ASSOCIATION OF BUSINESS TRIAL LAWYERS

abtl REPORT

ORANGE COUNTY

Volume XXV No. 2

Summer 2023

Q&A with the Honorable Maria D. Hernandez
By Yanlin Cecilia Chen

Editorial Note: Presiding Judge Maria D. Hernandez is a judge of the Superior Court of Orange County in California. She assumed office in 2009. She spent nine years with the county's juvenile court, serving as the presiding judge from 2014 to 2018. She also created and presided over a dedicated court addressing commercially sexually exploited children and cochaired a committee addressing boys in the child welfare system. She recently launched a Young Adult Court, which addresses the special needs of emerging adults charged with felonies in the criminal justice system. Judge Hernandez has also served the Judicial Council's Advisory Committee on Providing Access and Fairness, as well as the Keeping Kids in School and Out of Court Initiative.

Q: What drew you to the legal profession?

A: It all started with my father. He was and still is the hero of my life. My father came to the U.S. as a child of an immigrant looking for a better life. As Armenian immigrants, they were treated poorly. Despite only having a high school education, he fought for justice and made sure everyone had a voice, regardless of their race or color. His hard work and work ethic left a lasting impression on me from a young age.

-Continued on page 4-

- IN THIS ISSUE -

Social Media Evidence: What You Need to Know
By Dave Sugden

Is social media good or bad? Is it the best way to communicate or the worst? It is, of course, neither and both. Never before have non-celebrities or non-journalists been able to reach millions and display what would otherwise be undiscovered talent. And yet we also find material on social media that falls short of most bathroom stall graffiti standards. Consuming social media is like ordering the seafood tower at a new restaurant. If that first bite of shrimp is warm, leave the plate alone and focus on the dinner rolls.

Regardless of its merit, social media is here to stay and disputes over admissibility or exclusion are commonplace in today's trials. To best handle evidentiary questions about social media, litigators must understand the relevant evidentiary rules and their application.

What Social Media Evidence?

Starting with the obvious, information on social media certainly *is* evidence. In California, evidence is comprehensively defined to include "testimony, writings, material objects, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact." Cal. Evid. Code § 140. "Writing" is broadly defined to include "every other means of recording upon any tangible thing, any form of communication or representation, including ... any record thereby created, regardless of the manner in which the record has been stored." The Federal Rules of Evidence likewise define "writing," "recording," and "photograph" in an expansive way. Bottom line: Anything on social media—whether it's a 140-character tweet or a wordless Tik-Tok video—is evidence as defined in California and federal law.

-Continued on page 5-

President's Message
By William C. O'Neill

More attorneys are receiving this issue of the ABTL Report than at any time in our Chapter's history.

That's right folks, we did it. We broke the membership record that has stood for nearly a decade. Thanks to active participation from you, the Association of Business Trial Lawyers has become a prime destination for talented attorneys and jurists who want to hone their craft and open a dialogue on business litigation issues.

Our programming has been well attended and top notch this year already. And we're just getting started. On September 13, we will have an evening with the Chief Justice of the California Supreme Court, Justice Patricia Guerrero. That discussion will be moderated by our own California Court of Appeal (4/3) Justice Maurice Sanchez.

Our Annual Seminar (October 11-15, 2023) will be held at The Fairmont Orchid on the Big Island of Hawaii. Orange County will play a big role shaping the Annual Seminar's success. My continuing thanks to Vikki Vander Woude (of Umberg Zipser LLP) for her leadership as Program Chair and to Tamara Devitt (Haynes and Boone LLP) as our Chapter Representative on the Planning Committee.

Following right up on our Annual Seminar will be our November 8 dinner program where we will have a tools-of-the-trade discussion about evidence from Senior U.S. District Court Judge (and UCI Law School Lecturer on Evidence) Lawrence O'Neill, U.S. District Court Judge Cormac Carney, and Orange County Superior Court Judge Richard Lee. That night will also be special because it is our annual stuffed animal drive for adoptions at the Orange County Superior Court.

While the quality of our programming and this ABTL Report undoubtedly help us reach our membership records, the best value is in our relationship-building efforts. Thank you to each and every one of you who make sure that you attend ABTL events. You are truly the strength of the ABTL.

♦ *Will O'Neill is a partner at Ross Wolcott Teinert & Prout.*

ASSOCIATION OF BUSINESS TRIAL LAWYERS
abtl
ORANGE COUNTY

8502 E. Chapman Avenue, Suite 443
Orange, CA 92869
714.516.8106
abtloc@abtl.org ▪ www.abtl.org

The statements and opinions in the ABTL-Orange County Report are those of the contributors and not necessarily those of the editors or the Association of Business Trial Lawyers of Orange County. All rights reserved.

Friend or Foe — Is Artificial Intelligence Worth the Risk to Your Business?

By Robert Matsuishi and Connor L. Kridle

INTRODUCTION

As artificial intelligence (AI) rapidly advances, its integration into various industries brings forth an array of benefits, revolutionizing efficiency and productivity. However, alongside these transformative advancements lie inherent risks that businesses must navigate with caution. The emergence of AI technology has given rise to concerns surrounding trade secrets, employment laws, and data privacy regulation. Businesses now find themselves in a complex landscape, compelled to grapple with the legal and ethical challenges posed by AI while remaining compliant as both employers and market participants. In this article, we delve into the multifaceted risks that AI presents for businesses and explore how companies are being regulated in this ever-evolving landscape.

Would you be surprised to learn we didn't write that paragraph? ChatGPT did, in all of about two seconds. This shows just a fraction of the promise of AI tools, and both businesses and consumers are taking notice. One IBM study indicated that around 35% of companies globally had implemented AI in their business by the start of 2022 and an additional 42% had reported that they were exploring AI options. *IBM Global AI Adoption Index 2022*. A Pew Research study also showed that 62% of Americans believe that AI will have a major impact on jobs in the next 20 years and most Americans oppose the use of AI in making hiring decisions or tracking employee productivity. *AI in Hiring and Evaluating Workers: What Americans Think*.

