Silicon Flatirons
KNOW WHAT'S NEXT.

Transcript

Crash Course: The State of Privacy Law in California

November 17, 2021

Contents

David Zetoony's Presentation

https://www.youtube.com/watch?v=VjyCI5Q_wmE

[00:00:00.00] MARGOT KAMINSKI: Hi, I see some familiar faces in the audience, some new. I'm Professor Kaminski. I teach information privacy law and cybersecurity here at the law school. It is my very deep pleasure to introduce David Zetoony. David Zetoony is a partner at Greenberg Traurig and co-chair of that firm's US Data, Privacy, and Cybersecurity practice.

[00:00:24.75] David has helped hundreds of companies, establish, and maintain ongoing privacy and security programs. He has defended corporate privacy and security practices at the Federal Trade Commission. And the National Law Journal named him a cybersecurity and data privacy trailblazer. JD Supra recognized him four times as one of the most widely read names when it comes to data privacy.

[00:00:47.55] And Lexology identified him seven times as a top legal influencer in the area of tech, media, and telecom in the US, the European Union and in the context of cross-border transfers of information. He is the author of many publications including the ABA's primary publication on the EU's GDPR and the ABA's desk reference companion to the California Privacy Rights Act.

[00:01:12.27] So today, David will present his new book The Desk Reference Companion to the California Consumer Privacy Act and the California Privacy Rights Act. This reference guide collects over 500 of the most commonly asked questions concerning the CCPA and the CPRA and provides straightforward and easy to understand answers in one place. Please join me in welcoming David Zetoony.

[00:01:34.60] [APPLAUSE]

[00:01:38.60] DAVID ZETOONY: Thank You so much, Professor Kaminski. And it's a pleasure to be here. I love being at the University of Colorado, and I'm glad we can be here in person for some of us. So let me start off. This is kind of a hybrid. It's a kind of a book reading-- plug for the ABA. There's my plug.

[00:01:54.49] Crash course on the California Consumer Privacy Act and the California Privacy Rights Act, and just kind of weaving the two together. So beyond the crash course, I kind of want to get into some master level stuff and any questions people have actually implementing the act. So trying to weave all those together can be a little interesting, and so bear with me.

[00:02:10.16] I'll try to do a slightly different format. High level though, let me start with the book and just a little bit of an explanation. So I started writing this in 2018 when the CCPA was passed. And I had written a previous book on the European GDPR. That book took me a little bit less than a year to write. And I thought this would take me six, seven, eight months.

[00:02:31.79] This was a shorter statute, less legislative history. It ended up taking me three years. And there's a lot of reasons for that. It also ended up being about three times longer, if anybody's ever seen the GDPR book, than the GDPR book. And there's really three reasons for that. First is it never stopped changing. And that's one of the themes we'll talk about.

[00:02:51.23] When the CCPA was passed in 2018, it then was amended, amended again, amended again, amended again, and ultimately functionally replaced, and amended again by referendum. There were final regulations that were never really final. They were proposed regulations that kept getting changed. Deadlines were missed. And I'll talk a lot about that timeline.

[00:03:09.44] But that ended up taking something that was supposed to have a two-year time period for companies and organizations to get to compliance. And there really wasn't a two-year time period from when you actually had a static set of laws, rules, regulations that businesses can look at and say, that's locked in stone, to when you were supposed to have compliance.

[00:03:27.02] What the function meant for me from a drafting perspective was could come up with the original draft, and then even the smallest amendment meant you had to reread the entire thing and edit every single response to see, does it impact this? Or does it not impact this? After doing that two or three times or four times after every amendment, it was a process of strategically looking at, when is this going to be settled enough to put into paper something that isn't going to be outdated within a month?

[00:03:53.10] So it's kind of a first explanation on the process of writing a book on this which I think will inform a lot of people who either haven't practiced data privacy law or about to practice data privacy law in terms of giving advice to your clients.

[00:04:06.68] Second is, if anybody's ever written anything, if there's a time delay that is just more opportunity to keep writing, so any time you stop writing and you have to reassess, all of a sudden new questions, new issues would pop up. And I would put those into the book. So this started off. I was going to do about 150 of the most frequently asked questions that became 200, 250, 300.

[00:04:27.32] And ultimately, we ended up with, I think, 520 frequently asked questions, so bigger in size than originally thought. And then finally, it is an extremely confusing statute. And I can't emphasize that enough. For anybody who's practiced in the world of data privacy, CCPA is not done in a vacuum.

[00:04:46.41] There's a host of data privacy and security statutes. My personal opinion, I think, others would probably agree with this. I think most people might. It is probably the worst drafted every privacy statute that's been put out there. And that's putting aside whether you agree with what it's trying to do and the principles and the policy. I think that's a whole separate discussion.

[00:05:04.07] From a pure drafting exercise, it was a bit of a train wreck. So various versions, including the referendum version, had hundreds and hundreds of typos. And we actually went through the first version that was put on the referendum. And I think we stopped counting at 300 when we found spelling errors, comma errors.

[00:05:19.88] Many of those were fixed. Again, every time you fix something, recycle like, what does that mean? You move the comma from here to there. But from a drafting exercise, it was an interesting concept. So that's going to lead into kind of number one, the odd development of the California data privacy laws.

[00:05:38.00] I'll talk a little bit about what to do to comply with it. And then, I'm going to pull some selections. Again, this was structured as the most frequently asked questions. So I'm going to pull some of the most frequently asked questions and go through those and do an explanation. And then, I'm happy to respond to questions that you guys have in terms of what you think are your questions and issues that have come up or any inquiries on this or how it relates to other privacy laws.

[00:06:00.20] But I've given you a little bit of a background in terms of the odd development. And I'm going to read-- this is the only part that's going to feel like a book reading. I'll read a little bit of the foreword. I was hoping for this audio, but that's not going to work today. So everybody who is over the age of 35, go to anybody under the age of 35 and explain what this picture is, which you'll probably all grasp in a second.

[00:06:21.33] But let me start with a quick reading from the intro of the book. If you grew up in the 1970s, or the 1980s, you probably remember the Schoolhouse Rock! song, "I'm Just a Bill," which is what's on screen. It played every Saturday morning and explained at breakneck tempo the legislative process.

