Business Better (Season 2, Episode 32): Cyber Adviser – The Colorado Privacy Act and Draft Rules

Speakers: Phil Yannella and Greg Szewczyk

Steve Burkhart:

Welcome to Business Better, a podcast designed to help businesses navigate the new normal. I'm your host, Steve Burkhart. After a long career at Global Consumer Products Company BIC, where I served as Vice President of administration, general counsel and secretary, I'm now of counsel in the litigation department at Ballard Spahr, a law firm with clients across industries and throughout the country. This episode is part of our cyber advisor series where we discuss emerging issues in the world of data privacy and security. With its draft rules, Colorado has set forth a new model for state privacy laws. While there are many areas that are interoperable with the California model, the Colorado draft rules include important differences as well as rules on topics that have been notably absent from California's draft rules. We discuss the highlights of the Colorado Draft rules, differences with California, and practical steps for developing a comprehensive compliance plan for all of the upcoming 2023 laws. Participating in this discussion are Phil Yannella and Greg Szewczyk, co-leaders of Ballard Spahr's Privacy and Data Security Group.

Phil Yannella:

Hi everyone, and welcome to Ballard Spahr's monthly webcast of emerging issues in the world of data privacy and security. In our last webcast, we addressed the recent surge and wiretap litigation. Today we're going to focus on the Colorado Privacy Act and in particular the status of rulemaking. My name is Phil Yannella and I'm joined today by Greg Szewczyk, who is a litigator and co-chair of the Privacy and Data Security Group. Greg's based in Denver, and he's been tracking the Colorado privacy act since it was first proposed several years ago. He's going to be doing most of the talking today as he's been on the ground floor and has a lot of keen insights into the development of this law. As our listeners know, there are five comprehensive state privacy laws in the US, California, Colorado, Utah, Virginia, and Connecticut. If you poll most privacy professionals, they will tell you that the two laws that stand out with regard to complexity and scope are California and Colorado.

The CPRA, which is California's law, has gotten a lion's share of attention, but no one should be sleeping on compliance. With the Colorado Privacy Act, it contains almost all of the same privacy focus features as the CPRA, and adds some additional nuances that can make compliance broader and more complicated. For example, the CPA has explicit consent requirements for the collection of sensitive data, which is a first at the US state level. The Colorado Privacy Act is also the first state privacy law that applies to non-profits, which has raised alarm bells among higher ed and other charitable organizations that typically haven't had a concern themselves with US privacy law. The bottom line is that complying with the California law in is not necessarily going to entail compliance with the Colorado Privacy Act. The CPA is currently undergoing rulemaking. The Colorado AG issued regulations on proposed regulations and October of 2022, final regulations are expected to be released in the spring of 2023, and the law will become effective in July of 2023.

So here's the outline for our discussion this afternoon. I'm going to kick things off with a review of the timeline and the status of rule making. I'm then going to hand things off to Greg, who's going to discuss the details of the CPA, along with providing a summary and then some important takeaways. Again, as a Colorado based privacy lawyer, Greg is a unique view on the development surrounding the CPA. All right, so let's begin with a quick summary of the pillars of the Colorado Privacy Act. The CPA contains the same foundational features as really all of the US privacy laws, as well as the GDPR and other foreign privacy laws. Compliance begins with transparency. Colorado requires that companies disclose the collection use sharing and retention of personal information in simple, clear and understandable language. The second pillar is consumer choice. Armed with transparent disclosures that Colorado loss strives to empower consumers to make informed decisions about whether to provide their personal data to a website or open an account.

The Colorado Privacy Act like many of the other new laws also has a heightened focus on dark patterns, which are graphical interfaces that may nudge or even deceive consumers into making certain decisions about the use of their personal information. We're expecting a great deal of focus on the issue in the years ahead. The law also provides for role-based

obligations, which are dependent on whether a covered entity is a controller or a processor. These categories mirror the language used by the GDPR, whereas California speaks in terms of businesses and service providers. But the concepts are the same. If you're a company with a primary relationship with an online consumer, you are a controller and have heightened obligations under the Colorado law. If you're a vendor and that the company hires to process data consumers, you are a processor and you have different and lesser obligations for the most part.