Regulation follows innovation. The rapid development and adoption of AI technologies has led to increased regulatory attention and businesses are under increasing scrutiny for their use of AI. Three areas where this tension is palpable are trade secrets, em-

-Continued on page 8-

A New Era of Privacy Enforcement Has Begun in California

By Travis Brennan and Lila Reiner

California was the first state to enact a comprehensive consumer data privacy law, the California Consumer Privacy Act ("CCPA"), which took effect on January 1, 2020. Civil Code §1798.100, *et seq*. Since then, nine other states (Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia) have followed suit, enacting similar laws that comprehensively govern how businesses may collect, use and share personal information. In November 2020, California separated itself from the pack yet again with enactment of the California Privacy Rights Act ("CPRA"), a large package of amendments to the CCPA that became enforceable as of July 1, 2023. The CPRA ushered in a new era by creating and funding the California Privacy Protection Agency (the "Agency"), which is charged with implementing and enforcing the newly amended CCPA. The Agency is the only regulator in the United States dedicated exclusively to data privacy enforcement.

Businesses should take note of the recent changes to the CCPA and take action to ensure that they will not be vulnerable to Agency audits and enforcement actions. This article reviews the core tenets of California's privacy law, describes key changes that are enforceable as of July 1, 2023, and makes recommendations to businesses to help them navigate this new era of CCPA enforcement.

Summary of the CCPA

The CCPA's core requirements apply to a "business," which is defined as any entity that "does business in the State of California" and satisfies one or more of the following thresholds: (1) has annual gross revenues, from any source, in excess of $25 million; (2) alone, or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers (California residents) or households; or (3)

-Continued on page 15-

-Q&A: Continued from page 1-

He always encouraged me to pursue my dreams and do whatever I wanted, but he emphasized doing it with dedication. What also stuck with me was the desire to serve others, especially those who didn't have a voice. The legal profession was the perfect place to do it.

Q: What are the key experiences that prepared you for your role as a judge?

A: Life has taught me a lot. I learned the importance to communicate well, be open-minded, and be non-judgmental. I also learned to always push myself to do better and give back to the community. These are some of the things that prepared me for this role and beyond.

When it comes to my career, as an adjunct professor at Chapman and Western State, I always tell new law students to explore all sorts of experiences, including internships, externships, and volunteer experience. It is important to find what fits you best.

Q: You are the Presiding Judge of Orange County. Can you tell us about the role of a Presiding Judge?

A: As a presiding judge, I oversee all court operations in Orange County. We have multiple justice centers, 144 authorized judicial officers, around 1600 employees, and a working budget of about 250 million. It's akin to being the CEO of a major corporation. We work to provide access to justice to everyone equally and fairly, resolve issues that come before us impartially, and reach the people who need to be heard.

Q: You are also known for your work with juveniles. What led you to this work?

A: Juvenile work has always been a passion of mine. I spent about a decade in the juvenile court and was the presiding judge between 2014 and 2018. We often talk about assisting vulnerable communities, and I think the youth of this community is where we can have some of the most impactful and important work. I believe addressing the needs of vulnerable youth and families upfront is crucial as it will avoid some of the detrimental consequences on the back end.

I learned this also as a public defender. I spent 16 years doing criminal defense work at the public defender's office. It didn't take long for me to see that, for every capital case I had, the system could have been better at intervening or providing the resources the defendants needed when they were young. It is important for us to think about how intervening with prevention education for the youth and families can prevent what happens down the road.

Q: Can you give us some examples of the work you're doing for the juveniles?

A: We prioritize early intervention and support for families to create a stable environment. One key aspect is ensuring access to education, stable housing, and necessary mental health treatment. We diligently work on these projects, not only for minors but also on the adult side. For instance, we offer collaborative treatment courts. Recently, we are implementing the Governor's directives and statutory work through the CARE Act, which involves working with individuals with schizophrenia in need of proper treatment and stable housing.

In addition to these specific programs, we have various treatment courts and resources to address mental health, housing stability, substance abuse disorders, and interdependency issues. The focus is on providing voluntary programming and support for families to help them get back on their feet and ensure that families can remain unified. We understand the traumatic impact on a child when they are separated from their home, even if it is a bad home.

Q: As a judge and officer of our legal system, what do you think is the role of the legal system in helping minors in our community? What improvements do you think the system can make to better assist minors?

A: We have a unique opportunity to intervene appropriately, including early intervention and prevention with programming and resources as well as collaborating with stakeholders such as social services, healthcare agencies, probation departments, and law enforcement agencies. In Orange County, we have a strong collaborative approach involving various affiliate organizations like OCBA affiliates, ABTL, OCTLA, and many more. Despite our best effort, sometimes there needs to be a forum for people to be heard. The judicial system provides solutions to issues people cannot otherwise get. It is very important that we are available to them.

-Continued on page 5-

-Q&A: Continued from page 4-

Q: You were an adjunct professor at Chapman Law School and Western State College of Law. What inspired you to pursue teaching alongside being a judge?

A: I thoroughly enjoyed teaching, especially young lawyers who are just starting their careers. It's crucial to open their eyes to different aspects of the law and emphasize the importance of being open-minded and finding their fit.

Teaching is also essential to me because it empowers young lawyers and students to understand the privilege we have in upholding our democracy and the rule of law. We must stand strong with our principles and ensure that we fight for what's right. With this responsibility, we can make a positive impact on society and the legal system. It's both a privilege and a duty that comes with being a lawyer.

Q: What other advice would you give to young lawyers at the start of their careers?

A: Networking is crucial, even though it may take some of us out of our comfort zones. As lawyers, we often get comfortable within our circles of friends and colleagues. However, stepping outside our comfort zones opens up numerous networking opportunities within our legal community. Becoming part of organizations and volunteering can be incredibly rewarding. It not only helps you connect with new colleagues and friends but also allows you to learn from others and gain valuable insights.

Moreover, I encourage young lawyers to be bold and take action instead of just talking about it. Being willing to step outside the square box and embrace new challenges can lead to meaningful changes where they are needed most. Remember, when you join forces with others, you have the power to make movements and create positive impacts. So, don't hesitate to get involved and make a difference in our legal community.

♦*Yanlin Cecilia Chen is a Managing Associate in the Complex Litigation & Dispute Resolution Group of Orrick, Herrington & Sutcliffe LLP.*

-Social Media: Continued from page 1 -

Is Social Media Evidence Relevant?

