyzing cell phones. And this is one of our biggest challenges. The perfect example is the San Bernardino terrorism case, which we worked on in our laboratory down in Orange County. There's a case where he was an employee in the Inland Empire. He had a company phone, but there was no management software on it, so we couldn't break into the phone. So, we actually spent a tremendous amount of time, money, and resources to come up with a way to get into that phone.

Without a doubt, mobile technology and mobile forensics is not going to just be a challenge for us, but for all of your law firm clients. If you're going to have problems, it's going to come from the mobile aspect, I believe; mostly because it's just too easy to exploit. People are not sophisticated yet on how to deal with mobile scams, just as you guys just illustrated with great examples. I would say to companies, if you're going to have a "BYOD" approach to devices, there should be a clear policy on what rights the employer has and what rights the employee has. If law enforcement wants to come in and look at that device, the easier it is, the faster it goes. And that's really what you need in this cyber arena: speed.

From an investigative standpoint, the problem with breach investigation is if you don't move quickly, data is lost; data is destroyed; data is overwritten; data is erased. Speed is of the essence for us, in terms of trying to get access to the devices that you may need us to look at.

MODERATOR: Let's move on to incident response. How do you advise clients who have experienced a breach and are responding to it?

BRUNO: Well, obviously, we would like to have a relationship with the client just because if we do, they typically have an incident response plan already in place. We coach our clients to keep hard copies of their plan with them everywhere. We all know the stories of the incidents that require shutdown of entire systems and nobody had a hard copy of the incident response plan. So, the people who need it should have it in their cars and have it with them.

A piece of advice I give during that first call following an incident is to slow down, relax. Of course, you have to react to incidents, but, at the same time, clients often feel like their whole world is collapsing because they feel somewhat responsible for what has happened. The majority of the incidents I work on typically do not require notification, and we're able to resolve them quickly without there being further follow-up, or a class-action lawsuit, or all of the things you see in the headlines nowadays.

We're constantly dealing with little incidents that no one ever hears about that go away within two weeks or 60 days with no notification. So, I like to try to calm the client down right off the bat and have them just start from day one to give me all the facts, and then, make sure they're aware where consumers are located with respect to any notification requirements. The reason we care about that right off the bat is

> From an investigative standpoint, the problem with breach investigation is if you don't move quickly, data is lost; data is destroyed; data is overwritten; data is erased. Speed is of the essence for us.
>
> – **SA JASON G. WEISS**
> **FBI Los Angeles – Cyber and Forensics Branch**

just because it guides how panicked we should be two weeks after the incident because if we've got data at issue that's covered in a certain state, we may have the clock ticking.

But my first advice, again, is having that plan, and then, being calm and walking through the process slowly on day one and day two, as far as reporting the details and figuring out what happened before you go into the mode where you're starting to think about notifying and calling third-parties about notification.

WATTS: I would also make sure that you tell your IT people, "Do not try to remediate anything on the machines that might have been breached; just disconnect them from the network. Set them aside; don't touch them until you come up with what your plans are." Because it's just as important to know how little was breached as it is to ascertain if you had a breach. If you can prove later through forensics that your breach was very limited, i.e. maybe the machine was breached, but there was no personally identifiable information compromised, then you might not have to do notifications. But you're not going to know that if IT jumps in there and starts working on the machine. You're going to lose your ability to do forensics.

WILSON: The first question I ask is, "Do you have cyber insurance or other insurance?" And I quickly get either the risk manager on the line or the broker to determine what the requirements are to make sure that we can maximize the client's entitlement to any applicable coverages. And, oftentimes, that may include vendors, like forensics, PR firms, counsel, and the like. That, to me, is a critical first step.

The second step is trying to ensure that your client is not doing a DIY incident response project. Following an incident, IT departments may have understandable feelings of anxiety, angst and worry because it happened on their watch, right? Or if the client has a third-party security vendor, the vendor does not want to be blamed. That creates a dynamic where the IT folks want to bring in somebody that they feel comfortable with or the vendor wants to do the "forensics examination."

We always counsel strongly against that. You don't want your clients in a position where they may be subject to a deposition, may have to defend potential conflicts of interest, or a request on the adequacy of the investigation. It's better to bring in individuals and teams familiar with forensics. Just because you're in an IT department, it doesn't make you a forensics expert. And, in fact, we've had to deal with the repercussions where someone in IT has tried to fix a problem and the bleeding continues. It's actually not remediated, or they try to fix the problem and they lose valuable evidence that you might need in trying to figure out the extent of the incident and what was the cause, and trying to remediate forward.