The important point is that companies can be both a processor and a controller depending on their interactions with the consumer. The Colorado Privacy Act like all of these new privacy law adds limitations on the use of personal data. The law provides for opt out mechanisms so that consumers can prevent the sale or sharing of their data. Consent is required to collect sensitive data, and the law will restrict certain kinds of automated decision making activities, which will have particular relevance as the use of AI proliferates in the US business community. Lastly, the law imposes data minimization requirements, which has been another focus of global privacy regulators. The notion here is that companies should only collect store and use the minimum amount of personal data possible for the minimum amount of time. Now, this has been a soft regulatory requirement for years in the US and certainly at best practice, but there hasn't been any real enforcement, with the passage of the CPA as well as the CPA and other US privacy laws.

We're expecting that there will be increased enforcement of data minimization requirements, and frankly, we're already beginning to see that as reflected in some recent FTC consent decrease. This is a timeline and status of rule making right now in Colorado. In April 2022, the Colorado Attorney General released targeted questions seeking informal feedback on particular issues. Then in October of 2022, draft rules were released, and in February of 2023, we're expecting that the formal comment period will end. The period right now that's denoted in green highlighting is the comment period. We are in the midst of that right now, and I want to stress that this is a really important time period. Many of our clients, particularly many non-profit clients, have been asking us the extent to which the Colorado Privacy Act is going to apply to them. And one of our recommendations is for people to put in comments to to the Colorado AG.

They want comments, they've been explicit in their desire to hear back from the business community. They are considering those comments and there's every reason to believe that if the comments are well argued and well considered that they will be reflected in new regulations. So, if you have any questions about the scope of the CPA, particularly naughty compliance issues, we do recommend that you put in a comment. The end of the formal comment again is February 1st, 2023. The effective date is July 2023, and we are expecting to see final regulations from the Colorado AG sometime probably in the late winter, early spring of 2023. This slide, just to note some of the meeting and hearing dates.

November 10th, there was a stakeholder meeting that was addressing consumer rights and universal opt-out mechanism, which is an important issue that I believe Greg is going to go into more detail on. November 15th, there was another meeting that was addressing controller obligations and data protection assessments. Very recently, November 17th, another meeting that addressed profiling consent and definitions. And on February 1st of 2023, there'll be a formal rule making hearing. So, that brings me to the conclusion of my portion. I'm going to hand it off now to Greg to talk about an overview of the draft rules and some of the important takeaways. Greg.

Greg Szewczyk:

Thanks, Phil. One thing I just want to mention before we get started is Phil has just explained the Colorado Attorney General has made very clear that the office is interested in hearing comments. And, what we all expect is that that means that the regulations or the draft rules will be changing. So what we're going to do today is we're going to go over some of the more notable rules, some at a higher level, some at a little more detail. We're not going to provide a specific compliance plan for anything, but we're really going to try to highlight some areas where compliance will be different than California or some areas where the Attorney General has specifically asked businesses, consumer groups, and anybody else to comment. So, we'll dive right in. At a very high level, the Colorado privacy rules are 38 pages long.

That might seem like a lengthy set of rules and in some ways it is because they are very detailed. But the comparison is the red lined version of the CPRA rules that I believe 73 page at this point. So, there are a lot of information in these rules, but they are not necessarily out of what we've seen otherwise. There are 10 general rules with multiple subparts, general applicability, definitions, consumer disclosures, consumer rights, the interpersonal opt-out mechanism, controller duties, consent, data protection assessments, profiling, and accessibility. Although some of these are less controversial than others, as we go

through some of these rules today, I think that you can see a few different themes that come through on where the Attorney General's office is really focused, and in a lot of ways it tracks what we're seeing as a broader trend across regulatory actions and litigation right now.