Like any evidentiary question, the first question is whether the potential evidence is relevant. California Evidence Code section 210 defines relevant evidence to "mean[] evidence, including evidence relevant to the credibility of a witness or hearsay declarant, having any tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action." Cal. Evid. Code § 210. Evidence is relevant if it has some tendency, even a slight tendency, to prove or disprove an issue in the case. *See e.g.*, *People v. Carpenter*, Cal.4th 1016, 1048 (1999); *see also e.g.*, *Dorth v. Fowler*, 588 F. 3d 396, 401 (6th Cir. 2009) ("[A] piece of evidence does not need to carry a party's evidentiary burden in order to be relevant; it simply needs to advance the ball."). Asking whether "social media" evidence is relevant is like generically asking whether "testimony" is relevant. There is nothing inherent in social media evidence that provides any special rules in favor or against a finding of relevancy.

Is Social Media Evidence Authentic?

When it comes to authenticating writings or documents (or photographs or recordings), lawyers tend to make things unnecessarily difficult. Whether it's a deposition or trial testimony, lawyers tend to think that laying a foundation for a document requires a long and tedious windup of meaningless and repetitive questions. Authenticating documents (social media documents or otherwise) does not need to be overly complicated. To understand the simplicity of authentication, it is important to first understand exactly what authentication means.

The concept of authentication is closely related to relevance—or, more specifically, conditional relevance. For example, Federal Rule of Evidence 104 states that "[w]hen the *relevance of evidence depends on whether a fact exists, proof must* be *introduced sufficient to support a finding that the fact does exist.* The court may admit the proposed evidence on the condition that the proof be introduced later."

Rule 901, which identifies the requirements to authenticate evidence, includes similar language: "To satisfy the requirement of authenticating or identifying an item of evidence, *the proponent must produce*

-Continued on page 6-

-Social Media: Continued from page 5-

evidence sufficient to support a finding that the item is what the proponent claims it is."

Suppose, for example, a plaintiff sued his neighbor for allegedly driving his red truck across (and damaging) the plaintiff's front lawn on New Year's day. The defendant denies liability on the ground that he (and his truck) spent the New Year's holiday visiting the Grand Canyon. The defendant offers into evidence an undated photograph of himself standing beside his truck overlooking the Grand Canyon. Is the photograph relevant? Unless there is some evidence that the photograph was taken on January 1st, it proves nothing about the defendant's whereabouts on the day in question. The photograph would likely excluded because it's *irrelevant*.

But suppose the defendant testifies that the photograph was taken on New Year's day. The defendant has offered testimony that makes the photograph relevant. Is it now admissible? What about *authenticating* the photograph itself? Doesn't the defendant need the photographer? What about a chain of custody? Is an expert witness required to show that the camera that took the photograph was in good operating condition? Attorneys often assume that authenticating a writing is a significant task—that there is some terrifyingly strict standard to authenticate writings, photographs or recordings. To understand how simple it is, it is important to understand exactly what the rules require. As mentioned earlier, Federal Rule of Evidence 901 requires that the proponent of the writing "produce evidence *sufficient to support a finding* that the item is what the proponent claims it is." California has the same standard: "Authentication of a writing means ... the introduction of evidence *sufficient to sustain a finding* that it is the writing that the proponent of the evidence claims it is[.]" Cal. Evid. Code § 1400. This "sufficient to sustain a finding language" means that the judge does not decide whether he or she is persuaded that the document is what the proponent claims it is, but rather *whether a reasonable jury could do so.*

Returning to our New Year's hypothetical, the defendant could simply testify: "This is a photograph that was taken of me on New Year's day at the Grand Canyon." This testimony *could* be "sufficient to sustain a finding" that the photograph is what the defendant claims it to be (*i.e.*, a photograph of the defendant taken on New Year's Day). Thus, the photograph has been authenticated and would be properly admitted into evidence. But what if the plaintiff called a witness to dispute the photograph? This witness testifies that the defendant told this witness, "I have never been to the Grand Canyon. And on January 1st, I drove across my neighbor's lawn." Is the photograph still authenticated? We have conflicting testimony, but *could* a jury believe the defendant and not the plaintiff's witness? In other words, is the defendant's testimony (if believed) "sufficient to support a finding" that the photograph is what he claims it is? Yes, such conflicting testimony goes to the *weight* of the evidence, not its *admissibility. See, e.g.*, *McAllister v. George*, 73 Cal. App. 3d 258, 261 – 263 (1977).

California's Evidence Code identifies a number of ways in which a writing can be authenticated. It can be done by introducing evidence that the party against whom the writing is offered previously admitted or acted as though the writing was authentic. Cal. Evid. Code § 1414. A writing can be authenticated by the content itself, by the proponent introducing "evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing." *Id.*, § 1421. Even with various examples of establishing authenticity, California's Evidence Code expressly states that "[n]othing in this article shall be construed to limit the means by which a writing may be authenticated or proved." The Federal Rules of Evidence likewise provide examples of how evidence may be authenticated, but Rule 901 states that it is "not a complete list[.]"

When it comes to social media, the same authentication rules apply. Whether the evidence is a written message, photo, or video, the proponent of the evidence has to make a sufficient showing that the evidence is what it is claimed to be. An example of this is found in *People v. Valdez*, 201 Cal. App. 4th 1429 (2012). In *Valdez*, the defendant Vincent Valdez was convicted of attempted murder, and his sentence was extended for gang enhancements. During trial, the prosecutor introduced pages from, what appeared to be, Mr. Valdez's MySpace page. The page included photographs and written notations showing Mr. Valdez's affiliation with gangs and violence. *Id.* at 1433-34. On the page's "interest" section, Mr. Valdez purported to write that he enjoyed "Mobbing the streets and hustling, chilling with homies, and spending time with my mom." *Id.* at 1434. An investigator for the prosecution testified that he printed the pages a year prior to the attempted murder when he was doing Internet searches for individuals associated with local

-Continued on page 7-

-Social Media: Continued from page 6-

gangs. *Id.* The investigator explained that a person's MySpace pages were "accessible publicly without a password, but only the person who has created that MySpace profile, or a person who has a password for the page, may upload content to it or manipulate images on it." *Id.* The investigator further admitted that "he did not know who uploaded the photographs or messages on Valdez's page, who created the page, or how many people had a password to post content on the page." *Id.* The trial court admitted the MySpace page for the limited purposes of (1) corroborating a victim's testimony that he recognized Valdez from the MySpace site, and (2) the prosecutor's gang expert, who relied on the evidence as a basis for the opinion that Mr. Valdez was an active gang member.

