State Privacy Laws Feb 2023

**SPEAKERS**

Cecilia Jeong, Anna Westfelt, Frida Alim

**Anna Westfelt** 16:10

Hi, everyone. I'm Anna Westfelt. I'm a partner in Gunderson Dettmer, San Francisco office and I head up a data privacy group. And I am very fortunate to be joined today by our two data privacy associates, Cecilia Jeong from the New York office and Frida Alim from San Francisco. And we will aim to keep today's presentation as practical as possible. We have a lot of material to cover, a lot of the focus will be on the new California Privacy Rights Act, the CPRA, which just came into effect January 1, but we will also highlight some important points in other state laws coming into effect this year. So I will hand over to Cecilia to kick things off with an overview.

**Cecilia Jeong** 16:54

Thanks, Anna so I'll kick off this section by laying down some context for how we got to this landmark year and US privacy legislation and by discussing some key concepts around the scope of these laws. So key question, how did we get here? Well, 2022 was a really big year for data privacy in the US. Five states passed comprehensive privacy laws. That's what we'll be focusing on in this presentation, and 27 other states considered privacy bills, a whopping 58 state bills were considered but did not pass. And now focusing on the comprehensive laws. What do I mean by comprehensive? This means privacy laws that apply to individuals kind of generally, obviously state specific.

They are not industry specific laws that we have in the US such as the GLBA, which is specific to the financial sector, HIPAA, which is specific to the healthcare sector. And these laws are also not data specific, such as COPPA, which applies to personal information of children under the age of comprehensive privacy laws impose obligations on entities throughout the lifecycle of handling personal information. There was also a federal comprehensive privacy bill that was introduced in a bipartisan effort. They got the farthest of any comprehensive privacy bill that was has been introduced into Congress, which there have been many, but it's really not saying much. They haven't gotten very far. It was voted out of the House Energy and Commerce Committee, but ultimately didn't make it to a House vote largely due to issues around the preemption of state laws, namely, the California Consumer Privacy Act, which I'm sure everyone has heard of called the CCPA.

Okay, so there when did these new law come into effect? Some key dates for you to keep in mind. On January 1 of this year, the Virginia Consumer Data Protection Act TCPA and the California Privacy Rights Act, the CVRA went into effect. The BC DPA, the original law is a new comprehensive laws specific to Virginia, and CPRA, amend what everyone again has probably heard of the TCPA. While currently in effect, the regulations of the CPRA have not been finalized, and they add a number of additional requirements, interpretations and other key provisions. As of the latest update, we're expecting the regulations to be sometime this April. The next key date to keep in mind is July 1, when there's three main events that will occur. The first is the enforcement of the CPRA, which will apply to violations occurring after July 1. And note that there's a new enforcement body, the California Privacy Protection Agency, that will happen for some power over the CPRA. We'll get into that later.

And the Colorado Privacy Act will come into effect. That's another new comprehensive privacy law. And as of right now, the enforcement of the CCPA the Colorado law is July 1, but maybe pushed by the California Attorney General. Again, that law also has regulations that haven't been finalized yet. The Connecticut data privacy act a CT DPA will also come into effect. And as of now, again, this will be enforceable upon And it's effective date after that, so the next key date to keep in mind is December 31, when the Utah Consumer Privacy Act, the UCPA comes into effect. Again, no deal with delayed enforcement here. So it will be enforceable upon the fact that once it becomes effective throughout this presentation, we will largely be referring to these laws as the Virginia law or the Colorado law. So you don't have to rapidly memorize these acronyms. We may again, use the term CPRA, because that will be a primary focus of the of this presentation.

**Cecilia Jeong** 20:36

Okay, so we'll talk about sort of the specific thresholds around these laws on the next slide. But I wanted to introduce a core concept not just to these laws, but pretty much to every major comprehensive privacy law.

The primary party, there's two parties that are really subject to these laws who must comply with the laws. The primary party subject to these laws are often called controllers or businesses under the CPRA, because they'd like to do a lot of different things. They are the party that determined the peace purposes and means of processing personal information. And they're also a party that has the sort of primary set of obligations underneath laws, including with respect to notice and disclosure. So generally, they're the business whose privacy policy is provided to a consumer at the point of collection. Usually, this includes b2c companies, though this is not a hard and fast rule. But it's a very common one to think of like Etsy or eBay.

The secondary party that's subject to these laws are processors or again, service providers under the CPRA. They are the parties that process personal information under the instruction and on behalf of a controller, typically, to provide a specific service. These parties are have secondary compliance obligations, many relating to their obligations to a controller not directly to a consumer, for example, to help the controller facilitate a consumer request, such as to delete their information. A common example of these parties are b2b businesses, again, not a hard and fast rule. But an example would be AWS.

While these are primary rules, and why I say this is not a hard and fast rule is that there's nuances in between, for example, many processor based companies are also participating in some controller activities. So that this makes it important when considering your obligations to identify the different crops, your different processing purposes, and activities and the role you play for each of those activities. Okay, now on to some specifics. We are who must comply specifically, we're not going to go through this line by line because I don't want to torture you. But we will talk about kind of some general elements of the thresholds. So for each of these laws, there's some form of doing business or targeting business and each state kind of trigger in order for these laws to actually apply. And that will vary between each law. And in addition to that, that's not going to be reflected in this table. But that should be sort of considered an underlying base consideration.