And those areas are consumer consent and having meaningful consent, disclosures of seeing what is actually being done, especially on an analytical level and profiling. And you'll see that these rules bleed through and touch several different areas of it. In connection with the initial draft of the rules that was released, there was also a formal statement released by the Attorney general's office that, like I said, specifically requests input across the board, but the AG listed nine topics on which he felt that input would be particularly insightful. Now we'll highlight some of those as we go through, but I'd welcome everybody who watches this, take a look and see where those topics are and whether they affect either your businesses or your consumer advocacy group, how those impact what you see. And moving right into consumer personal data rights, which is rule four.

In many ways, the specific procedures laid out are not all that controversial. One thing we see with the Colorado rules is that where the Colorado Privacy Act itself already states what needs to be done, the rules don't restate that. Instead, they try to provide guidance on areas where the rules did not specifically lay out the method. One area where I think it is noteworthy is authenticating consumer requests. As many people watching this webcast will know the California model set by the CCPA and carried through for the CPRA is very prescriptive in what needs to be done as far as how requests are authenticated. The Colorado model takes a little different approach, and instead of having the very prescriptive model, it is much more of a standard based approach that just requires reasonable methods. It also provides some general guidance about avoiding requests and additional data and making sure that reasonable security measures are taken.

But really at a general point, this is more of a standards based rule that provides guidance that will likely change for different companies depending on what kinds of data they're having and how sensitive it is. And in some ways, this is a good thing. This will allow companies to tailor products that are more consumer friendly than some of the very specific ways that are done under California. But at the same time, it does allow for interoperability because those California ways will still be acceptable under Colorado. Another area that is worth highlighting is the response to consumer personal data rights. Under the draft Colorado rules, there is a focus that the response must be in an understandable form with the specific data at issue for requests for access to what personal data is held. Now, as any company that has gone through the process of providing a request to specific personal data under the specific pieces of personal information under the CCPA knows this may not be as easy as found.

If personal data is held in a few different databases that blows out some fairly complicated spreadsheets, it may arguably not be understandable and comply with this rule. Another noteworthy portion of the rules is that if a company does not respond to a consumer request, it still needs to provide a response explaining why it does not respond. And so, the one area to think of is for companies who are used to receiving consumer requests, if they've received some of the automated systems that send out blast purporting to exercise rights that are not compliant in most ways, there still arguably could be a need to respond to that to explain why the company's not respond. And then the final is notice to processors under the CPA rules, a controller that complies with a personal data right request, the controller also has to notify all processors that process that consumers personal data, of the consumers request and the controllers response.

So that something else that's going to need to be into any policies and procedures to ensure that that's happened. The last area about consumer personal data rights that I want to highlight is appeals. The rules are actually fairly slim on appeals, but the Attorney General specifically asked for comments on whether or not there should be more rules about appeals or rather if the provisions of the CPA are sufficient. So, regardless of whether it is a business in industry group or a consumer advocacy group, that's something that is very clearly still in play right now and companies should take a look and decide whether or not they think that this is something where they might want more rules. Moving on the universal opt-out mechanism, which is one of the more notable areas of the CPA. The universal opt-out mechanism rule is contained in rule five, and it has a few different components to it. So I'll start by saying with the California the CPRA itself, it could be interpreted as providing more of an opt-out signal that applies to online as opposed to a true universal opt-out mechanism.

This current draft is of the CPRA regulations operate more like a universal opt-out mechanism. So, we may be going into 2023, we may be going towards a world where it is more overlapping than it initially looks like, but what is clear is under the CPA there is express authority for this type of universal opt-out mechanism, that will include offline recognition, and maybe one of the most notable aspects is Colorado's rules contemplate a do not call type list. There's still a lot to be done on this area

on what the technical specifications will finally be on notice and timing, but one important thing to note is that while these issues are spelled out in the current draft of the rules, they also state that by April 1st of 2024, the attorney general will issue a list of recognize and approved universal opt-out mechanisms. So companies should be looking at these technical special specifications and paying attention, but they should also know that coming down the pipe will be a list of approved universal opt-out mechanisms that they will have to abide by.