After his conviction, Valdez appealed the court's admission of the MySpace evidence. The Court affirmed, and the Court reiterated the standard for authenticating evidence: "[T]he fact that the judge permits a writing to be admitted in evidence does not necessarily establish the authenticity of the writing; all that the judge has determined is that there has been a sufficient showing of the authenticity of the writing to permit the trier of fact to find that it is authentic." *Id.* at 1434-35. The Court explained that "like any other material fact, the authenticity of a document may be established by circumstantial evidence." *Id.* at 1435, *citing Chaplin v. Sullivan*, 67 Cal. App. 2d 728, 734 (1945). The Court reiterated that there was nothing special about social media evidence, but instead the same authentication rules applied: "The author's testimony is not required to authenticate a document (§ 1411); instead, its authenticity may be established by the contents of the writing (§ 1421) or by other means (§ 1410)[.]" *Id.* at 1435. Valdez was "free to argue" that the pages were not authentic, but regardless "a reasonable trier of fact could conclude from the posting of personal photographs, communications, and other details that the MySpace page belonged to him." *Id.*

A similar result can be found in *In re KB*, 238 Cal. App. 4th 989 (2015). In *KB*, the Court reviewed another criminal conviction where photographs uploaded to Instagram were admitted in evidence. An officer had been using Instagram to follow various criminal suspects. *Id.* at 992. When the officer saw photos posted online of the defendant holding firearms inside an apartment, he confirmed his address and probationary status (*i.e.*, the defendant was not allowed to possess firearms). *Id.* The defendant was arrested wearing clothing and in an apartment that matched the photos that were posted online. *Id.* The defendant argued that admitting the photographs was in error because there was no testimony from anyone who actually took the photograph or actually uploaded the picture to Instagram. The Court rejected the argument: "The evidentiary foundation 'may—but need not be—supplied by the person taking the photograph or by a person who witnessed the event being recorded.' In addition, authentication may be supplied by other witness testimony, circumstantial evidence, content and location' and other means provided by law[.]" *Id.* at 293, *citing People v. Goldsmith*, 59 Cal. 4th 258, 268 (2014).

Typical Evidentiary Analysis

Assuming the social media evidence is relevant and authentic, the evidence should be analyzed like any other piece of evidence. There may be hearsay challenges or other reasons to exclude the evidence (such as improper character evidence or privacy issues). These issues have been covered in prior articles, for example, here and here.

Conclusion

The above rules are important and can help litigators and trial lawyers handle admissibility questions related to social media. If the above article was helpful, be sure to share it ... on your favorite social media platform.

♦*Dave Sugden is a shareholder at Call & Jensen. Dave is an ABOTA member and has been recognized from 2020 - 2023 as one of the "Top 50 Super Lawyers in Orange County." This past June, the Trial Attorneys selected Dave as its California Trial Lawyer of the Year. Dave Sugden is the founder of Evidence at Trial (evidenceattrial.com) and provides courses and teaching videos for attorneys.*

-Artificial Intelligence: Continued from page 3-

ployment law, and data privacy. This article will look at each of these areas to help businesses better spot the AI-related risks they face as both employers and market participants.

TRADE SECRETS

One of the most popular and widely used types of AI technology is "generative" AI. Generative AI refers to algorithms (like ChatGPT) that can be used to create (or "generate") new content—including everything from audio, text, images, and video to code or full-blown simulations. Generative AI has applications across industries and within organizations, and businesses are interested in the myriad benefits that this technology provides. But these benefits are not risk-free.

Generative AI works by "training" an algorithm to "learn" how to mimic real content. This occurs over time by, essentially, punishing the algorithm for making content that seems fake and rewarding the algorithm for creating realistic content. To create sophisticated and realistic programs like ChatGPT, the algorithms need to be trained on massive datasets filled with copious examples of all types of real information. A well-trained generative AI program can then use user-generated inputs (like a prompt, asking for the software to write a story or a line of code) to create finely tuned and realistic outputs. To create larger and more detailed datasets that allow for even better training of these algorithms, many generative AI programs rely on data (like the words, code, or other information) that users enter into their programs.

An obvious and serious risk with this technology is what these programs can do with the information that users provide them. Once information is inputted, it is captured and stored. Often it cannot be deleted and could end up being used or reviewed by the developer of the AI application. The information might even be used as a future output to a different user. There is the possibility then that an employee could input a company's trade secret into an AI application and thus put trade secret protection at risk.

Imagine an employee wants to draft an internal memo describing a breakthrough made in her company's process for creating a specific widget. ChatGPT could certainly help. To do so, however, the employee would need to input some information about this breakthrough with enough detail for the program to help write a comprehensible memo. ChatGPT would then store and be able to access any information that employee provided. ChatGPT also could use that same information to train its algorithm, meaning it could end up as an output to a different person's prompt—maybe even a competitor.

Because trade secrets are not formally registered, maintaining confidentiality is essential to the protection of the trade secret. Generative AI may complicate trade secret law and introduce novel risks for businesses.

Applicable Law

Under both the Federal Defend Trade Secrets Act (the "DTSA") and its California analogue (found at Cal. Civil Code section 3426 *et seq*.), the owner of a trade secret must take "reasonable measures to keep such information secret." 18 U.S.C. § 1839(3)(A). In fact, information cannot be a trade secret at all unless it "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Cal. Civ. Code § 3426.1(d)(2). Thus, if the owner of a trade secret does not take "reasonable" efforts to maintain its secrecy, they risk surrendering its status as a trade secret altogether, along with any associated legal protections.

Neither the DTSA nor the California statute define what "reasonable measures" are. Instead, the determination of whether the efforts to maintain secrecy are reasonable under the circumstances is fact-specific, and a reviewing court will look to a range of contextual factors. *See Mattel, Inc. v. MGA Ent., Inc*., 782 F. Supp. 2d 911, 959 (C.D. Cal. 2011) ("The determination of whether information is the subject of efforts that are reasonable under the circumstances to maintain its secrecy is fact specific.")

Though no court has directly addressed how generative AI and trade secrets interact, some analogies from similar situations can be made. For example, in *DVD Copy Control Assn., Inc. v. Bunner*, the California Court of Appeal overturned an injunction after it failed to find trade secret misappropriation for information that had been publicly shared on the internet. 116 Cal. App. 4th 241, 244-45 (2004). In reaching this conclusion, the court explained that "[t]he secrecy requirement is generally treated as a relative concept and requires a fact-intensive analysis." *Id*. at 251. With this in mind, "[w]idespread, anonymous publication of the information over the Internet may destroy

-Continued on page 9-

-Artificial Intelligence: Continued from page 8-

its status as a trade secret." *Id*. That said, "[p]ublication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known" to competitors or other persons to whom the information would have economic value. *Id*.; *Cf. Precision Automation, Inc. v. Tech. Svcs., Inc*., No. 07-CV-707-AS, 2009 WL 116135, *2 (D. Or. April 28, 2009) (holding that posting of information on company's website, even if briefly, rendered it not a trade secret).