And then above that, there are sort of the three kind of big buckets that these laws look for. One is the revenue threshold. And revenue is generally considered pretty broadly, it's not state specific, and it can include, or it can be calculated across businesses that share common branding. The second category is a data count. So basically, the number of consumers who whose personal information is under the control or is being processed by a specific entity. Here, it's really important to note that even IP addresses are considered personal information, we get a lot of commentary from companies that say we don't have you, we don't collect personal information.

And then we'll look on to the marketing website and ask them how many individuals are visiting and often they will reach a lot of these thresholds. It's really important to keep it have a general understanding of your figures to figure out what you may or may not have to comply with. And note here, I just want to put a little asterisk that like the way consumers defined is going to impact how you calculate this, and we'll discuss that on the next slide.

The last part is that these laws generally look for certain processing activities such as selling of personal information. And if you are conducting that, which will again discuss later in this presentation, there's a couple of different ways that this can be defined. They'll look to specific revenues in connection with those activities or data, again, to collect the number of individuals whose data you are actually selling.

Another key note that I wanted to talk about in the scope of these laws is that there are exemption general exemptions under these laws. For example, under the some of the industry laws that I mentioned in the previous slide, the GLBA HIPAA as well as the SCRA for example, organizations that fall under these exemptions or that have datasets that fall under these exemptions may not be subject to these laws in whole. And so if you are working within a specific industry that's particularly regulated, that's really important to consider maybe as even a first step to determine what, what parts of your business or what parts of the data sets you have will actually be subject to these laws. Okay, so as I mentioned, who is a consumer, the law, aka, who are these laws aims to protect four of the states take one approach, and then California takes a slightly different approach, actually a pretty meaningful, different approach.

So Colorado, Connecticut, Utah, and Virginia really consider consumers to be what you would kind of typically expect to have a definition, its residents, individual residents acting within a personal or household context, aka not really a commercial context. What does that mean? Well, you can see it when you compare it with California, where California includes the definition of consumer residence in the previous sort of bucket as well as individuals acting in an employment or commercial context. That will include job candidates, employees, business contacts. And we'll talk a little bit more about that it's often called the HR or b2b exemption under California that sunsetted with the CRA. But we'll talk about that a little bit more in detail. Okay, so I'm going to now kick it off to Frida who are going to talk about the similarities and differences.

**Frida Alim** 26:39

Great, thanks, Cecilia. So each of the new laws draws inspiration from the California Consumer Privacy Act and the EU General Data Protection Regulation, the GDPR. So companies that have started complying with those laws are going to be in a good starting position to start working towards compliance with the new state privacy laws. There are also a number of similarities among the laws, which will substantially facilitate compliance for companies that are subject to more than one of the laws. For example, each of the laws require that the covered entity have a privacy policy outlining their practices with respect to the collection use disclosure of personal information.

Companies will also need to disclose the specific rights that consumers have under each of these laws in their privacy policy. Each law also requires that the controller provide the consumer with certain rights. And there are specific rights that are common across all of these laws. And those include the right to erasure or to delete personal information, the right to access personal information, the right to opt out of the sale of personal information and the right to opt out of retargeted marketing. Additionally, there is a right to non discrimination that consumers have, if they exercise any of the above privacy rights. Each of the laws gives enforcement authority to state agencies. The one unique thing here is that California's law is actually creates a new privacy agency in California, which is the California Privacy Protection Agency, which is solely dedicated to enforcing the CPRA.

We can go to the next slide for some key differences. There are obviously a lot of commonalities between these laws, but there are a few areas where they diverge. As we discussed previously, the threshold for applicability differ between these laws. You may be subject to one but not subject to another because you don't meet the thresholds into the other law. Most of the laws have exemptions for employee and commercial data except California. And again, it's going to go into further detail on that further down the line in the presentation. While there are several key rights that we just discussed, that apply in all of the states, there are a few states that don't offer certain consumer rights. For example, Utah consumers don't actually have the right to correct their data, or the right to opt out of certain automated decision making, which is typically called profiling and the other loss.

Companies will also need to make sure they keep track of the exceptions to complying with consumer requests, because they vary across the laws. You may need to comply with a specific type of request in one state. But there may be an applicable exception if the same right is exercised by a consumer in another state where you're subject to the law in that state. Another thing to keep in mind is that the definition of a sale of personal information varies across the laws. Again, you could be selling personal information of a resident in one state, but that may not actually qualify as a sale in another states. That's something you'll need to dive into when you're drafting your privacy policy if you're subject to more than one of the new state privacy laws.