We known to privacy policies, which might be one of the most notable areas where there is a difference from California. The Colorado rules follow a fundamentally different approach to California, and that's a purpose based approach requiring... And taking a step back onto the California rules, it's much more of an information based approach is anybody who has drafted or looked at CCPA and soon to be CPRA privacy policy knows, it is all tied off of the type of information that is collected. And so, there are several different categories that are defined by the CCPA, and all of the disclosures are tied to those categories of information regardless of whether they're being collected for multiple different purposes. Colorado's takes a different approach where it is tied to the purpose rather than just the type of information. And so for each purpose of collection, there will have to be disclosures relating to whether what types of personal data are collected for that purpose, whether or not those categories of personal data are sold or shared with third parties, and the categories of third parties with whom the controller sells or shares those categories of information.

And, if you want to hear a little more about why the Colorado Attorney General has adopted this approach, you can both look at that statement that's attached to the draft. And you can also go to an event that we hosted with the Attorney General back in September where he gave a little insight into this. And, part of the mindset is that if you share information, the same sets of information with a company in two different contexts, you could have very different expectations about how that information is going to be used. The example that I've seen talked about that I think makes a lot of sense is if you share your name and email address with a company for the purpose of signing up for a newsletter, you might have every expectation that they are going to market to you based on to based on the fact that you signed up for that newsletter and gave them your email address.

By contrast, if you provide a company with your name and email address because you are contacting them for customer service, say that you bought a product in a store and that you're having issues with it, you might not have a reasonable expectation that they're going to market you based on the fact that you sent in a customer service complaint. And so, consumers should get that disclosure to explain how their data's being used based on the context in which they provide it. This obviously could have some interoperability issues with California, but I can say as we have helped some clients start to prepare to comply with this, it has not been quite the difficult lift that it may look like at first because when you're running the data maps to figure out what information has been collected, and as you are going to some of the older formats of privacy policies that were conducted under KAAPA and the Delaware Privacy Law, and it was the format before the CCPA, it somewhat fits in with that format.

Another big area of the privacy policy is profiling disclosures. We'll talk about those a little more later, but there are some very specific disclosures required if there is profiling done. And then finally, and maybe one of the other big areas of the privacy changes to privacy policy are going to required consent for secondary use. And, as we'll see in a second, this is not simply the updating the privacy policy. If categories of information are going to be used for a secondary use beyond what the initial disclosure was, the company is going to need affirmative consent for that secondary use. So as to what consent entails, when it's required? It's required for the processing of sensitive data, which is part of the CPA. It is not something new for the rules, but it is worth highlighting again, because under this California model, it is an area where there is an opt-out, not an opt-in under the Colorado law, it is opt-in.

You also need opt-in consent to process the personal data of a known child. You need it after an opt-out has been exercised and then you need it when there is a secondary use as I just mentioned. I have a little asterisk next to the after opt-out because there are specific rules about how that consent can be obtained. It's something that may be changing. So we're not going to go into specific detail right now, but it is something that companies should go look at and see how it's going to impact their operations, because the types of methods of just potentially having a popup that asks for an opt-in may not be allowed under the Colorado. We'll see how they are, we'll see how they morph, but it's an area that companies should look and see how that is going to impact them and whether or not they're going to have to be operational changes within your platform. How consent must be obtained?

It must be a clear affirmative act, it cannot be implied consent. It must be freely given, it must be specific, it must be informed, it must be part of an unambiguous agreement. So what we're looking at here is it can't just be part of a continued use that is within the privacy policy or terms. There really does have to be affirmative specific consent, which leads into the dark pattern. Rule 7.09 of the Colorado rules goes into great detail about what constitutes a dark pattern. And, I would welcome everybody to check out our webcast that we did several months ago about dark patterns because this really does overlap a lot with what we discussed. But at a general level, there has to be a symmetrical choice. You can't have two different choices, one of which is much easier and one of which takes a lot more effort.