[00:06:39.14] And it would talk about-- and this is the excerpt. I will not sing it. That's why I put this in here. But you know what? I'm going to play it, so you can see the pretty pictures behind me. How about that? And I'll turn the audio down so there's no interference. There you go. So start always with the, I'm just a bill.

[00:06:54.60] Yes, I'm only a bill. I'm sitting here on Capitol hill. Well, it's a long, long journey to the capital city. It's a long, long wait while I'm sitting in committee. And the song goes through literally in three minutes. It encapsulates everything you can learn from a legislative history class at law school in about a semester, but it did it in three minutes.

[00:07:10.91] And it was right. It was really detailed, go from committee to joint committees to the reconciliation committees. That's the process that we learned. I learned when I was a kid. That's the process you learn in law school. That is not the process of California Privacy law. And so here's a little bit from the foreword.

[00:07:30.80] "In practice, the normal legislative process, draft legislation, committee discussions, subcommittee reports, hearings, conferences in the same process starting over and over again in the companion legislative branch sometimes doesn't happen. Indeed, in the world of data privacy, the normal process feels more like the exception than the rule.

[00:07:48.51] The data privacy world has two landmark changes in the past decade, European GDPR and the California CCPA and his companion the CPRA. Neither the European approach to privacy regulation nor the California approach to privacy legislation fits the traditional model. Indeed, they should have been taught in every law school as case studies to understand how divergent the legislative process can be."

[00:08:10.20] I'm not going to bore you guys with going through the GDPR legislative process. I'll skip through that other than to say, years and years and years-- like if you were to do a Schoolhouse Rock! song on that, it would not have been three minutes. It would have been like three hours because it goes, tosses between committees and subcommittees and working groups and advisory committees.

[00:08:27.96] It is on one end of how you exhaustively think about a legislative and regulatory process and try to come up with something with all stakeholders who contribute. But I will read a little bit in terms of the description of California. "The process that created the CCPA and the CPRA were far from exhaustive or thorough.

[00:08:47.01] For DC Comics fans, you could consider the legislative process that created California's privacy laws the Bizarro World of the orderly and thorough European GDPR creation process. In 2017, a California real estate developer turned privacy advocate filed a ballot initiative for California right to Privacy Act.

[00:09:04.53] The ballot initiative which was refiled and amended several times was ostensibly based upon portions of the GDPR. But there's no indication that it was drafted by any attorney let alone one familiar with data privacy. Under fear of passage of what was considered by many a poorly drafted and poorly conceptualized initiative, the deal was reached on June 21, 2018, between the proponents of the ballot initiative and certain members of the California legislature under which the ballot initiative would be withdrawn if the legislature adopted and the governor of California signed a statutory replacement by June 28, 2018.

[00:09:38.85] For those keeping track mentally in their head, that's seven days after this was put forward. So California signed a statutory replacement on that date. Assembly Bill 375, it was an inactive proposal that had been gathering dust from the previous year, was never fully drafted, vetted, or reviewed, was pulled from the inactive file.

[00:09:59.49] On June 21, 2018, it was referred to the Judiciary Committee for hasty approval. June 25, four days later, it was referred to the Appropriations Committee. On June 28, it was enacted and signed by the governor. So in essence, it took seven days to transform a previously abandoned bill to legislation.

[00:10:16.20] During that time, it's not clear if any legal privacy experts, as opposed to privacy advocates, reviewed, revised, or opined on the text. While subsequent amendments in 2018 and 2019 tweak the language, they mainly corrected grammatical errors and typos doing little to modify the substance of the original text. The only real overhaul came in 2020 when the same California real estate developer turned privacy advocate filed a second ballot initiative.

[00:10:40.86] That's the history. That does not match anything that is taught or was taught to me when I went to law school in terms of how legislation comes into being typically, how it should come into being. But you have to understand that backdrop when trying to apply it. So if you look at this as courts do and you assume the legislature, in its grant wisdom, consider each and every word, and we're going to give effect to every single comma, and that is how courts will probably interpret this.

[00:11:07.39] You have to realize that it is, in essence, a fiction, an incredible legal fiction. Seven days to take what is a 20 to 30 page statute from inactive dead to passed and is going to govern the world. That is breakneck speed, and you're going to end up with errors and inconsistencies and ultimately a 500-page book on how to interpret it.

[00:11:30.88] So that's a little bit of background in terms of the book writing process driven by that odd history. So I'm sure you guys would have liked to hear a cartoon much more than hear me read that, but there you go. So I'm putting on screen, just to kind of encapsulate this, the odd history after the passage.

[00:11:49.35] I couldn't do a timeline for the seven days that would just look like a little tiny bleep of how long it took to get all that legislative history that normally happens and get it passed into law. But you can certainly do a timeline after it gets enacted. So what you have on this page is October 12, 2017.

[00:12:07.83] The privacy advocate put forward the first initiative, the CRPA, the worst acronym ever. You fast forward to June 28th, where it actually gets passed as a different piece of legislation. After that, you've got SB 1121, AB 25, AB 874, AB 1146, AB 1355, AB 1564.

[00:12:30.36] Each of these are assembly bills or Senate bills that amended the act. These are happening real time as companies are trying to come into compliance. You then fast forward to November. And this is interesting, so November 13, 2019, you get the filing of the new referendum item, the CPRA, which is going to replace amend and supersede the entirety of what had been passed a year before.

[00:12:55.72] But that date is literally a month and a half before the original one goes into effect. So now, you have organizations which have worked at breakneck speed with things changing real time to come into compliance. And a month before this is supposed to come into compliance, you have an entirely new proposal that lands as a referendum initiative.

[00:13:13.87] And so organizations again questioning, well, what do I do with this? Do I keep going forward? Do I not go forward? Do we Pause Do we not pause? What's going to be the law? That ultimately did get m the CPRA. So right after you have the CCPA which goes into force, you now have a new one that's going to supersede it within two years.

[00:13:33.53] And you can see-- the timeline doesn't simplify from there. So now, we're coming up to real time here, the "You are here" button. That's where we are. There has never been a two-month cycle in the past two years where there has not been a change to what is required of the CCPA or the CPRA or what's going to be required or how it's been interpreted.