Most of the laws require that you or you know, have language around providing an appeals process. California's appeals processes only at the discretion of the controller so you can actually you know, does decide whether or not to offer an appeal process. California has a limited private right of action, which the other states don't have. That's actually limited to the data breach contexts. But other than that, typically it's an agency or an attorney general that enforces violations of the law. Finally, three states require that the covered entity or the controller obtain consent to process sensitive data, whereas two states which are Utah and California have an opt out standard. You can process what's considered sensitive personal data, and we'll dive into that later in the presentation. But you have to give Utah and California residents right to opt out subject to certain exceptions that we'll discuss. So now I'll hand it off to Anna to discuss how the laws will be enforced.

**Anna Westfelt** 30:50

Great, thank you Frida. A lot of attention this year, of course, is on the CPRA with enforcement starting on July 1. And as we mentioned, what is new under this law and unique to California is this privacy protection agency of the cppa. But what's interesting is that the California Attorney General's still have enforcement powers under the CPRA. And if both are actively investigating, the agency actually has to defer to the Attorney General. Last year, we saw the first official settlement with AIG under the CCPA. That was a Sephora settlement published in August. And this settlement which resulted in a $1.2 million fine was for since a very clear message from the AG’s office that it is serious about enforcing California privacy laws. And the settlement related to support use of third party cookies and tracking technologies and its failure to honor opt out requests via the global privacy control. But other than that we don't have much to go on in terms of enforcement other than what we've seen, the Ag focus on kind of starting investigations and sending notices out with relation to that enforcement action, of course, was under the cppa at CCPA, which was the predecessor law.

As you'll see here, penalties are essentially the same under the CPRA ranging from $2,500 for each violation to $7,500. For each intentional violation. New under the CPRA is the inclusion of personal information of minors under 16. And this higher tier of penalties $7,500 per violation. The CPRA as we mentioned, unlike the other state laws has a limited private right of action. It is only for security breaches of certain kinds of more sensitive personal information. So for example, Social Security numbers, driver's license numbers, health information. What's interesting here and was new under the CPRA is that this private right of action also applies in the event of a breach of usernames or emails together with a password or answer to a security question.

Information needed to gain access to an online account. This means that many more data breaches will be in scope for this private right of action and expect to see many more class actions filed under this available private right of action. Step two damages under the private right of action are a little bit different than if enforced by the agency or the AG. The statutory damages are 100 to $750 per consumer per incident or actual damages, whichever is greater. A couple of things to note with that is that effective, consumers don't actually need to show any injury or harm as a result of the breach. The statutory damages are available if it is a breach that is within scope for this private right of action. And also, as you can imagine, if you have a breach that involves several million consumers, damages could potentially be very, very high hair.

The liability under the private right of action or data breaches is not strict. It only applies if the breach was a result of the business failing to implement reasonable security procedures and practices. And we know that the CCPA has already led to an increase in data breach related class action filings. These have not been adjudicated yet they're all working the way through the court system. But as we will mentioned throughout this presentation, it is really important to get your security measures tightened up because you do not want to be subject to one of these class actions. Next slide please.

Similar to Virginia on the other slide, Colorado Utah, Connecticut, have enforcement by the Ag or the state agencies, no private right of action, and monetary damages and injunctive relief are also available. And of course, injunctive relief means that you could be ordered to do something or stop doing something. And that could potentially be really disruptive to business. And as you can see, potentially substantial monetary damages. Next slide, please.

So it's interesting to pull together some common themes. And as we've seen by now, a private right of action is really unpopular, it's hard to pass a law that has said it is unpopular with industry. We just don't expect to see a lot of private raction private rights of action in state law. So we just have at this time, we just have California's limited private right of action for breaches of certain kinds of sensitive information. However, without even without this private right of action, state AGs are very active enforcers in privacy and consumer protection laws, in particular, in the last few years. So we expect to see a lot of activity in this area in 2023. And of course, we also see a lot of activity from the Federal Trade Commission. And that's only going to ramp up this year.

And as I mentioned, statutory damages per violation can add up to very significant amounts. So for some practical tips, we recommend that you document your compliance program before anything happens. Make sure that you can show that you took reasonable steps that you implemented security that you that you really thought about how to protect this data is really important to have timestamp evidence of security, for example, security measures before a breach happens, because we know that implementing reasonable security after a breach is is not considered a cure of that breach.

If you think one of the state laws don't apply to you, doesn't apply to you just make sure that you've documented why so that you're not put on the defensive if an AG approaches you. It's a really good idea to have thought about that before. Next slide, please. So there's this really interesting concept of a cure period, it was available under the CCPA, there was a 30 day opportunity to cure and it wasn't certain how it applied to data breaches, if the information is already out there, questionable whether that could actually that breach could actually be cured. But it was a very, very helpful right available to companies. The CPRA eliminated that mandatory cure period, and is now discretionary for the agency to provide a business with a time period to cure.

Looking at the other state laws, there are cure periods. But in Colorado, Utah, and Connecticut, these will sunset either next year or the year after. So really only Virginia has a cure period that will last and remain in place. So the practical tip here is that this cure period is a really powerful, right available to you and in the States is not going to be available for that long. Do make sure that you avail yourself of it when you can, especially as you are ramping up your privacy program for the states. Carefully watch out for any notices that may start the cure period, we tend to take a very broad view of what my start secure period just to be on the safe side.