Another instructive context is in cases dealing with the publication of trade secret information on things like court documents. *See, e.g*., *Kittrich Corp. v. Chilewich Sultan, LLC*, No. CV1210079GHKARGX, 2013 WL 12131376 (C.D. Cal. Feb. 20, 2013); *Hurry Fam. Revocable Tr. v. Frankel*, No. 8:18-CV-2869-CEH-CPT, 2023 WL 23805 (M.D. Fla. Jan. 3, 2023; *The Equal Rights Center v. Lion Gables Residential Trust*, No. DKC 07-2358, 2010 WL 2483613, *3 (D. Md. June 15, 2010); *HMS Holdings Corp. v. Arendt*, 18 N.Y.S.3d 579 (Table), *8 (N.Y. Sup. Ct. Albany Cnty. 2015).

For example, in *Frankel*, the court explained that, though information that was arguably a trade secret was posted on the court's electronically available docket, because the publication was obscure or otherwise limited, it did not destroy trade secret protection. Even though the information was technically publicly available, it was not easy to access, and Plaintiff's competitors would struggle to locate it. Members of the public would only be able to find the information if they knew specific information about the case because the relevant information was unlabeled and located within a docket entry that contained numerous attachments. These impediments to easy access outweighed the fact that the information was publicly available through a searching inquiry.

Applying the reasoning of *Bunner* and *Frankel* above to the context of generative AI, we can draw some conclusions about how a court might rule on the issue. Information inputted into a generative AI model has the potential to be made publicly available. Even so, the information cannot be easily viewed or disseminated by third parties. Because of the various layers required to potentially view this information, it is possible that a court could find any trade secrets disclosed to a generative AI model are—like information buried on a court docket—still protected. That said, if for some reason the trade secret information was easily accessible (such as, for example, if a specific recipe is given in response to a generic question about how to make a famous soft drink) then it is possible that it could just as easily lose its trade secret protection.

Takeaway

The key takeaway for businesses keen on balancing the risk and reward of generative AI technology is to understand that the "secrecy" of information will be determined by the context of any disclosure and that mere posting of the information online may not be enough to destroy any protection. Still, if a generative AI model is trained on the information and somehow manages to easily spit it out in response to benign requests, it may lose its status as a trade secret.

Businesses should always read and understand the scope of any end-user license agreement provided by the vendor of any generative AI applications it or its employees may use. Many of these agreements used by AI companies allow the company to review, release, or even sell sensitive information shared with it. These generative AI applications also almost uniformly contain unilateral confidentiality provisions, binding the user but allowing the AI purveyor free reign (besides privacy law constraints) to use information shared with it.

These risks should remain top of mind for businesses intent on capitalizing on the benefits of generative AI.

EMPLOYMENT LAW

Increasing Federal Attention

On April 25, 2023, four federal agencies released a "joint statement on enforcement efforts against discrimination and bias in automated systems." *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*. The joint statement expressed commitments by the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Federal Trade Commission to "ensure that these rapidly evolving automated systems are developed and used in a manner consistent with federal laws." *Id*. at 2. The joint statement also provided links to guidance documents prepared by each agency explaining their enforcement roles in dif-

-Continued on page 10-

-Artificial Intelligence: Continued from page 9-

ferent areas touched by AI technology.

This heightened agency attention follows in line with the Biden Administration's push for a unified federal approach to AI, which culminated in the "Blueprint for an AI Bill of Rights" released in October 2022. *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*.

One of the first agencies to envelope AI within its regulatory purview was the EEOC (or the Commission). In 2021, the Commission launched an agency-wide initiative "to ensure that the use of software, including artificial intelligence (AI), machine-learning, and other emerging technologies used in hiring and other employment decisions comply with federal civil rights laws that the EEOC enforces." *EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness*. The EEOC explained that this "Algorithmic Fairness" initiative would "examine more closely" how technology like AI "is fundamentally changing the way employment decisions are made." *Id.*

The Commission's attention to the use of AI and its technical guidance was covered in detail in *Are Your Applicant Screening Tools Violating the ADA?*, published earlier this year. *ABTL Report*, Winter 2023. While the Commission's earlier guidance was focused on the Americans with Disabilities Act, the Commission's recent guidance shows that it is continuing to work through how the use AI technologies applies to the full range of federal antidiscrimination employment laws.

Artificial Intelligence and Disparate Impact Discrimination

On May 18, 2023, the EEOC fulfilled another objective of its Algorithmic Fairness initiative when it released the initiative's second technical guidance document, this time analyzing the relationship between AI technology and discrimination under Title VII of the Civil Rights Act of 1964. *EEOC Releases New Resources on Artificial Intelligence and Title VII*. This guidance focused on the disparate impact certain AI tools may create when used as "selection procedures" for hiring, promotion, and firing. *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964*.

Title VII protects employees and applicants from discrimination on the basis of a "protected class" like race, color, religion, sex, and national origin. *See* 42 U.S.C.A. § 2000e-2(a). This includes both intentional and unintentional, or what is called "disparate impact" or "adverse impact" discrimination. *See* 42 U.S.C.A. § 2000e-2(k). In the employment context, this refers to an employment practice which appears neutral yet has a discriminatory effect on a protected class. An employment practice, like a procedure for selecting which candidates to hire, that results in disparate impact discrimination violates Title VII unless the procedure is "job related for the position in question and consistent with business necessity." 42 U.S.C. § 2000(k)(1)(A)(i).

The EEOC's guidance examines this issue in several different ways.

What the EEOC considers a "selection procedure" is quite broad. The EEOC notes that under Title VII "any measure, combination of measures, or procedure" counts as a "selection procedure" if it is "used as a basis for an employment decision." With this expansive definition as a guidepost, Title VII's requirements apply to any range of AI tools used "to make or inform decisions about whether to hire, promote, terminate, or take similar actions" toward an applicant or employee. In practice, this means that the EEOC considers a selection procedure to include all criteria used to make any decision about an employee's standing in a company—basically anything related to any decision made from application to separation.