[00:13:54.46] And that really drove-- again, for publishing a book, you have to get to a point where it's not going to change so much that a book is going to be out of date the month after it issues. I think we are now, however, in that law which is kind of why I came forward with this. The CPRA has passed.

[00:14:11.78] There does not look like there's any amendments really on the horizon. We do have final regulations under the CCPA. And until 2023, so at least a year, we have a law that is in effect. And after 2023, there will be additional changes coming from the California Privacy Protection Agency.

[00:14:28.43] And then, going up to 2023, we're going to have changes that are anticipated. Things like employee data is going to be covered by the Privacy Act. This is a business contact data. It will be covered by the Privacy Act. We're going to get more proposed regulations from the new agency.

[00:14:44.63] So we're going to be-- I think the takeaway here is, it's a long process. It's been tortured. We're in a lull period where, I think, companies can step back. Most companies should have operationalized some element of this. They should be road-mapping for the future. There probably are going to be some changes, but the hope is that instead of having radical reversals and radical changes, we're probably in some kind of area where we can focus on minute changes and trying to perfect compliance programs.

[00:15:12.58] So that transitions into, what does it mean to actually comply with the CCPA, CPRA? You've heard about the tortured history. You've heard about the difficulties to comply. But at the end of the day where it all panned out, what does it require? So I put up a slide here. I don't know how many people in this room are familiar with European data privacy law, and I'm not going to go through all of it.

[00:15:31.06] But some of you are. And European data privacy law is the backdrop for all US data privacy law at this point. It is the language [INAUDIBLE]. It is the common denominator internationally. When you start talking about data privacy you compare it to the European GDPR. So the first column here has the basic building blocks of a compliance program under the GDPR.

[00:15:49.71] The second column shows where there's overlap with California and where there's not overlap. So the blank spaces, there's no analogs. You start talking about permissible purpose or data minimization, collect more than you need or put retention periods in terms of what you do collect. There's no real analog in the CCPA for that.

[00:16:06.24] But there is analogs to things like notices to data subjects, privacy policies. There's an analog-- there's no analog to financial incentive disclosure. So one thing you see from this chart is there's some aspects of California which didn't replicate Europe. They went beyond or diverged and went into a different direction. One of those is the financial incentive disclosure requirements.

[00:16:24.66] There are analogs to things like right to access or right to be forgotten or the right to opt out of sale. But there's no analogs to things that were under European law like the right to rectification, right to fix errors if there's an error in some of these data. There's other areas that are new. The right to provide services on equal terms doesn't really exist under the GDPR.

[00:16:44.85] And then, there's a lot of areas where there is some commonality, using appropriate security to protect information, notifying in case of data breaches, contractual requirements, if you send data from an organization to service providers or vendors or processors, and then finally, consent for our tech cookies.

[00:17:01.32] There's overlap here, but talk about [? MS. ?] And I'll talk about that a little bit later where-- you may end up in the same place or something very similar. Both statutes touch on it. But California does so in such a bleak way, kind of obtuse. It's not really directly addressing what they're trying to get at. That it's difficult for a lot of companies to try to understand what's happening.

[00:17:25.17] And then of course, you got the CPRA which is the 2023 referendum item. This is going to supplement replace to proceed. And so in the second column, you have everything that is in place now for a company subject to California law. And then, CPRA is everything that we're going to see in a little bit more than a year.

[00:17:42.57] And the ones involved show the delta. So what you're seeing is one way to conceptualize it trying to patch these areas where California law did not fully come up to the European standard and bring in things like data minimization, and bring in things like the right to rectification to correct errors, bring in things like the clear statement about what to do with adtech cookies, bring in things like automated decision-making and profiling, bring in things like privacy issues with sensitive data collection, collecting health information or biometric information.

[00:18:15.48] So on some level, 20,000 foot-- you see convergence, California coming back towards Europe. But again, the devil's in the details. It is still the worst-drafted privacy and security statute bar none. And so when you start implementing them, you can lead to a lot of ambiguity when it comes to the technical implementations.

[00:18:33.81] So let me pause there and kind of just recap. I know I've talked a lot about the legislative history, but I want you guys to understand the real takeaways besides knowing this is a tortured legislative process. There is a law right now in California, the CCPA, that is in force. It applies to almost every multinational company, large company in the United States, anybody who collects a large amount of data about Californians-- and not even that large amount of data.

[00:18:57.48] In 2023, we're going to get the new version of that, version 2, and that's the CPRA. And that is going to strengthen, replace, supersede, and then bring more stuff into California that more aligns it with Europe. So that's the very high level, total crash course. I've taught before compliance programs for CCPA, and usually I break each one of those components into an hour.

[00:19:18.88] So data minimization might be an hour. Privacy notices might be an hour. This is like a three-minute-- here you go, table of contents, of what it means to be compliant. So for this course and this discussion, I wanted to focus more on the frequently asked questions. And that's kind of how I approached it in the book is instead of talking about this in the academic or the legislative, although I talk about that in the foreword because I think it's important to understand, I really wanted this to be about practical questions.

[00:19:46.68] Can I do this? Can I not do that? Do I have to do this? Can I get sued for that? And so that ended up being that 520 questions that went into the book. Not all those questions are created equal. So one thing I did is I got permission from the American Bar Association to pre-publish about a third of the questions independently as articles.

[00:20:05.52] And from those free published articles, I could get statistics in terms of which questions resonated more with which people. So my standard to get into the book was I had to have at least three companies asked me the same question in one week. That's how I figured it was a frequently asked question.

[00:20:21.27] If I had three clients who called me up on the same week and said, I want to know the answer to x or y. I'm like, this needs to go in the book. Other companies have it. When we published the articles, about 100 of them, then I could see actually readership. This article was read 100 times. This one was read 2,000 times.

[00:20:37.89] And what they put here is the actual readership pattern. You can see there are some articles that have readership in the thousands. And there are some articles that were around 150 or 200. And these are all subsections. So this is basically-- when I publish at a firm or almost any firm publishes, they get picked up by aggregators who republish law firm articles.