And it's worth noting that Sephora did have the 30 day cure period on the CCPA. And they did not cure the violation in that period. So it is something that we pay a lot of attention to. So that concludes part one of our presentation and now we will move on to highlight some key compliance considerations. And I am going to kick it off with talking about sensitive personal information. Under the CPRA we have this new concept of sensitive personal information, it did not exist under the CCPA. The definition includes things that you would expect to have a heightened level of sensitivity. For example, Social Security numbers, passport numbers, information revealing a consumers finances. That's not very surprising to see a heightened level of sensitivity and increased obligations with respect to we also see some similarities to the EU's GDPR. Here. There's inclusion of for example, biometric information, genetic data, ethnic or racial origin, religious beliefs and so on. These are consistent with the GDPR definition of special category data. Rationally surprising or at least noteworthy is the inclusion of a consumers present geolocation, that is something that a lot of tech companies collect.

Also the contents of a customer's communications, so email, mail, texts, unless these are directed to the business. So whatever consumer sends to you in an email is not sensitive personal information. But if as part of your service you access a consumers communications that is sensitive personal information, there is an exception for publicly available information, and that that concept is a little broader under the CPRA, than it used to be under the CCPA. It is a potentially helpful exception. Next slide, please. Do you need opt in to collect the sensitive personal information under the CPRA? The answer is no. There is an opt out right? That applies in some circumstances, but not opt in. If you are using the sensitive personal information for a purpose, outside of what the statute says are permitted purposes, then you have to provide consumers with a right to opt out there are limitations to it. And you have to notify them of this right. And you have to have a link on your homepage that says limit the use of my sensitive personal information.

Some of you may have started to see these links pop up on websites. So how does this work? In practice? What are some examples of permitted purposes, probably the most useful one is the first one here on the list, performing services or providing goods reasonably expected by the consumer. So for example, if you have a health tracking app, the consumer will reasonably expect that you will need to collect certain health information to provide that app to the consumer. If you process payments, the consumer will reasonably expect that you have to collect credit card information and use it for that purpose. You are also permitted to use the sensitive person information for product or service improvements, which is a really helpful permitted purpose for a lot of tech companies. Because this is something that is commonly done in practice, the way you have to think about if say, for example, with a health tracking app, if you are also using the health information to build a profile about the individual and maybe monetizing that or figuring out other ways to use it outside of providing the service to the consumer, then you will have to provide an opt out right for that.

So really, the practical tip here is if you're collecting anything that falls under this sensitive person information, categories, make sure that you evaluate how you are using it. If you need to implement an opt out procedure, then make sure that that is also followed through on the on the back end, it's not enough to just put up the link on your website, you have to make sure that it is followed through in every step of your your organization. Next slide, please. So I'm going to touch on Virginia here as well, since that's when that is in effect. Now as well. It is quite different from the CPRA. In this area, you actually need opt in consent to collect sensitive data, which is the term used in the Virginia law. And what's interesting here is that the standard of consent, and they were set in the GDPR, which I think many of you will know is a very high standard. Consent has to be clear, affirmative. freely given specific, informed and unambiguous, there is a lot of enforcement under the GDPR for failure to get the right standard of consent or consent was insufficient.

That may be something we start to see here. We were really watching this closely. What's interesting to note here, though, is that the definition of sensitive data is narrower in Virginia, and then California. So it could be that you are collecting sensitive personal information in California, but you are not collecting sensitive data in Virginia. So the practical tip here is to consider the narrower definition in Virginia. If you do collect sensitive data, you have to implement an opt in process. And again, make sure that it is followed through on the back end. So now I am going to hand over to Cecilia to talk about selling sharing and targeted advertising.

**Cecilia Jeong** 44:34

Thanks Anna. This might become everyone's least favorite topic that we discussed today. But I am going to go through them one by one. Okay, so targeted advertising or sharing under the CPRA. There is the definitions. What we're seeing is that each of the privacy laws impose certain obligations surrounding the types of activities and while the definitions will vary between the law As you can think of it broadly as the sharing of personal information with another entity for the purposes of targeting advertising to a consumer, based on the consumers activity across businesses, distinctly branded websites, applications and services.

What that means is we're really looking at the combination of dates of data from two different sources, two distinctly branded platforms, websites, application services, combining that data for the purposes of specifically targeting a consumer with an advertisement based on that consumers activity across websites. And so really, what they're trying to get at is kind of tracking what we would call cross your cross contextual Behavioral Advertising targeting advert targeted advertising, you'll hear these terms kind of used relatively interchangeably, but there's really kind of getting the same kind of activity. There are some general exclusions. We'll go through them one by one, advertising based on activities within a controllers own website or online applications. And that's just one controller.