The guidance also gives examples of AI selection procedures that can create liability, many of which are widely used, including:

- Resume scanners that prioritize applications using certain keywords;
- Employee monitoring software that rates employees on the basis of their keystrokes or other factors;
- "Virtual assistants" or "chatbots" that ask job candidates about their qualifications and reject those who do not meet pre-defined requirements;
- Video interviewing software that evaluates candidates based on their facial expressions or speech patterns; and
- Testing software that provides "job fit" scores for applicants or employees regarding their personalities, aptitudes, cognitive skills, or per-

-Continued on page 11-

-Artificial Intelligence: Continued from page 10-

> ceived "cultural fit" based on their performance on a game or traditional employment test.

Second, the EEOC guidance reiterates a key point from its prior ADA guidance—that employers can be liable for the use of AI tools even if they are designed or administered by a third party (such as a software vendor), even if the vendor represents that use of its tool does not result in disparate impact.

Third, the guidance explains how employers can assess their AI tools for disparate or adverse impact. The EEOC recommends that employers determine whether any AI-assisted selection procedure causes a "selection rate" for members of a protected class that is "substantially" lower than individuals of another group. If this is the case, the tool would thereby violate Title VII's protections.

"Selection rate" refers to "the proportion of applicants or candidates who are hired, promoted, or otherwise selected," and it is calculated by dividing the number of persons hired, promoted, or otherwise selected from the group by the total number of candidates in that group. To determine if the selection rate for a particular group is "substantially lower," the EEOC recommends that employers utilize the "four-fifths" rule. This rule states that one selection rate is "substantially" different than another if the ratio is less than four-fifths (or 80%).

The EEOC provides the following example:

> [S]uppose that 80 White individuals and 40 Black individuals take a personality test that is scored using an algorithm as part of a job application, and 48 of the White applicants and 12 of the Black applicants advance to the next round of the selection process. Based on these results, the selection rate for Whites is 48/80 (equivalent to 60%), and the selection rate for Blacks is 12/40 (equivalent to 30%).

The ratio of the two rates is thus 30/60 (or 50%). Because 30/60 (or 50%) is lower than 4/5 (or 80%), the four-fifths rule would hold that the selection rate for Black applicants is substantially different than the selection rate for White applicants, which could be evidence of disparate impact discrimination against Black applicants and thus a violation of Title VII.

Lastly, the EEOC notes that although this guidance does not address other stages of the Title VII disparate impact analysis, including "whether a tool is a valid measure of job-related traits or characteristics," employers should consider evaluating their use of AI tools in this area as well. This could be the subject of additional guidance in the future.

Takeaway

Though the guidance is non-binding, it does indicate how the EEOC is thinking about Title VII enforcement going forward. With that in mind, there are a few things employers should consider to reduce potential liability.

Employers should take stock of the AI tools that they use. The EEOC is taking an expansive approach to enforcement in this area. Many employers may unwittingly rely on numerous tools that use AI technology. Though the use of the technology is itself not an issue, it can—as the guidance demonstrates—inadvertently create risk.

Employers should understand that they will not be able to shift liability for inadvertent violations of Title VII to the vendor or purveyor of any AI tools that they use. Even if a vendor states that their tools do not result in disparate impact discrimination, employers can still be subject to enforcement actions for any violation. Employers must understand how the tools they rely on work. Employers should ask the vendor what steps have been taken to evaluate whether the use of the tool causes a substantially lower selection rate for individuals of a protected class. Most of all, employers should determine whether criteria used by the tool is "job related and consistent with business necessity" or whether alternatives with less possibility of disparate impact exist, as these are the most reliable ways to reduce risk.

Time is of the essence. As the increasing federal attention (and the growing patchwork of state laws not covered here) show, regulators are moving almost as fast as the technology in this space. Waiting for more law or clearer instruction risks a lawsuit or an enforcement action. In this area a little bit of foresight can go a long way.

DATA PRIVACY

For many businesses, before AI was the buzzword of the day there was "data privacy." Data privacy essentially means the bundle of rights, establish by laws

-Continued on page 12-

-Artificial Intelligence: Continued from page 11-

and regulations, allowing consumers (including employees) to exert control over the personal information that businesses collect about them.

In California, data privacy is primarily regulated by the California Consumer Privacy Act of 2018 (CCPA) which provided California consumers with various new privacy rights, including: the right to know, the right to delete, the right to opt-out, and the right to non-discrimination for exercising privacy rights. California voters adopted Proposition 24 (also known as the California Privacy Rights Act) in 2020, which amended the CCPA and added a handful of new privacy protections. The CCPA (as amended by the CPRA) is enforced by the newly created California Privacy Protection Agency (the CPPA or the Agency), which is tasked with implementing and enforcing the CCPA. One the Agency's most powerful tools is its ability to adopt and enforce regulations related to the CCPA.

The CCPA is not the only mechanism available in California for regulation of data privacy, however. Over the past few years, as implementation of the CCPA has been cumbersome and confusing, some legislative complements to the CCPA have slowly begun taking shape.

Recent activity by both the state legislature and the CPPA reflect that California regulators are keenly aware of the intertwining risks created by AI and data privacy. Both bodies are attempting to quickly fill regulatory gaps created by AI's ever-expanding reach. Businesses that use AI tools, in ways both customer-facing and internal, should keep abreast of these developments and the risks that they pose.

A.B. 331

The legislative answer that is furthest along in addressing data privacy risks created by AI is a bill that was introduced by California state representative Rebecca Bauer-Kahan on Jan. 30, 2023. The bill, A.B. 331, which would add a chapter to Division 8 of the California Business and Professions Code, aims to create a detailed framework for regulating the data used to create and implement "automated decision tools." A.B. 331, *Automated Decision Tools*. Though the bill was held under submission earlier this year, it is likely to be reintroduced in largely the same form at the next legislative session.

Under the proposed legislation, an automated decision tool is defined as "a system or service that uses artificial intelligence and has been specifically developed or marketed to, or specifically modified to, make, or be a controlling factor in making, consequential decisions." Consequential decisions, in turn, are those that would affect certain enumerated individual rights and opportunities—namely employment, education, housing, healthcare, financial services, and criminal justice. The bill focuses on the creators of these tools (the "developers") and those who use the tools to make consequential decisions (the "deployers"). The bill would place several new requirements on developers and deployers, would add an enforcement mechanism, and would also create a private right of action against deployers for "algorithmic discrimination." Each of these will be discussed below.