[00:20:59.70] And some of those provide statistics, so you can see some statistics about one of the republishing sources. So what I'm going to do for some of the rest of the time is go through each one of [AUDIO OUT] these compliance blocks and pull out one question, the question that either was the most asked, frequently asked, or kind of fundamental, and try to walk through that.

[00:21:20.25] And then again, I'm happy to answer any other questions. I hope you guys have some to dive into these because again, I'm pulling out one question from probably a chapter of the book which might have 30 or 40 or 50 questions. It's not going to be able to explain all the contours. But starting with data minimization, so question 91 in the book, will the CPRA require publishing the data retention period that applies to personal information?

[00:21:44.14] The answer to that is yes. And the reason I pulled this out-- this is not a complex thing to find in the statute, but it is a very surprising aspect of this law to most organizations and companies because it really has no US analog. Data minimization-- think retention schedules and retention periods, how long you keep data as a company. It has always been a best practice.

[00:22:07.02] We all know we shouldn't keep information from longer than we need it. We also know that we need to keep information for a certain minimum amount of time. And those have always in the US been a little bit of a backdrop in terms of setting up a retention schedule. How long do we keep emails? Is it 30 days or 20 years?

[00:22:20.82] And you end up with something usually in the middle to try to balance. Well, we need to keep it for a certain amount of time for regulatory compliance because our clients may have questions or consumer may come back with the inquiry. But we don't want to keep it forever because after 100 years who needs this stuff.

[00:22:34.54] Now, for the first time though, we have a law that is mandating that you have a reasonable appropriate time for the maximum, meaning try to keep it for a small amount of time and justify it. And you now have a law that says, oh, by the way, you have to tell people what that amount of time is.

[00:22:48.97] That is night and day from a compliance strategy of any US company. It is very hard to find a US organization that publishes its retention schedules and tells the world, I keep emails for this long, and I keep your name for this long, and marketing information for that one. There's an analog in Europe.

[00:23:06.70] So under the GDPR, you arguably have to do this already. I would venture to say that compliance is relatively low. And Professor Kaminski might have her own thoughts on that. You can go to a lot of European websites, and it is hard to find retention schedules published. There have been some enforcement actions in Europe on this.

[00:23:23.41] But in the US-- while in Europe it might be relatively low compliance, in the US, this is a foreign concept. So it is a requirement. Under the CPRA, when you collect information, and I put the quote here, "You are supposed to disclose as part of your notice at collection the length of time the business intends to retain each category of personal information collected."

[00:23:45.37] I'll throw it here just a few other things for those who are practitioners to consider. The reason that this is not standard practice in the United States is because it's an incredibly hard exercise. Companies collect information for hundreds of different purposes. Think name, you may collect it about your employees. You may collect it about a consumer, a consumer who issues a complaint, a consumer who doesn't return, a consumer who does a transaction.

[00:24:08.26] All of those may have need a different retention period. To try to disclose the hundreds and hundreds of permutations is an incredibly hard exercise, to even identify the hundreds of permutations. And in effect, companies end up having one catchall that says we're going to keep it for x amount of time. It's kind of a medley of all these different things because we may have some use for it.

[00:24:30.22] But even if you were to disclose that period, companies are also afraid of another thing, which is UDOP cases. So nobody-- there are some litigation under the CCPA, but by and large, not a ton. But there is an immense quantity of litigation in California. One of the plaintiffs bars, most friendly statutes, is the CLRA, the FAL, UCL, which is a collection of statutes about unfair and deceptive practices.

[00:24:53.32] It is basic consumer protection law. You cannot lie to people. You cannot deceive them. You cannot mislead them. The fear here is that a company in good faith says, look, all right, we're to keep your information for a year. What happens when it's not kept for a year? What's really going to happen is the plaintiff, of course, is going to grab than that.

[00:25:10.21] And they're going to say, you told me it was collected for a year. And we found out it was a year and a week. And because of that, we're going to see under a deception theory. Because record retention and data collection and this issue is so hard for companies to do internally, when you have so much data you're collecting so many different purposes, trying to come up with an accurate statement that doesn't deceive people, that doesn't lie to people is an incredibly challenging exercise.

[00:25:34.36] And again, the stakes to this are not about CCPA violation to most companies. The stakes to this are about the plaintiffs bar who has a history of seizing on technical violations, not about things material necessarily sometimes. I'm not going to criticize all plaintiffs attorneys. I'm sure there are some wonderful ones in the audience.

[00:25:52.30] There's a history of some lower-feeding plaintiffs attorneys who love to find the "gotcha" moment, things that the record retention period didn't get applied, that somebody accidentally turns something off. And so that's really the concern with the data minimization.

[00:26:06.55] So let me go on to the next one, notices to data subjects. One of the most frequently asked questions, and it's 122 in the book, can a company be sued by consumers for failing to post a privacy notice? A lot of people are surprised by this. The answer is no, under the CCPA. So the CCPA mandates that you have a privacy notice, but the private right of action that it gives is very narrow, and it only applies to data security issues protecting the information from breach.

[00:26:29.14] It does not apply to the data on privacy issues, meaning privacy notice is almost everything on this list that doesn't deal with security. Can you be sued by somebody else? Yes. You can be sued by the California Attorney General's office, or soon to be here in California Privacy Protection Agency. But there's a huge difference, again, between enforcement done by a regulator and enforcement done by a consumer hashtag plaintiffs attorney.

[00:26:53.02] So by and large, if you don't post a privacy notice, it could be a violation to the CCPA. Your potential exposure and liability would be the risk of being litigated against or enforced against by the California Attorney General.

[00:27:07.91] Financial incentives disclosures, this is another brand new thing, and it didn't exist in Europe. It didn't exist in the United States. So the CCPA obliquely talks about this concept of giving financial incentives. The California Attorney General's office really seized upon it. And in its regulations to the CCPA really expanded, and arguably-- one might argue, well beyond what the statute was discussing, what has to be done for financial incentive.

[00:27:31.13] So it defines as a financial incentive any program, benefit, or offering that is done in relation to, I believe, personal information, the collection sale disclosure personal information. This has caused a lot of concern among organizations because that definition is so broad it doesn't even include the word "incentive."