I think you really need to keep in mind this sort of consumers perspective on this. And it's if there's two distinctly branded websites that are owned by a common use or common controller, that doesn't necessarily mean that you're going to fall within these kinds of general exclusions. Advertisements directed to a consumer in response to the consumers Request for Information feedback, or search query. If you are, for example, operating a marketplace and I look for shoes, right, or a consumer looks for shoes, and then is given advertisements for shoes based on that search, that wouldn't be considered or across contextual behavioral advertising for these types of purposes. And that advertising would be served just on that marketplace. And the third one is processing personal information solely for measuring reporting, advertising performance, reach or frequency. Again, not hard and fast rules. But we think these general buckets will help folks kind of discern what activities are likely to fall within this category.

Our practical tip is really to identify all applicable activities. with a particular focus on advertising, marketing and retargeting cookies, I think this is going to be the most common way that entities trigger this, these types of activities, and therefore have to have obligations to provide an opt out. And so really, take a look at those, if you haven't done a cookie stand, please do one ASAP. And then you can see the types of cookies that you have on your website. I think a lot of a lot of companies are surprised at what actually exists on their website. And once they do this are able to actually weed out some of the cookies that are being used, or at least start questioning what they're used for. And if you are participating in these types of activities, then then you should implement one to two mechanisms to opt out that really depends on the law, California requires two mechanisms to opt out. And each of these laws really are going to include at a minimum opt out via a global privacy control.

Now global privacy control we use in capitalized terms because that's sort of the closest thing we have to an industry standard of a seamless opt out global the GPC is you can just Google it, look it up online, they it's basically a signal that's sent via particular browsers or a plug into a browser that and that sends a signal to any website visited via those browsers that says that this individual does not want to be sort of tracked provided targeted advertising, things like that. Generally speaking, these states are looking to those signals as they are considering those signals and opt out to targeted advertising or sharing activities. Oh, if you are if the cookies are the reason why you are sort of targeted advertising for sharing, we really recommend working with Cookie consent mechanism providers, and a lot of times they will have a built in feature that acknowledges GCCs. And we'll let that flow down into the data that's being collected via the cookies on your sight. Okay, selling, selling is also a really hot topic under these privacy laws. They are this is distinctly different from sharing or targeted advertising, but we're gonna see a lot of overlap, particularly because of the CTR A, and I'll explain that.

There's generally two forms of definitions that is that the state laws use for selling there's a broad and a narrower, the broad for example, under California or Colorado, where sharing personal imperfect work, which includes sharing of personal information in return for monetary or other valuable consideration. And the key here is the other valuable consideration, because that means it doesn't have to be a data for dollar transfer, but that you could have some other kind of commercial or business value in return. For the data that you're sharing with another party, and the narrow definition is, for example, under Virginia, which includes sharing of personal information in return for monetary consideration, and that is more of a classic data for dollar kind of transfer. In effect, what does this mean, when looking at the state's kind of broadly, you should just basically assume that all data sharing relationships constitute a sale unless subject to an exception.

And this is really particularly looking at California, because I think that obviously, there's six of us there, that law probably has the most teeth, and it has the broader definition of sale. And so, the most common exemption, or exception that is used for sale under the CPRA is a service provider is that if you're sharing data with a service provider, it does not constitute a sale, and your contract will have to have a specific language to this effect. However, under the current regulations of the CPRA, it clarifies that any recipient of sharing or targeted advertising as we previously discussed, like actually defined sharing, it cannot be a service provider under the CPRA. And therefore, a lot of sharing relationships will also constitute a sale under the PcrA. So and I want to make that really clear that a lot of sharing relationships will constitute a sale, but that does not mean that all selling relationships will constitute a share.

So it's a little bit complex, there's going to be a bit of an overlap, but they are, they're both related and distinct. Okay, so practically speaking, it's pretty similar to sharing, you have to inventory all of your third party data sharing relationships, make sure you have the risk provider language where they apply. And if you are sharing also make sure that that that it process is considered when you're determining what relationships constitute selling. And if you are selling it's a similar opt out process with sharing or targeted advertising, you have to implement one to two mechanisms to in California. And they will include again, the GTP. Okay, so I'm going to move it to Frida, we're going to talk about GPA.

**Frida Alim** 52:09

Great. Thanks, Cecilia. If we move to the next slide, we can kind of look at an overview of what the new requirements are around data protection impact assessments. Next slide, please. Great. So most of the new state privacy laws have some requirements around conducting a risk assessment where there's some form of processing, that the legislature or regulator views as high risk to the privacy of consumers or to the security of their data. This, this slide kind of shows you an overview of how these laws stack up side by side. I'm not going to go into detail on this. But generally, the triggers are pretty similar across these across these laws, the content of the risk assessment is also pretty similar.

There is some variation in terms of whether these risk assessments need to be disclosed to the regulator. Some of them will require that you disclose the risk assessment to the regulator on a regular basis, whereas other others only require disclosure upon request of the attorney general or the other enforcement agencies. We can actually go to the next slide just to talk about takeaways from reviewing the risk assessments from these laws, which I refer to here as DPI a takeaways.