Impact Assessments

A.B. 331 would require both developers and deployers to perform "impact assessments," which is defined as "a documented risk-based evaluation of an automated decision tool" that meets certain disclosure or analysis requirements. An impact assessment must include a disclosure of, for example: the purpose of the tool including its intended use, a description of the tool's outputs and how they are used to make consequential decisions, and summaries of the types of data collected and the outputs used to make consequential decisions. The impact assessments must also analyze potential adverse impacts on protected classifications, as well as describe several key aspects of the development and monitoring of the tool such as how the tool will be evaluated for validity or relevance.

Each impact assessment is to be completed "[o]n or before January 1, 2025, and annually thereafter," and the developer and deployer of the AI tool must provide the assessment to the Civil Rights Department within 60 days of completion. If a developer or deployer fails to do so, the Civil Rights Department may bring an administrative enforcement action and seek up to $10,000 "per violation." This means that "[e]ach day on which an automated decision tool is used for which an impact assessment has not been submitted…shall give rise to a distinct violation of this section." Presumably completed assessments will be collected by the Civil Rights Department, as the bill states that the Civil Rights Department is to share collected assessments with "other state entities as appropriate," potentially indicating that the California Attorney General or other public attorneys could play an added enforcement role.

-Continued on page 13-

-Artificial Intelligence: Continued from page 12-

Notice and Disclosure Obligations

A.B. 331 would require a deployer of an AI tool to provide, "at or before" the time the tool is used, a notice to individuals that the tool is being used to make a consequential decision. This notice must also explain why and how the tool is specifically being used, as well as a "plain language description" of the tool which includes a description of human or automated components that play a role in the decision-making process.

The bill also places on the deployer the requirement to add an "opt-out" mechanism, which would allow—if "technically feasible"—an individual to choose not to be subject to an automated decision tool and instead utilize an "alternative selection or accommodation."

Deployers are not the only ones with disclosure obligations. The proposed law also would require developers of AI tools to make available a statement regarding the intended uses of the automated decision tool. This disclosure specifically must include known limitations and risks of algorithmic discrimination created by the tool, a description of the data used to train the tool, and a description of how the tool was evaluated before sale or licensing.

Governance Requirements

The bill also places a governance requirement on developers and deployers. This governance program must contain "reasonable administrative and technical safeguards to map, measure, manage, and govern the reasonably foreseeable risks of algorithmic discrimination" associated with the use of any AI tool.

CPPA Rulemaking

The CPPA has engaged in a proposed rulemaking also aimed at "automated decsionmaking." *Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*. The Agency states that it invites comments on its proposed rulemaking to better "determin[e] the necessary scope of such regulations." *Id.* at 6.

In its proposed rulemaking, the Agency explains that the CCPA directs the Agency to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology." *Id.* at 1 (citing Civ. Code § 1798.185(a)(16)). Specifically, the statute requires that these regulations include "profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer." *Id.* The Agency also lists various specific topics that it is interested in—including the use of opt-outs and algorithmic discrimination. *Id.* at 6-8.

The text of the CCPA, in conjunction with the substance of the questions posed by the Agency in its invitation to comment, hint at several features that can be expected in the eventual regulations propounded by the Agency. One of the most obvious features of any CPPA regulation of AI is likely to involve an opt-out requirement. Not only is this statutorily required by the CCPA, but it is a common feature in other areas of data privacy. We can almost certainly expect new transparency requirements related to "meaningful information about the logic involved" in an AI decisionmaking process, "as well as a description of the likely outcome of the process with respect to the consumer." This may mean required disclosures of the specific data used as an input into the AI tool and an explanation of the outputs and how they are used to make specific decisions. It is also possible this could include required disclosures of data used to train or develop an AI tool.

While there are currently no privacy regulations related to the use of AI, the CPPA's proposed rulemaking indicates that the Agency has such regulations on the agenda.

Takeaway

As A.B. 331 and the CPPA's proposed rulemaking show, California privacy laws will inevitably cross paths with the use of AI technology, adding another risk that businesses should have on their radar as they grapple with this emerging technology.

CONCLUSION

Much ink already has been spilt about the benefits of AI for businesses, but much less is written about the risks. This article does not aim to cover every possible risk, but instead aims to show businesses the range of risks that this technology can create as a balance to its undeniable benefits. Overall, only the leaders of a

-Continued on page 15-

-Artificial Intelligence: Continued from page 13-

business know its true risk appetite. But, to better appreciate that calculation, it is appropriate that businesses know where to look and what to look for.

♦*Robert Matsuishi is a partner at Payne & Fears LLP. He has extensive experience litigating labor and employment matters, with a focus on wrongful termination claims, discrimination, harassment, accommodation, and retaliation claims, alleged violations of medical and family leave laws, whistleblower retaliation claims under the California Labor Code, the False Claims Act, and the Defense Contractor Whistleblower Protection Act/NDAA, and alleged violations of federal, state, and local wage-and-hour laws. The scope of these matters has varied from single-plaintiff cases to high-stakes class actions and representative Private Attorneys General Act ("PAGA") actions.*

♦*Connor Kridle is an associate in the firm's labor and employment and insurance coverage practice groups. Connor's labor and employment practice includes representing employers in all types of matters ranging from single-plaintiff lawsuits to large class or representative actions.*

-Privacy: Continued from page 3-

derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

The CCPA defines personal information broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Examples of this type of information include online identifiers, biometric information, professional or employment information, Internet Protocol addresses, email addresses, browsing history, search history, geolocation data, and information regarding a consumer's interaction with a website or online application or advertisement. The CCPA also covers "inferences drawn" from any personal information that is used "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

The CPRA defined a new category - "sensitive personal information" – which is a subset of personal information entitled to extra protections. Under the CPRA, sensitive personal information includes a social security, state ID, driver's license or passport number; information that would allow access to a consumer's financial account, like a credit card number in combination with a security code; precise geolocation data; genetic data; a consumer's racial or ethnic origin, religious or philosophical beliefs or union memberships; and contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication.