[00:27:50.28] So the original idea was financial incentive probably means you're being incentivized to do something with information like you're going to pay somebody. Here's $50 if you take my survey and give me information. How it was defined in the regs had nothing to do with incentive. It's just anything related to the collection of information which could include, at the ridiculous level, you walk into a store in California and give your credit card.

[00:28:09.29] Well, they've collected information, and they've given you a benefit. They've sold you something, right? They give you an offer. We will sell you something. That, at a particular [INAUDIBLE], might be defined as a financial incentive program. But there's a lot of areas in between. So what most organizations in the [? AG ?] has said is, look, we know the loyalty program is a financial incentive program, or at least they've argued it. I think there's an argument that it's actually not.

[00:28:30.98] And then, there's shades of gray from there. What about when you collect someone's email address to go on to a listserv? What about when you collect somebody's email address to get exclusive discounts? What about when you send out newsletters to people's mailing address? Are those financial incentive programs?

[00:28:45.02] Maybe they are, maybe they're not. There's really no direction on this. But if it is classified as a financial incentive program, a couple of things kick in. So first, you have to notify the consumer, the data subject, about the financial incentive program. You have to get their opt in. They have to agree to do it, and you have to permit them to revoke the consent, to opt back out of the financial incentive program.

[00:29:04.67] Those may sound fairly easy. They can be a little complex. Think about a mailing that might come from a big retailer to every residency in the country that gives you 20% off going to the store. Well, is that a financial incentive program? They have collected personal information as defined by the CCPA if they bought a bunch of mailing lists, lists about people's households and where people live.

[00:29:28.46] Did they get consent and opt in to the financial incentive? No, they didn't because they bought a bunch of publicly available information. And so there's a lot of nuance here. Can you take that information out of scope because it's publicly accessible therefore it might not be personal data, therefore it might not be a financial incentive program?

[00:29:44.82] But by and large, the real stickler for financial incentive programs comes with another requirement in the regulations. And that is to include an explanation of how the value of the data to the business is reasonably related to the value of the data to the consumer implying that there must be a reasonable relationship, by the way.

[00:30:03.65] And under the regulations, it implies or states, one could argue, that as part of that disclosure, you have to do a good faith estimate of the value and explain to the consumer how you came up with good faith estimate. I think maybe what was intended by this is that any time there was a financial incentive program, I think loyalty program, the business would have to say, do you want to join? Fine.

[00:30:25.13] Are you going to opt in? Fine. Oh, by the way, if you opt into our loyalty program or airline miles, we value your data at $150 or $200 or $800 or $0.50. Oh, and by the way, the value that we think you're going to get out of it is $50 or $80 or $75. And the implication here is there has to be a reasonable relationship. Of course, there's no definition of what that means.

[00:30:45.91] Is it reasonable to be 2 times, 3 times, 100 times, 50 times, or does it have to be a direct? And in addition to that, one of the other concerns with this is trade secret. So companies, by and large, don't like to publish the value of the data that they collect and how valuable their programs are to their competitors.

[00:31:05.15] That's just not something that airline 1 wants to be disclosing to airline 2 so that airline 2 can decide whether its program is better or worse or whether it should revise to airline 1. So you run into a situation here in terms of how do you comply with this where companies really have to make strategic decisions about, are we going to disclose the economic value?

[00:31:23.15] Are we going to claim that it's a trade secret and try not to disclose it? If we are going to disclose it, how are we going to compute it? And if we do compute it, how are we going to try to

establish this concept of reasonable relationship between what somebody gets out of a program and what we get out?

[00:31:38.78] I'm happy, by the way, to answer any questions as we go through this. If anybody has a question a particular compliance topic, don't feel like you have to hold off to the end.

[00:31:46.77] Right to access, so one of the most frequently asked questions on that, question 129 in the book, did the CCPA create the right to access? So for those who aren't familiar with it, the right to access is the ability of the Californian to go to an organization or business and say, give me a copy of my personal information. I want to see what you have on me.

[00:32:05.91] Fairly new in the US, at least people weren't used to it. It's actually not new legally in the United States. So I think most people weren't aware of the right to access. Most organizations weren't aware of it because it didn't happen in all contexts. And this is the first time it really got applied universally to most businesses.

[00:32:22.38] But it already existed under HIPAA. It already existed under FERPA. It already existed for GDPR for Europe. It already existed in about 25 other state privacy statutes that focused on employee data. They gave employees the right to ask for certain categories of information back. So definitely, this is a new expansion without a doubt far broader than this ever existed in the United States, but conceptually not brand new.

[00:32:45.91] And again, one of the most frequently asked questions is, I think, a lot of businesses weren't even aware of where this was already hitting them and certain aspects, definitely, the employee information side. They weren't aware that rights of access already existed for a lot of data subjects. So they saw this, and it's kind of eye-opening of how broad that right is.

[00:33:04.69] So right to fix errors, I flagged on one of the previous screens that's not in the CCPA, but it will be in the CPRA. And so one of the questions that we get very often is, does it exist in the CCPA? Do we have to do it now? And one of the reasons for that is, again, that right of rectification or correction is found in other data privacy laws particularly in the GDPR.

[00:33:20.92] People assumed that it came into California law as one of the three main rights, access, rectification, deletion, but it was omitted. So as of today under California law, you don't have to fix an error if you find an error. That will have to happen in 2023. But a reminder, there are some other, not very many, but there are some other US privacy laws that do already contain rights of rectification.

[00:33:43.24] The main one is the Fair Credit Reporting Act. Again, that's very narrow, meaning it applies to Consumer Reports. So if somebody runs, say, a consumer report on you if you're applying for a bank account, and they come back and they deny you, and they say, well, we can't give that to you because you've been bankrupt five times. If that's inaccurate, you have a right to challenge that under the FCRA.

[00:34:01.36] So that concept of how to handle challenge has already existed in the United States, but historically existed for a very narrow subset of organizations, consumer reporting agencies, people who furnish data to consumer reporting agencies, and people who use the data that came out of the consumer reporting agencies.

[00:34:18.58] This is going to be far broader. So this is going to be anybody in California. And I should put a pin in this one. I keep saying California which is true. CCPA applies only to Californians. But we're starting to see these issues pop up in other state laws, including Colorado, which has its own Colorado Privacy Act modeled, hybrid between California and Europe.