There are key activities across most of these laws that trigger the DPA requirements. So if you are engaging in targeted advertising, selling data, certain types of profiling, which is essentially automated decision making that produces legal or similarly significant effects for the consumer, or you're processing, what ever data falls into the category of sensitive data, you'll likely be required to conduct a DPI A. So you may need to actually perform more than one DPA. If you're doing more than one of these activities. There's pretty substantial overlap between the requirements in terms of what should comprise the risk assessment or the DPA. You may need some customization to accommodate requirements in a different state. But generally, if you do perform one for one state, you could probably use a version of that to satisfy requirements in the other states.

For example, candidate kids law actually explicitly provides that a DPA that's conducted for purposes of complying with another law would satisfy Connecticut requirements, if reasonably similar in scope and effect to the Connecticut DPA. So again, some state regulators may request the DPI A's. Other regulators expect to just receive them on a regular basis as you're updating them or drafting them. One thing to note is that most of the laws have language around disclosure of dpi A's and the fact that those DPI A's will retain their confidential status or their privileged status, and that they'll be exempt from Freedom of Information Act requests, which are essentially requests that a consumer can make to access public agency documentation. So again, in most cases, disclosure to the Ag or the other agency is not going to waive privilege or protection. But we do recommend for that reason that you work with your counsel to make sure that the DPA is actually a privileged document. We can actually go to the next slide. We're going to talk briefly about data processing agenda.

On the next slide, please, each of the laws have specific language that's required in agreements with service providers or processors. We refer to this as a DPA or data processing agenda. So what should you be doing now in terms of preparing for these laws or getting into compliance with the CPRA law or Virginia's law, so processors or service providers should be updating their contracts to make sure they have the most up to date, language in their agreements, and companies that are controllers or businesses should be checking vendor contracts on a go forward basis to make sure that they reflect the appropriate language. If the controller is subject to the CPRA, there's very specific language that actually needs to be included in the agreement with their service provider. What needs to be included within these updated contractual terms. Generally, the laws have a lot of commonalities in terms of what should be in these terms. It should state for example, that the service provider or processor is not going to use the personal information that's processed on behalf of the customer for any other purpose than performing the services.

Typically, there will be restrictions on the service providers ability to share that data, data or sell that data to any third parties. Some of the laws that come into effect this year have some unique requirements. For example, California states that the agreement should explicitly state that the business or the customer can take reasonable and appropriate steps to ensure that the service provider acts consistently with its obligations under the law. In terms of our takeaways from looking at the industry, here, there is generally a trend towards having state or country specific agenda or exhibits to the DPA that cover requirements in specific regions. Since there isn't an exact overlap. There are different kinds of ways that you can approach this but if you are, you know, a service provider that's providing services to your customers, you should make sure that your TPAs are up to date with the new requirements. And if you're a Gunderson client that's been using our form DPA, feel free to reach out to us and we can help you move on to our updated form DPA. And I will hand it off to Anna to discuss employee and candidate data.

**Anna Westfelt** 57:52

Great, thank you Frida. Something really interesting is going on in California when it comes to employee and candidate person information. The original CCPA was never intended to be an employee privacy law, and there was an exemption in place that excluded employee and candidate data from most of the provisions of the CCPA. However, that exemption expired January 1, when the CPRA came into force, and the California Legislature really surprised us all by not renewing it. This means that employees and candidates now have all the rights of consumers under the CPRA. And the most important ones to discuss here are the rights of access and deletion. These rights already applied to employees and candidates in the EU and UK under the GDPR. And as we have seen, these are often weaponized pre litigation or as an alternative discovery process. We expect to see something similar here.

This is why we're paying a lot of tension attention to requests from current and former employees and candidates. And we do recommend that you consult with your counsel if you do get one of these requests. There is already more limited right to know for employees under the California Labor Code. But what we have now under the CPRA is much more extensive. And the exceptions aren't completely helpful in the HR context. The right to delete can be quite problematic because there are often very good reasons to keep information about current and former employees and candidates and that includes for reasons of defending or exercising legal rights or to prove your compliance with HR related loss.

There can be a lot of reasons why you want to hold on to this information. Also worth mentioning, is that the right to opt out of automated decision making technology now applies in the employee and candidate context and automated decision making This technology is used very frequently in the employment and hiring process. This is something you need to pay attention to. We're also seeing this concept and other laws. For example, there's a New York City Law and automated employment decision tools that comes into effect this year. For practical tips, make sure you update your employee and candidate notices. The ones you had under the CCPA are now out of date, because they don't have all the applicable rights.

You need to make sure that your job postings for at least for California residents have the candidates notices linked, you need to make sure that your employees receive this notice that they notice. You can send it out via email, you should also include on your new hire materials, you may want to post it where your OSHA policies are posted, you basically have to look at all the ways you distribute this notice to make sure it reaches California, employees and candidates for the candidate notice, a very important point is to make sure you provide internal training on thoughtful document creation. The safest approach is to not create something that you don't want to give access to. And really any document created in a truck context can now be subject to an access request. It is really important to make sure that everyone is aware of this within your organization.