There can't be emotional manipulation. There is no implied consent with silences acceptance. There can't be default options that draw somebody to one conclusion over the other. And it can't have a different number of steps or confusion or a false sense of urgency. And then that one over on the left hand side in the middle I think is actually a very important one, is experience interruption. You can't obtain consent by interrupting the user's experience of the website. And so this is what we're getting into about popups to try to capture consent. It may not be permissible because it may be a dark pattern rendering the consent ineffective. One other thing that I think is worth mentioning about the dark patterns rule, and this is more of a global comment, not just related to Colorado. The dark patterns are obviously very important as to whether or not consent is effect, but that is really the only area where dark patterns come into play under the Colorado Privacy Act is whether or not consent is effective.

And although that's very important, it's also a fairly small component of the CPA, but the dark patterns rule is pretty lengthy. It is comprehensive and it provides a lot of information. This is similar to what we've seen under California, it's similar to what we've seen the attention of the FTC. And I think what all companies should be taking from this is that there is an increased focus on dark patterns, not just from a privacy law standpoint, but from a general consumer protection standpoint. Because although this is the Colorado Privacy Act rules, it is done by the Colorado Attorney General who has greater consumer protection authority. And if you do listen to our discussion with the Colorado AG from back in September, this is something that he gets into. So I'd welcome everybody to take a look at that and take this as an opportunity to do a true review of your platform or your website's interface to take a scan for dark patterns to see if there are broader issues beyond just privacy statutory compliance.

We've mentioned profiling a few times today. This is an area where the rules are detailed. There is a dedicated rule just to profiling at a high level you can see the four buckets of what is required on in profiling, and that is transparency and opt-out consent in some situations, and that it has to be specifically considered in data protection assessments beyond just what is already required, which we'll look at in a second. When it comes to transparency, if a company is profiling in a way that is going to have legal or other types of binding impacts on the consumer, and that is a broadly defined term that can include things like whether or not to make special offers to somebody based on the data you have in your possession or otherwise. There will have to be a dedicated section in the privacy policy discussing what the decision is that constitutes profiling, the data used, the logic used, why it's relevant, and then additional if that decision relates to housing, employment, finance or living.

The opt-out has a unique provision to it that is a little different where it treats three different types of profiling different. And the three types of profiling are solely automated and human reviewed in which the opt-out must be honored. However, if it is a human involved profiling decision, there is some discretion that with other disclosure obligations. With respect to consent, there are specific mechanisms and specific disclosures. That is another area where we may see things changing. But the takeaway right now is that companies need to be considering that if they are profiling, they're going to need to make sure that they're getting into this. And I'll turn right to the DPAs. The Data Protection Assessments are contained in rule eight, and this is an area where it is a first in the United States issue, just like the profiling. And I say that because under the current version of the California rules, they don't discuss data protection assessments or privacy risk assessments as they will likely call them.

And they don't discuss profiling yet. We widely expect to see that, but they're not in the current set. So these Colorado rules are really the first time for purely domestic companies, they're going to be seen. The Colorado DPA rule is fairly detailed. The good side of it for companies that are used to complying with GDPR is it's going to be within what they're used to seeing for DPIAs under the GDPR. And it's got specific requirements related to purpose and specific tasks, the necessity, benefits of risk, the names and categories of recipients, including third party processors, the expectations of the consumers safeguards and alternatives, and some other specific requirements to be in there. But if companies are used to using the ICO template, they're

largely going to be used to doing what's required under the Colorado books, or at least under the current version. The timing is a little more noteworthy.