[00:34:38.38] And so as practitioners, you take these concepts of California but keep in the back of your mind is probably not limited there, definitely not for Colorado, Virginia, but really going forward we're

going to find other states who are adopting as well. Now for CCPA, if you think a company has anything wrong about you, your birth date, your eye color, what your preferences are, they flagged you is a big consumer of energy drinks. Nope, I'm a big consumer of vitamin shakes.

[00:35:07.48] I mean, to that level you could do a rectification request and say, nope, I think you flagged me incorrectly. I'll tell you practically, having done ratification requests for the last 15 years in the European data privacy law, this seems like a big deal to organizations because it means they have to have a system that allows for adjudication and input from the consumer about all the data they collect about the consumer and to be able to fix it in their systems.

[00:35:30.76] In reality, very few rectification requests get made. Anecdotally, when you start looking at Europe historically, it's about 80% deletion, 19% access, 1% rectification. Rectification requests are unusual. Consumers typically don't take the time. They'd rather either just get their information deleted or access it. Yeah?

[00:35:56.50] AUDIENCE: Like practically speaking, this is also going to be-- it's going to be a request to access or access request as well, right, because they have to see what you have on them in order to see if it's incorrect. Or do they just-- they usually get spawned by like something being sent out that the consumer notices of being wrong?

[00:36:19.69] DAVID ZETOONY: It can be both. I mean, again, historically, all we have to really draw upon is your own. And one could argue whether European consumers are the same as Americans consumers in their behavior. But they've been so infrequent in Europe. But when they do happen, which is rare, it's either because the consumer just knows.

[00:36:36.64] So think, you get a mailing to your house, it has your name on it, but it has the wrong last name, has the wrong address. You open it up and it's your alumni newsletter that says you graduated five years off. You didn't do an access request to find that out. Theoretically, you have a rectification. We see that maybe 50% of the time in Europe.

[00:36:53.50] The other 50% of the time is it is a spawn from the access. And that explains why you see the cascade. You maybe have 80% deletion, 70% deflation. You get almost everything else access, and a lot of times the rectifications are a follow on from the access request. Again, in my experience, and not many data points, this is a small data set, it's about a 50/50.

[00:37:14.05] Rectification request, the other sources, employee rectification requests in Europe, they don't need to do an access request to say, I should have gotten the better evaluation, so I'm going to do a rectification request. Professor Kaminski?

[00:37:26.84] MARGOT KAMINSKI: This is a question from the webinar which I think is an important one. Is there any sort of standard of evidence for what counts as an error?

[00:37:36.13] DAVID ZETOONY: Yeah, so the answer is, no, not really. I don't think. If anybody else is aware of one-- the standard in Europe is you either correct it or you document and flag the file, meaning, look, if you're not going to make the correction because you think that what you have is right and what they've challenged is wrong, you flagged the file and say the consumer has challenged this so that if you're going to use it in the future internally, if you're going to share it with your third party, or you're going to give it back to the consumer, if there's a notation.

[00:38:00.43] So the standard is not like you must follow what the consumer says and say, you must make a determination. And if you disagree with the consumer, you must at least note that this has been objected to. I think that's the same standard for the CPRA. But I'll be honest, because we haven't had to apply this yet, I haven't focused as much on the terminology to see whether or not there's an evidentiary verbiage in there that might have to be applied.

[00:38:23.47] This is also an area where I think we might get regulations from the CPPA, who has the ability to interpret the CPRA, which hasn't come to effect. And they might clarify as to what standards you have to achieve for the rectification. I'll also say, that might end up being academic. So again, I'll apply what's happened in Europe.

[00:38:41.60] Rectification requests are not that common. And 9 times out of 10, the business is more than happy to fix it. So if the consumer says, hey, you got my address wrong. This is great, like, give us your right address, give us your right email address, give us your telephone number. They have no interest in having inaccurate data.

[00:38:56.45] There are situations-- I said the employee who says, my performance evaluation is wrong. Fix that. Yeah, that's a little trickier. The answer to that is no. We're not going to fix that. Your performance evaluation is right just because you disagree with it. So I think the conflicts between business and consumer is very rare on the rectification side, or at least, it has been in my experience.

[00:39:17.82] So moving on, deletion requests, if a business receives a deletion request, is it prevented from collecting personal information about the consumer in the future? This is one I didn't expect a lot of organizations, but I was asked multiple times. The answer is no. I think consumers or [INAUDIBLE] may be a little confused about this.

[00:39:33.95] I told you to forget me. Why do you still have my information? Well, the answer is, because I collected it again. I deleted your information. You came back to my store. You gave me your information. I now have it. Deletion requests are not persistent. And just because you tell the company to delete your information doesn't mean the company has to close its eyes every time you interact with it or if it buys data from a third party.

[00:39:52.19] It doesn't mean that company has to maintain your information, scrub it against the information it's going to buy, and make sure it never recollects. Yeah?

[00:40:01.52] AUDIENCE: So I know that there are limits to when you have to respond to a deletion request. I think CCPA is what, 35? 45.

[00:40:08.86] DAVID ZETOONY: 45. Yeah.

[00:40:10.10] AUDIENCE: So does that mean that you actually have to delete the data, or can it be built into your records retention and disposal process, and you'd only need to respond at that point?

[00:40:19.94] DAVID ZETOONY: Yeah, so my recollection is the verbiage of the CCPA is that you have to provide a response. But it doesn't say you have to effectuate. As a practical matter, I don't know many organizations that would respond and say, we've received your request, and it'll be deleted in three years.

[00:40:33.36] And I think that may pick a fight with those who are intending the CCPA to actually mean the data was actually deleted within 45 days. That's my recollection. But I know that-- this is one of those bad drafting. Time periods for access and deletion were not drafted in the same way. They just use the same verbiage, whether that was intentional or unintentional? Open question. It did leave open some ambiguity as to what you can respond with in a deletion request on the 45th day. Any other questions on right to be forgotten?

[00:41:10.30] Right to opt out of behavioral advertising-- so one of the most asked questions is, is the use of behavioral advertising cookies consider the sale of personal information? I've spoken about this for about an hour, or two hours. I think we did a two-hour course on adtech. So the short answer is, there's a huge amount of ambiguity.