For example, when you create interview notes, or hormones, record records, or internal communications about an employee or candidate, you should always think of this with the lens of this could be subject to an access request at some point. And you should always have a plan in place for handling requests from employees and candidates. That often means involving your counsel if there was litigation brewing, which is often the case when we see these requests. Next slide, please. Just very quickly here, the b2b personal exemption, personal information exemption also expire January 1. So this means that your b2b contacts now have all the consumer rights under the CPRA. That includes personal information collected in the context of contracting sales, support services, etc. You have to make sure that you comply with the rights, the various consumer rights and that you provide the required notices. This does seem a little bit less risky than the employee and candidate exemption expiring, but it is something worth noting. So now I'm going to hand over to Cecilia to kick off part three of our presentation talking through the practical compliance steps that we recommend.

**Cecilia Jeong** 1:02:39

Thanks, Anna. This is probably the most useful part of our presentation for everybody. We're going to be going over these next, these sort of eight buckets of steps that you can take that we recommend in order to comply with all the laws that we've been discussing today. So first kind of moving broadly, this is kind of a big picture to do for most companies, especially those that have taken preliminary steps to comply with the existing privacy laws, I guess prior to January 1, the largely GDPR and CCPA, which is to conduct a gap assessment. Generally speaking, this means to determine which privacy laws apply, and how. And after that, you would then identify your very clear specific obligations under each of the laws, you can conduct an assessment against your current existing privacy practices. That would be the identify the gaps, and then you would work with counsel to form a remediation plan.

As part of this, what's really key and probably one of the most like painstaking parts of it is to take inventory and to update your data related documents. I know this is a hard term for everybody. But data mapping really needing to create or updating an inventory of your data is really important. And we know that this is a strenuous process for a lot of companies. But you at least need to know kind of the big buckets of the types of personal information that you're collecting, for what purpose and from who that flows into my next point, which is to identify your data flows. So input, who in the company internally is is handling this type of data? Where is it being stored, and output where you sharing it with? Again, that will impact a lot of your obligations. Under these laws.

The third step would be to compile a list of third party vendors, processors, sub processors, again, as previously discussed, there may be obligations of contractual provisions that need to be included with each other with respect to each of these parties. The fourth is compiling all privacy related agreements, often it's going to be DPA. But there could be other privacy or security provisions in other types of agreements. And lastly is to identify all privacy related documentation other documentation in the agreement, so for example, policies and that will be internal and external and determine if they are up to date.

Okay, the next practical tip We recommend is to assess your processing activities. And again, they are really specific. So you should identify each of these specific processing activities and in particular, look to see if you're conducting an activity subject to heightened compliance obligations, or that's likely to be the target of enforcement. These are some examples collecting sensitive personal information selling, sharing targeted advertising, collecting children's personal information and financial incentives, which was another part of this before enforcement action that happened last year. From the trends that we've seen in CCPA enforcement. So far, the areas that have priority has been online advertising failure to address consumer rights, notice regarding financial incentives, and then service provider contract terms, and largely their impact on sort of selling activities. I'm going to kick this next one off to Frida.

**Frida Alim** 1:05:58

Thanks. I'm just going to quickly go through what you can do now to start preparing to comply with consumer requests. As we discussed, consumers under these new privacy laws have a number of rights including accessing deleting, correcting data, etc. to prepare for being able to comply with those requests, you'll need to understand the types of data you hold and where that data is stored. If you have vendors that are processing personal data on your behalf, you'll need to make sure that you flow down requests to those vendors and make sure that they also delete any data that they hold on your behalf. You need to provide consumers with a way to exercise their rights and some laws are more prescriptive than others in terms of prescribing the exact method by which the consumer should be able to exercise their requests. Some require recognition of opt out signals for certain activities in other instances, and may suffice to have an in an email to field a request, you should also devise a way to verify the consumer again, here some laws are more prescriptive than others and require specific methods of verification. Depending on whether the individual has an account with you or not.

You should also ensure that you can provide data in a portable manner where that's required by law, you should ensure that you can delete personal information for all from all relevant databases. This is an area where sometimes companies struggle, they may think that they deleted all of the personal information they hold about a consumer. But then a consumer comes back a few weeks later saying hey, you sent me a marketing email, which shows that obviously, that data wasn't deleted from a marketing database. Some of the laws have specific timing requirements. You need to answer the request within a certain period of time. You want to make sure that you are actually operating within those prescribed time periods. And most of the laws, again, have some language around an appeals process. So if you're required to provide an appeals process, you want to think through what that's going to look like and potentially describe that in your privacy policy.

Finally, I just wanted to note that it is worth thinking about developing a strategy to how you'll honor requests from consumers, depending on where they're located. We do increasingly see companies decide that they're going to honor requests, regardless of whether the where the consumer is located. Other companies decide they're only going to honor requests, if it comes from one of the states where the consumers actually have rights by law. And I think we can move to the next slide on updating public facing privacy policies. Each law has some disclosure requirements. You'll need to disclose generally, the types of data you collect, how you share that data and your purposes of processing that data, you'll also need to disclose the rights that consumers have over their data. When you're approaching updating your privacy policies, there are a few things that you should keep in mind. One is understanding your role, whether you're a controller versus a processor over the data, because that will impact how the privacy policy is drafted.