The CCPA and CPRA established and expanded privacy rights for consumers that allow them to assert greater control over personal information that businesses collect. These rights include:

- Consumers have the right to know what personal information a business has collected about them and to access their personal information.
- Consumers have the right to deletion of their personal information, subject to certain exceptions.
- Following the CPRA amendments, consumers have the right to correct inaccurate personal information.
- Consumers have the right to know what personal information is sold and to whom. The CCPA

-Continued on page 16-

-Privacy: Continued from page 15-

defines a "sale" of personal information broadly, to include providing access to personal information to a third party for monetary or non-monetary consideration.

- Following the CPRA amendments, consumers also have the right to know what personal information is "shared" and to whom. "Sharing" is defined as sharing for cross-context behavioral advertising purposes, whether in exchange for consideration or not.
- Consumers have the right to opt out of the sale or sharing of their personal information.
- Following the CPRA amendments, consumers have the right to limit a business's use and disclosure of their sensitive personal information.
- Consumers have the right to not face any retaliation for exercising their statutory privacy rights.

In addition to responding to consumer requests to exercise those rights, a covered business must:

- Minimize the collection of personal information to that which is reasonably necessary for business purposes.
- Publish a comprehensive privacy policy, and separate notices at collection, that explain the business's online and offline collection, use and disclosure (and, if applicable, sale or sharing) of personal information. The privacy policy must also explain the rights consumers have under the CCPA and how to exercise them.
- If the business offers a financial incentive in exchange for a consumer's personal information (such as offering a discount in exchange for a consumer's email address), publish a notice that explains how the business places a value on that personal information and how the incentive works.
- Make available to consumers two or more designated methods for submitting requests to know/access, delete or correct their personal information.
- If the business sells or shares personal information, or uses sensitive personal information to build a profile of a consumer, offer consumers an appropriate mechanism to opt out.
- Enter into appropriate contracts with service providers, contractors and third parties to whom the business discloses personal information.
- Implement reasonable security procedures and practices to protect the collected personal information from unauthorized or illegal access, destruction, use, modification or disclosure.

A New Era of Implementing Regulations and Enforcement

Prior to the CPRA, only the California Attorney General had authority to write CCPA implementing regulations, investigate potential violations and bring civil enforcement actions. But the CPRA delegated rule making authority to the Agency, which the Agency has already begun to exercise. And as of July 1, 2023, the Agency has authority to investigate potential violations and bring enforcement actions. The Agency is governed by a five-member board with one seat currently vacant. The board includes two law professors, a consumer privacy advocate and a technology equity advocate.

The Agency's statutory functions include:

- Adopting implementing regulations to clarify, and expand, CCPA requirements pursuant to the statute's mandates.
- Conducting investigations of potential violations.
- Bringing administrative enforcement actions.
- Providing guidance to consumers regarding their rights under the law and guidance to businesses regarding their duties and responsibilities under the law.
- Appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with the CCPA.
- Establish a mechanism pursuant to which entities doing business in California that do not meet the definition of a "business" set forth by the CCPA may voluntarily certify that they are in compliance with it, and make a list of those entities available to the public.

Because the Agency can now bring administrative enforcement actions against businesses, that means that the Agency can find businesses in violation of the CCPA, levy fines and issue injunctions under its own authority, without taking a business to court. Importantly, the Agency has subpoena powers, and can compel witnesses and require production of any records from a business to audit that business's compliance with the CCPA. The Agency cannot bring an administrative action more than five years after the date

-Continued on page 17-

-Privacy: Continued from page 16-

that a violation occurred.

The Agency may audit any business, service provider, contractor, or person to ensure compliance with any provision of the CCPA. Audits may be announced or unannounced. The Agency may select entities to audit based on possible violations of the CCPA, or if the subject of the audit is collecting or processing personal information in a way that presents a significant risk to consumer privacy or security, or if the subject of the audit has a history of noncompliance with any privacy protection law.

The California Attorney General retains jurisdiction prosecute violations of the CCPA, and can request that the Agency stay an administrative action or investigation to allow the Attorney General to pursue an investigation or civil action. However, the Attorney General cannot file a civil action for a violation after the Agency has issued a decision against an entity for that same violation. Agency enforcement does not affect the private right of action provided for by the CCPA, which remains limited to breaches of sensitive personal information that result from a business's failure to maintain reasonable security measures.

The Agency issued its first set of final regulations on March 29, 2023, and recently announced that it is launching a second round of rulemaking. However, a California Superior Court recently ruled that enforcement of Agency regulations cannot begin until a year after the rules were finalized. Therefore, the Agency's regulations will not be enforceable until March 2024 at the earliest. Additionally, the Agency has not issued final regulations in the areas of cybersecurity, audits, risk assessments, and automated decision-making technology, which are among the key areas requiring clarity.

Despite this, the Agency is already empowered to enforce the text of the CCPA itself, as amended by the CPRA, and the limited regulations previously promulgated by the Attorney General pursuant to the original CCPA. Therefore, now is the time for businesses to conduct a fresh review of privacy practices and ensure compliance with the CCPA. To that end, it is important that any covered business, if it has not yet done so, develop a mature data map to understand exactly what personal information it has about consumers, why it has that information, and where that information is stored.

Recommendations

Covered businesses should review the adequacy of their procedures for the following:

- Mapping data flows and integrating new instances of data collection, use and sharing into that map, with a special focus on "sensitive personal information" as defined in the CPRA.
- Translating the output of data mapping efforts into a compliant privacy policy, notices at collection, and other disclosures required under the CCPA.
- Assessing whether the business sells or shares personal information, with consideration for how those terms are defined in the CCPA and its implementing regulations.
- Processing and responding to consumer requests to opt out of the sale or sharing of personal information or limit the use of their sensitive personal information.
- Processing consumer requests to access, correct or delete their personal information.
- Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer.
- Ensuring that the business does not discriminate against consumers who exercise their rights under the CCPA.

♦***Travis Brennan*** *is a shareholder at Stradling and leads the firm's Privacy & Data Security practice. He helps clients turn data privacy compliance into a business asset rather than a regulatory burden. Travis also represents companies in commercial litigation, consumer class actions and government investigations concerning data privacy and security matters.*

♦***Lila Reiner*** *is an associate in Stradling's Litigation practice group. Lila attended the UCLA School of Law where she served as an Associate Editor of the UCLA Law Review. Drawing on her diverse background and prior work for the California Legislature, she brings a creative and multi-disciplinary approach to solving problems for clients.*

ASSOCIATION OF BUSINESS TRIAL LAWYERS
abtl
ORANGE COUNTY

8502 E. CHAPMAN AVENUE
ORANGE, CA 92869