MODERATOR: There was an issue that Jason brought up earlier about the reluctance companies have in contacting law enforcement out of fear that they will publicize an issue. What do the attorneys among us think about if, when, and how a client should reach out to law enforcement?

BRUNO: That's one of the hardest questions we typically deal with when you have an incident, and so many factors come into play. The size and nature of the company; the data at issue; the nature of the incident, and then, the client's temperament with respect to management of the issue and whether we think law enforcement will be help-

ful. Many clients grapple with this, and I've had scenarios with bigger incidents where the decision was made not to notify law enforcement because the incident was so public and so many companies were dealing with a similar attack that their CISO and CTO were reading about in the news. They had inside contacts at the FBI that they were getting information from, but they didn't formally report it as something to investigate.

So, every scenario is different. I've had some smaller companies who immediately go to the FBI and end up not really needing our services anymore or the services of a forensics company. On the other hand, I've had clients who've gone to the FBI where they've gotten no response or it wasn't one that the FBI thought was worthy of an investigation.

WILSON: Right.

WEISS: One thing to note is the FBI is not the one that's going to publicize any kind of breach. We try to work as low-key as possible. We do not go to the media and will not share that information without working with the victims.

There's some inherent reluctance to come to law enforcement, but I think most folks would be amazed at how much support we can provide in a breach, especially if we're brought in early on in the breach.

For example, we do a lot of forensics work. We have the capability to run a great deal of information. We can track down IP addresses and other information. We have huge databases through which we can run such information. For example, we have the single largest malware database in the world. If we can get access to that malware, we can learn a lot about it. We can run it, and we can identify it in usually less than 24 hours.

I don't understand, with all due respect, the aversion to reaching out to the FBI because, ultimately, if we can't help, we'll tell you, and if we can help, I think we can bring a wealth of information, not just to the victims, but to the attorneys as well, and provide information and work as partners in an investigation.

We have tremendous resources available. Specifically, there are three resources I would encourage attorneys to tell their clients about. And, really, it comes down to networking.

One is the FBI's InfraGard program. Every field office in the FBI—there are 56 of them around the country—have an InfraGard coordinator who coordinates networking among citizens in the community, regardless of occupation. It's a great opportunity to not only work with the FBI, but you also get access to our cyber squad. You get access to the people you need to talk to if you need help.

There's a Citizens Academy that the FBI puts on in every field office. We give attendees presentations from our various departments, including cyber and forensics. Everything about the FBI that we can share publicly, we do.

Finally, in Los Angeles, for example, and I think San Diego now has one, too, we have the Cyberhood Watch program where we bring in what we call neighborhoods of various businesses that may even be competitors, but work together from a security standpoint to keep networks safe and secure.

Those three avenues alone offer ways to get help from the inside. They don't cost anything, and can potentially assist you in getting the help you need more quickly.

WATTS: I would like to add one thing. If you're going to work with law enforcement or any other outside party, those decisions should be made by the information security manager; they

DONNA L. WILSON, is the Managing Partner-Elect at Manatt, Phelps & Phillips. She is nationally recognized for her high-profile work for companies facing litigation and government enforcement actions, with a focus on consumer financial services and privacy and data security spaces. Donna has extensive experience in crisis and risk management as well as litigation. She has successfully represented a wide range of clients in heavily regulated industries, including banks, mortgage servicers, auto finance companies, retailers and other financial services, in matters ranging from advice and counseling, to class and individual litigation, to government enforcement and regulatory actions.

Approaching law enforcement is a complicated balance. There's the tension between hoping that the government forensics and resources can help you track down what you need in terms of the investigation and managing other considerations.

– **DONNA L. WILSON**
Manatt, Phelps & Phillips, LLP

should not be made by IT. IT should not be in charge of incident response. All of that needs to be coordinated. You need the information security manager to serve as the quarterback so everything is coordinated and you properly respond to an incident.

WILSON: Approaching law enforcement is a complicated balance, as Sarah mentioned. There's the tension between hoping that the government forensics and resources can help you track down what you need in terms of the investigation and managing other considerations. Whenever you're dealing with a data breach response, you're not just looking at the response itself, but you're really engaging in litigation and regulatory enforcement risk mitigation and management. That's always in mind. Clients, understandably, get really concerned about losing privilege down the line in the event of an investigation or having some other blowback from the government involvement, which is unfortunate. From a public policy perspective, really there should be safe harbors across the board in order to enable companies to feel comfortable about sharing very sensitive information with law enforcement and others, because it's always a tension and there's always that worry.