It needs to be done before there is a commencement of certain types of processing. It needs to be done periodically, or if there is profiling involved, it needs to be done annually. And then the other is when there is a material change in the level of risk. And the current draft of the rules spells out specific things that may constitute a material change and level of risk. Now, we'll see if any of those change, but right now it includes some things that could trigger it on a fairly frequent basis, such as changing the processor that you're using. It won't necessarily, but it's important to make sure that whoever at a company is in charge of overseeing DPAs, is aware when processes are changed. And at least the way I read the current draft of the rule is that if you are changing from say, Salesforce to AWS as your processor for some types of data hosting, it wouldn't necessarily lead a complete review of your DPA.

But if you're switching from a Salesforce or AWS to a very small vendor that doesn't have the level of data security, it might require it. So it's something that companies need to make sure are built into their processes to make sure that it is getting on the right desk when certain decisions are being made. And another thing to make sure that everybody's aware is that these DPAs are going to be subject to attorney general requests. So, ensuring that they are done correctly, that they are done not just as a rote process that are siloed off from legal or compliance, but they need to have the eyes of legal and compliance on them to make sure that they are justifiable from a legal compliance stand. As Phil mentioned data minimization is a big part of the Colorado Privacy Act. It's also a big part of the rules.

I have the rule up here on the screen, not so much because it is drastically different from what we have seen in other contexts, but because I just want to highlight the growing importance of data minimization. As many companies will know, the FTC recently announced a settlement with Drizzly over the data breach that drizzly suffered a couple years ago. And while in many ways the data breach itself was nothing new, the settlement was in that there was a specific allegation that Drizzly failed to minimize the data as it was supposed to. Essentially, the thought that you can't lose what you don't have, and they should not have been maintaining this data as long as they did. And so, I just want to highlight how important the data minimization requirements are and the CPA and all the other 2023 laws, especially because it may come into play more in the context of data breach litigation and enforcement actions.

Loyalty programs are another area where the AG has specifically asked for comments. Under the current draft of Colorado, companies are allowed to offer bonafide loyalty programs, which is a defined term. They can discontinue the loyalty program after the right to delete, if it's impossible, and opt-outs can also impact the eligibility for the program. But if a company wants to take this route, it will need to include several specific disclosures in its privacy policy about what the loyalty program is, how it's using data, and other specific issues. I'm not going to get into all of the specific details now because again, this is an area where the AG has asked for guidance, but if you are a company that is using a loyalty program, you should assess how this is going to impact your loyalty program, how feasible the disclosures are, and if you think it may be worth submitting a comment as to what you might think would be a better revision to that.

So just a couple quick takeaways. One is what we've been saying for well over a year at this point, which is a data map and inventory is critical, not just of what data you have, but of what third party vendors you be using because it's going to be very difficult to comply with these rules, or the law, or the California law, or any of the other 2023 laws unless you know what you're actually doing. You're also going to need to assess operational impacts. Some of these issues in these rules such as secondary use or the various interfaces that you may use might be impacted. And it's going to need to be built into how you are collecting consent, or how you're making certain disclosures, or whether or not you're able to honor the universal opt-out request across everything. Also say, start developing policies to document compliance.

The rules may change over the next several months, but there are some core components that you can start building into policies now. And finally, what I've said a few times is submit a comment if the rules impact you in a way that you think could be better from everything we have said and as the Attorney General told us himself, he wants to hear from you, and they will take seriously. One last thing before we leave, as I just want to say, in addition to speaking in a blog in about cyber litigation, we've written a book on it. Cyber Litigation by Thompson Reuters, it covers a wide range of data breach, data privacy, digital rights litigation, on everything from retail data breach to online tracking to website accessibility. It's available at the URL listed on this slide, and I invite everybody to check it out just to say one last time. Thank you for joining us today, and we'll talk again next month.

Steve Burkhart:

Thanks again to Phil Yannella and Greg Szewczyk. Make sure to visit our website, www.bowerspa.com, where you can find the latest news and guidance from our attorneys. Subscribe to the show in Apple Podcast, Google Play, Spotify, or your favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.