Another thing we always recommend doing is conducting a data mapping exercise that Cecilia outlined to really get your arms around the data that you collect and how you use it to make sure that privacy policies accurate. Obviously, always involve the appropriate internal stakeholders. And consider all sources of data, whether it's your know your offline collection, your website collection or collection, through your application, and then understand whether you collect and process sensitive data in a way that triggers opt in or opt out. Again, this kind of goes to the consumer rights that need to be disclosed within the privacy policy.

Finally, I just wanted to flag that the CPRA has a unique requirement around providing a notice that collection which is essentially notice that should be provided to consumers at or before the first collection of their personal information. You want to think about when you would display that to the consumer. And we can move to the next slide please. And I'll just quickly mentioned that there are some technical solutions out there that you can use to assist with certain aspects of compliance. So there are now vendors that assist with for example, conducting a data map rake exercise. Some of these vendors are more automated than others. If you know that you have a ton of data sources and you need help understanding, you know where data is coming from which vendors are processing it, etc. It's likely worth engaging one of these vendors to help you with doing the data mapping exercise. We also previously mentioned you can use a vendor to assist with Cookie banners and operationalizing opt out and opt in to certain cookies. There are also vendors that assist with security. For example, you can obtain ISO or sock two certification which will help you establish appropriate appropriate level of security for these new privacy laws. There are also vendors that help conduct penetration tests and prepare vulnerability reports for you. And that, and I will then hand it over to Anna,

**Anna Westfelt** 1:11:05

thank you Frida. Another really important compliance step here is implementing a data retention policy. Many companies already have one, but it may not be actually compliant with these new new laws. And some relevant concepts when we talk about data retention are the concepts of data minimization and data limitation. And this essentially means that you shouldn't collect process or retain more data than you need. And you shouldn't hold on to it for any longer than is necessary for the purpose for which it was collected. These are GDPR concepts that are now pressing the US state laws. And this will likely require many US companies to change how they think about data as an asset, you just you can't over collect, and you can't hold on for things for as long as you would like, which might be indefinitely. So how do you implement a data retention policy?

The first step is as we have mentioned, throughout this presentation, you really have to do an inventory, you can't do a data retention policy, if you don't know what kind of data you have. You need to bring all the relevant stakeholders to the table within your organization that will be data related to marketing, to HR to analytics, there are so many different types of data within an organization, you will need to make sure you're interviewing the relevant people, you really need to know your internal and third party systems where all the data is kept. retention policies typically have to be very customized for each company. But what's also very important is to make sure that you meet state by state requirements, but different types of data, for example, tax data or HR data, there are some very specific obligations under US state laws. And these vary. Also, if applicable to your organization, you may have to consider GDPR data retention limitations when you create this policy. Under the CRA, you have to make sure that you inform consumers of your data retention periods, at or before collection. So there has to be some information in your privacy notice about the information that you collect from consumers and how long it is being retained. Think about how your data is getting deleted, can you rely on automation, where appropriate, you really reduce your risk by not holding on to data for longer than you need. And it is not uncommon for data breaches to involve legacy databases that an organization forgot they had, we see a lot of that at this time.

You may also need to tighten up your vendor contracts deletion requirements. These in the past sometimes are a little bit loose that you have to actually request deletion or otherwise the vendor will hold on to the data even after you have terminated the relationship. Data breaches very often happen at the vendor level. And it's really common to have a data breach where you basically you find out that an old vendor still had your data because it was breached and made public and you didn't even know that they still had your data. And finally, and this is really important. It's great to have your data retention policy done. But you have to make sure that it's actually followed throughout your organization and by your vendors. This is not a matter of creating a policy and putting it away in a drawer, you really have to train the relevant people and consistently make sure it's followed. So next slide, please.

Since we're about to hit the hour here, but the data security measures are really important under all these state laws. It is a clear obligation under the CPRA to implement reasonable security. The CPRA doesn't tell you exactly what that needs to be is do you have to determine it on a case by case basis depending on the risk and sensitivity associated with that data. We do have some guidance and some statements. From previous ag predating the CCPA, endorsing the Center for Internet Security, the CIS control as an example of reasonable security. So that's something we're very often look towards. But we also look at other industry frameworks and standards depending on what kind of organization you have. So we look at the ISO 27,000 series, SOC two type two HyTrust, maybe PCI DSS if you have credit card information. And NIST is a very commonly used framework, and consider engaging vendors. They can help you with a lot of these steps and security.

And, as I mentioned before, make sure you document your security measures before something happens. You want this document to be time stamped, put it in a memo and send it to the relevant stakeholders so that you can show that this wasn't done after a breach or legend violations. And that wraps up our presentation today. Right at the hour. We really thank you for joining us. And if you have any questions, feel free to send them to insights@gmail.com and keep an eye out for future webinars on the various developments on the state and federal sites this year. There's a lot happening in the privacy world and we love talking to you about it. Thank you also to the other panelists for presenting and have a great day everyone.