MODERATOR: Is there a risk of more regulatory scrutiny by going to law enforcement?

WILSON: I've been asked in particularly sensitive matters by law enforcement, for example, to share forensics images or to answer questions that can present issues. Typically, what we will do is we will, at the very least, file a report, if it's warranted, with the IC-3, just in order to be good corporate citizens, balancing the risks that could be involved. That said, you always want to cooperate with law enforcement, and if something is requested, then it becomes a different question.

You have to balance the risks and benefits of affirmatively reaching out to law enforcement. To Sarah's earlier point, many times, you do make a report or you do reach out and it's all about prioritization. Many times, you don't hear back, but you've created a record that may always have the potential of biting you in the future if there's litigation or regulatory enforcement. So it's a matter of balancing risks and benefits. But I want to underscore that we always cooperate with law enforcement when asked.

BRUNO: I second everything Donna said. It also depends on the nature of the incident. And, frankly, regulatory scrutiny can come because of the definition of breach. If you're dealing with a global breach, for example, or one that hits in a few different jurisdictions, you may be dealing with different interpretations of whether there was an actual breach, whether data was lost, acquired, or accessed. Your obligations in each of those jurisdictions could be different. In some cases and with some incidents, you're making some decisions as to whether you'll fall within the definition of a breach in a particular jurisdiction, and you may make a decision that makes you uncomfortable to reveal something to law enforcement in another jurisdiction.

WATTS: I would encourage the customer to reach out to law enforcement if they're open to it, but it's ultimately their own decision to make. It's one of those Catch-22's. If you don't report it, then we're not helping society as a whole fight against all of the threats, but I see why people, sometimes, have some trepidation or resistance to going to law enforcement.

I have had situations where, regardless of who you're working with—outside forensics, law enforcement, or any other outside party—where, sometimes, especially smaller customers, want to get back to production and back to operations as quickly as possible, and they don't want to bother with what they perceive as unnecessary bureaucracy and complication that will slow them down. Whether there's any truth to that is a separate question.

MODERATOR: Jason, coming from the FBI, what are your thoughts after hearing what everyone else has said: That companies are sometimes hesitant to reach out because it's going to be slow, or there may be a risk of scrutiny or future liability and litigation?

WEISS: I think the impression that many in the FBI have is that people don't understand our capabilities. We're able to move quickly and effectively. I think we're a lot leaner than people give us credit for. We could be a tremendous asset to your customers and your clients because our interests are very separate. We're not worried about civil liability; we're trying to catch the bad guy and put the bad guy in jail. That's what the job is.

MODERATOR: On the topic of privacy, which businesses does the California Consumer Privacy Act of 2018 impact the most right now, and how are you advising clients on how to prepare for that?

BRUNO: Well, it has broad reach: if you do over $25 million in gross revenue, or if you receive or disclose over 50,000 records from California residents, or if you derive 50 percent of your revenue from data processing activities. So, those three buckets hit many different companies.

The other part of this that makes it broad is that the definition of "personal information" is more broad than what we've typically had in the U.S., and that, essentially, if you're capable of identifying an individual, it's considered personally identifiable information.

So, smaller companies that maybe weren't doing business in Europe earlier, are now scrambling to get in compliance with it. It essentially has many of the same broad requirements as the GDPR, but now, it's hitting those companies that weren't doing business in Europe.

WILSON: Yes, the scope is extremely broad. Getting data on 50,000 people a year is actually not that high of a threshold. And, I think, many relatively smaller companies are being really surprised that they are subject to this law, or even surprised about the existence of a law. It's going to ensnare many less-sophisticated companies.

It's obviously going to most affect tech companies. But, again, it affects anybody who's touching consumer data. That spans retailers with loyalty programs to social media companies, and Adtech companies—so basically, just about anybody that you can think of.

The other broad aspect here that's a trap for the unwary, I think, is that the statute is named the "California Consumer Privacy Act." One of the hot debates, from a compliance perspective, is who is a California resident? Does it include employees; does it include contractors? To what extent does it sweep people in? And is it more towards the GDPR-type of an approach, or is it something that's more practical?