[00:41:26.74] The California AG was asked to clarify this during a rulemaking process, and they did us all the great favor coming back without anything other than it's a fact-specific question which I think doesn't really provide great clarity. But in terms of variables, what facts might influence. Whether adtech cookies or behavioral advertising cookies online are the sale?

[00:41:44.92] Did the consumer give opt in? I'd argue if they did give opt in like an opt-in banner, you can use cookies. It's not the sale of an environment. Did the behavioral advertising company agree to limit its use, retention, and disclosure, which would be under CCPA verbiage, making the behavioral advertising company its service provider? I'd argue if they agreed to that, it's also not the sale that's come to your service provider.

[00:42:04.18] And then, did the company that place the adtech on the website get something back specific for its placement? I think if nothing went back to the company, then it's also not a sale. These may sound a little academic. They're actually not. I can't tell you how many times companies' websites have found out that they've been leaking data.

[00:42:21.61] They've been sending data to third party inadvertently because somebody puts a tag on the site three or four years ago. But they're getting no benefits from that company. They're not even serving ads from that company. And one could argue very strongly that is not the sale of data because there has been no consideration. There's been nothing that they've received in return.

[00:42:38.17] Because of this, I think, it leaves a lot of ambiguity. It's very hard to answer this with a yes-or-no question about whether adtech in general is a sale. Yeah?

[00:42:47.50] MARGOT KAMINSKI: [INAUDIBLE] that. I might be misremembering but I think CPRA imposes a different standard for sensitive personal information, right?

[00:42:55.99] DAVID ZETOONY: It does.

[00:42:56.44] MARGOT KAMINSKI: It's not just do not sell. It's do not share.

[00:42:58.42] DAVID ZETOONY: Yes.

[00:42:58.72] MARGOT KAMINSKI: So would behavioral advertising be governed under that for CPRA with respect to particularly sensitive information?

[00:43:08.77] DAVID ZETOONY: Yes, it would. And CRPA-- CPRA, pardon me, imposes a lot more behavioral advertising. So one of the changes that happened-- and kind of fast forward, but for 2023, there was more clarity given. So now for CPRA, it says we've got the sale of data and we've got the sharing of data.

[00:43:28.39] If it's sharing of data which is going to be defined as giving any information over to a company that's going to do targeted advertising across websites, you have to give an opt-out right called Do Not share My Information. If it's a sell of data where you're going to give information to a company for consideration or for money coming back to you, you also have to give the opt-out right.

[00:43:46.24] So I think one could say, in 2023, it's very clear you're going to need an opt-out right universally, whether or not you have sensitive category data. On top of that, if you've got sensitive category data in 2023, there's going to be a separate obligation that you allow consumers to opt out of limiting your use of sensitive data for something other than what [AUDIO OUT] was provided for or what they've contracted for or kind of a list of some exceptions.

[00:44:10.39] In a world of adtech, it'll be interesting to see whether the sensitive issue has any bearing. I mean, typically, adtech cookies aren't transmitting sensitive category data because they're transmitting the data of the individual that's gone to the website. So it's usually the fact that you went to the website

but it could be transactional data or behavioral data depending on how much that is and how it's structured.

[00:44:30.40] Theoretically, since you're going to have to give the opt-out right for sharing and for sale, it's not really clear that having to give another opt-out right for not using the sensitive data does anything more. Either way, an opt-out right has been given or will have to have been given by 2023.

[00:44:47.98] Right to opt out of sale-- so one of the frequently asked questions-- 212 in the book-- how many companies that put a "do not sell my personal information" link on their website? So one of the foundational ideas of the CCPA was that companies that sell information should put a link on their websites at the bottom that people can click and say, do not sell.

[00:45:04.81] There's been a lot of misinformation about how many companies, A, say that they sell, and how many companies have offered the link. Some people, some regulators have said everybody's doing it. Other people are saying nobody's doing it. The real statistics is 21% of the Fortune 500 have put up the "do not sell" link.

[00:45:21.46] I would argue-- and I think this is beyond argument-- that is more Fortune 500 companies are doing it than people below the Fortune 500. Once you dip out of the Fortune 500, you end up with a lot of companies without lawyers, legal departments, or privacy attorneys, who have no idea what the CCPA is.

[00:45:36.16] So I think this is kind of the outer boundaries. You see about one in five companies putting up a "do not sell" link. That reflects that some companies are selling data and then have given the right reflects that other companies may be selling data but haven't given the right. There might be a violation.

[00:45:49.60] And it reflects the fact that there are some ambiguities about adtech and some strategic decisions companies have made about whether that is the sale or not the sale. But what we can't say is 79%, I mean, almost 80% companies have not put up a "do not sell" link. So we have a bunch of other things, and I to make sure we have enough questions-- time for questions-- so yes?

[00:46:10.51] AUDIENCE: On that basis, thinking about aggregate insights and selling that, how does that relate? And then, moving that into, say, the world of synthetic data, are there any rulings around these synthetic data as a non-personal information that can be sold?

[00:46:23.08] DAVID ZETOONY: Yeah, that's fantastic question. So aggregate data is exempt from the CCPA. It's not personal data if you've aggregated. So if you take data from hundreds people, you combine it together, come up with a statistic, that can't be really traced back to any of them. You're golden. You can sell that information.

[00:46:35.59] 20% of people who go to websites, eat pizza, whatever it is. Synthetic data and other ways of identifying data or trying to move it from identifiable to de-identifiable data is a strategy. And I say strategy because there's not a bright line on how much the identification is needed in order to really get to where you can't reasonably relate.

[00:46:56.62] But there is a standard. And the standard is if you can get there, so you can make it so it doesn't reasonably relate to the individual, and there's some differences here between the CCPA and the CPRA about what else you have to do in terms of, do you have to make a public representation that you're not going to try to re-identify? Do you have to make a public representation that you're not going to disclose the de-identified data or the synthetic data to third parties?

[00:47:16.31] Those differ between now and 2023. But by and large, there is the concept that you can explore de-identification to take things out of scope.