This statute was enacted very quickly in order to keep an initiative off the ballot. And, as a result, it looks a little bit, I always say, like a sloppy term paper. So, there are ambiguities in it and a lot

> "I would encourage the customer to reach out to law enforcement if they're open to it, but it's ultimately their own decision to make. It's one of those Catch-22's. If you don't report it, then we're not helping society as a whole fight against all of the threats, but I see why people, sometimes, have some trepidation or resistance to going to law enforcement."
>
> – **DAVE WATTS**
> **Inovo InfoSec**

of open questions that will either be resolved by a legislative amendment, regulation by the California Attorney General, or in litigation. And I think that this statute, in many respects, is going to resemble the Song-Beverly Act litigation where you had a statute, and there was not a lot of detail to it. And a number of basic issues had to be decided through litigation, which is, obviously, inefficient and impractical. I call it the "Full-Employment Act" for lawyers for both the plaintiff's side and the defense side.-

WATTS: I read the Act as 50,000 residents, households, or devices. Assuming a California resident could have personally identifiable information on multiple devices that is being collected by these different companies, that could significantly broaden the scope, right? Because 50,000 devices is a much lower threshold than 50,000 people.

WILSON: Definitely. Operationalizing on the compliance obligations is going to be a heavy lift for many companies. For those who went through the GDPR process, it's going to be less of a heavy lift, but you have many companies that this affects where you're not coming from a regulatory or compliance culture such as a retailer or a mom-and-pop chain. All of a sudden, they've got these regulatory and compliance obligations and they don't even know where to start.

For most California companies that tend to be mid-market, the advice we give is to start with the best practice that exists, regardless of whether there was such a thing as a CCPA or GDPR. Begin with data mapping, figuring out what you have, why you have it, do you really need it, and what do you do with it. Work with counsel to define the scope of the data mapping process, and then, look at your policies and procedures and, again, operationalize whatever compliance obligations there might be.

BRUNO: I'll jump on that and say that one industry I think is going to be particularly hit hard is the automotive industry and auto dealers because the business is more segmented, especially with the dealers, but also with manufacturers. They have market-specific models and market specifics, so they were able to avoid the GDPR completely. And many of the dealers had GLB as well that they're grappling with. So, now, the dealers in California, as well as all those auto manufacturers that thought that they didn't have to worry about GDPR, are now in a position of having to look at their entire business model to figure out how to comply with CCPA.

MODERATOR: Are there going to be changes companies need to make in their insurance policies or allowances in insurance in response to the CCPA?

WILSON: The advice we have been giving our clients is to sit down with their brokers and, even better yet, their coverage counsel, and make sure that their policies match up to what are new liabilities.

BRUNO: Yes, I agree with that.

WATTS: I agree. If they have cyber liability insurance, they need to get in contact with their cyber insurance companies before an incident. Because, often, my experience has been that they're going to dictate some requirements in order to pay for whatever response is necessary, whether it be forensics, breach notification, or something else.

In California, there is also a definition of reasonable security that many companies are supposed to uphold. And I believe that's also in the California Consumer Privacy Act, though it's worded slightly differently. In 2016, the California Attorney General's office came out and said that if you're not complying with CIS critical controls, you're actually failing to provide reasonable security.

So, regardless of the statute we're discussing, if you're not aligning your own internal cybersecurity with well-established controls—like NIST-based ones or a subset of NIST, like the CIS Top 20—you're setting yourself up for an ad hoc plan. And I would think that would make it much more difficult to defend yourself following an incident.

MODERATOR: Is geoblocking a practical, realistic strategy for risk management under these statutory privacy laws?

BRUNO: I think geoblocking works or could work with the GDPR, but it has not come up as a viable solution for the CCPA because, frankly, California is a place where everyone wants to do business.

WILSON: And that's one of the challenges. As companies are looking at compliance, the question is do we do this for a subset of our customers? Do we try to segregate and just fulfill these obligations or segregate for California residents, or do we just do it across the enterprise, particularly as other states are starting to pick up on the GDPR and CCPA bandwagon? And I'm finding that a lot of clients are just saying, "You know what, let's just operationalize it across the enterprise and across the country."

MODERATOR: That's interesting. So, I want to touch briefly on 5G. Do you anticipate particular security issues with this burgeoning technology?

WATTS: It's very limited right now. So, it's a lot more hype right now than it is actual reality. However, if it really does provide the greater bandwidth that is promised, then I would think it would further exacerbate the mobile problems we touched on earlier. Mobile-related vulnerabilities and malware will increase as more traditionally stationary functionality moves into more mobile devices due to the increase in bandwidth.

WEISS: In short, it's convenience versus security. People want to be able to use mobile devices quickly, easily, and without restriction, but the tradeoff is security. If you want devices to be secure, by definition they're going to be inconvenient. I've seen that through 20 years of doing forensics.

I would agree completely with what Dave said. At this point, 5G is just too new. But it's going to be a paradise for people who are not good people because it's going to be very easy to hack if people don't configure their devices correctly.