[00:47:23.38] AUDIENCE: To take it a step further, if someone's going to apply an algorithm to data that's held on site, is the access of the algorithm to the data considered selling personal data? Or is that--

[00:47:33.84] DAVID ZETOONY: Oh, it's a good question. It's a good question. The area of de-identification is a fascinating topic unto itself, particularly because the standard under the CCPA Virginia, Colorado, and Europe are different. So when you start getting to specific use cases of how much de-identification is de-identification, it can be a little tricky.

[00:47:54.22] MARGOT KAMINSKI: [INAUDIBLE] We actually have only around four or five minutes remaining until we get kicked out of the classroom for another class.

[00:48:00.71] DAVID ZETOONY: OK, I understand. [INAUDIBLE]. So let me jump forward, and we're not going to go through all of these other than kind of pick and choose. I think this actually might be the one to land on. So this is probably the number one question when I look at leadership. Do the CCPA and CPRA have the same definition of sensitive information?

[00:48:18.58] And the core layers of this, you could spin them off. What is sensitive information? Does x feels kind of sensitive information? There is probably no area that's more confusing in terms of how they drafted it. So under the original CCPA, there is no category called sensitive information. You won't find it.

[00:48:35.17] But there is a category of data that is given protected status more rights, and that is de facto sensitive information. So every privacy attorney in the world before the CPRA was passed would say, yeah, the CCPA has a sensitive category information. It consists of 13 data fields where they say, if you've had it breached in terms of hacking event or data breach and inadvertent loss, you can get sued on it.

[00:48:57.46] And this suit-- damages can be astronomical. That was the de facto. These are the sensitive categories. It included things like Social Security number, driver's license number. CPRA comes along, and they've now defined sensitive information. But they define it much broader. So it's a 21 data fields not 13 fields.

[00:49:14.90] They don't take away the old one, though. So you now have kind of a three-tiered sensitive category or three-tier personal data. You got big tier, all personal data. You've got the next tier which is sensitive data, and by that I mean, it's the 13 fields where if you lose it, you could get sued and have huge liabilities.

[00:49:31.93] And then, you have the officially designated sensitive data which has nothing to do with the private right of action necessarily, nothing to do with being sued. But it brings in, what Professor Kaminski was referring to, a new right that says you have to tell people that if you collect this and you're going to use it for some purpose other than what you originally collected it for, they have a right to opt out.

[00:49:52.27] I think the confusion around there is, again, you have this hidden de facto sensitive category which is what most attorneys historically have considered which doesn't get any label in the CCPA. It's just hidden in there some special category of 13. More confusion, because the 21 fields don't match Virginia and Colorado which followed closer to the 13 fields, and they do define sensitive information.

[00:50:13.94] So you could do a chart between Europe, California, now California 2023, Virginia and Colorado, on just what sensitive information is. And it's a mess. There's no really uniformity. So with that, those are some of the questions I want to highlight. I think we may have a minute. If anybody else has any questions, I'm happy to answer it or after the program.

[00:50:35.62] MARGOT KAMINSKI: I wanted to give you the opportunity to talk a little bit about the different models that are out there privately, not asking you to do that any form of detail. But you just referenced the Colorado Act which is very similar to the Virginia act. If you had to make a prediction of what model is going to win on a state level, what other states are going to copy, and additionally a

prediction on whether we will ever get federal data privacy law in the United States, what would your reading of the tea leaves be?

[00:51:05.08] DAVID ZETOONY: Yeah. So I'll say Colorado, Virginia, I think, are hands down better drafted. They're shorter. I mean, it's like one fifth the size, one sixth the size, but at the same time, there's less ambiguity. So they've accomplished the succinct writing that actually is more operational. I don't think I could have written a 500-page book on the Colorado law.

[00:51:22.06] Not that it doesn't do amazing things, it's just not that ambiguous. I think they're a better structure, and I would advocate that Colorado, Virginia be at least the starting place rather than California. And my sense for predictions is that most other states are going to go that way. And there's more of a history here.

[00:51:35.77] Colorado and Virginia were both modeled after a failed initiative in Washington. So the fact that you already have the Washington failed initiative being adopted in two other states and not the California-passed initiative being used as the model, I think, shows where most of the states are going when they start picking this apart.

[00:51:52.24] So my prediction as we see more states emulate Colorado, Virginia, federally, I've never gone out on a limb, I mean, I think the chance of-- it's just a crapshoot always. And I think at this point injunction, I don't see any real clear path to federal preemption, federal legislation. Yeah. I would think next year, we're going to see three or four more states, but we're not going to see federal government. Great question, though. Any other questions? And if not-- yeah?

[00:52:22.00] AUDIENCE: What's going to happen to the CCPA regs on January 1, 2023?

[00:52:28.52] DAVID ZETOONY: Oh, if we have them?

[00:52:29.41] AUDIENCE: You know the regulations that are in place now for the CCPA, what's going to happen to those on first 2023 when the CPRA comes into effect?

[00:52:39.08] DAVID ZETOONY: They're not rescinded, I don't think, officially by the legislation. So I still think that they progress forward. [AUDIO OUT] wonders, and we've had these discussions frankly with some regulators. One wonders what effect they have and whether or not their underpinnings have already been modified.

[00:52:53.99] I mean, you've got regulations on statute that won't exist. So can that regulation be enforced? I wish the California Attorney General's office would be clear about its intention, meaning I don't think there's a automatic rescinding of the new regs. I think they could if they wanted to try to enforce them and then leave it to the business to try to defend and say, your regulations have no statutory basis.

[00:53:15.96] That might be on a section-by-section question, though, for the regs because there's some regs that really-- they're interpreting a statutory provision that hasn't changed. And there's other ones that are interpreting statutory provisions that's totally changed. And it would behoove, I think, a regulator to try to clarify that situation and not let companies sort out themselves.

[00:53:35.45] AUDIENCE: Because I mean, it's not-- CPRA doesn't completely knock out CCPA. It's just a very significant amendment.

[00:53:41.51] DAVID ZETOONY: It's a very significant amendment, so because of that there's more ambiguity about what happens to specific line items in [INAUDIBLE].

[00:53:50.04] MARGOT KAMINSKI: So please all join me in thanking David.

[00:53:51.80] [APPLAUSE]

[00:53:57.37] DAVID ZETOONY: It's been a pleasure. Thank you all for having me.