Podcast Transcript

2022 DSIR Report Deeper Dive: The Expanding Landscape of State Data Privacy Laws

Date: October 5, 2022

Guest: Elise Elam, David Potter, **Host:** Amy Kattman

Run Time: 16:08

For questions and comments contact:

Elise Elam

Associate
Cincinnati
T: 1.513.929.3490 | eelam@bakerlaw.com

David Potter

Associate
Chicago
T: 1.312.416.6278 | dpotter@bakerlaw.com

Kattman: Ransomware, MFA, extortion, fraudulent fund transfer schemes. These topics and many others make up the key findings section of the 8th Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group, or DADM, provide statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets and frankly, anyone interested in or tasked with their company's digital asset and risks. I'm Amy Kattman, and you're listening to BakerHosts.

This, our ninth episode in this series exploring the 2022 DSIR report, is focused on the expanding landscape of state data privacy law. Our guests today are Elise Elam, an associate and member of our Digital Risk Advisory and Cyber Security team, and David Potter, also an associate and member of our Digital Risk Advisory and Cyber Security team. Welcome to the show, Elise and David.

Elam: Hi Amy, happy to be here today.

Potter: Thanks for having me, Amy.

Kattman: Elise, let's begin with you. Is the law in this area continuing to change regarding cyber security? And if so, what kinds of trends are you seeing year to year?

Elam: That is a great question, and the answer is yes. The legal landscape in cyber security and privacy is constantly in flux, and legislatures have continued to pass laws around these subjects generally. Between July of 2021 and May of 2022, four states, Colorado, Connecticut, Utah, and Virginia, enacted privacy acts that are very similar to the California Privacy Rights Act or the CPRA that took effect in December of 2020, and an additional five states, Massachusetts, Michigan, New Jersey, Ohio, and Pennsylvania, have similar bills pending in their respective legislatures.

Kattman: David, can you tell us what is different about the privacy acts being enacted over the past two to four years from the existing breach notification laws?

Potter: That is a good question also, Amy, and since the enactment of CCPA, the California Consumer Privacy Act, legislatures have been focused more so on enacting statutes that are focused on the consumer, and specifically the rights of consumers, obligations of processors and collectors, and how these rights and obligations are enforced. Generally speaking, the data breach notification laws that were enacted beginning in 2002 with California's statute were designed to create a notification obligation for entities that had experienced a data breach involving personal information. The last two states to enact such data breach notification statutes were Alabama and South Dakota, which both took effect in 2018.

The recent legislative trend since the enactment of CCPA, which continued in 2022, is enacting comprehensive data privacy statutes that really spell out the rights of consumers whose data is at stake and the obligations of entities that control or process that data. Consequently, the potential liability of entities that process or control data that includes personal information is increasing as states move to create different enforcement mechanisms as a means to encourage compliance and deter noncompliance. This changing landscape is hard for entities that deal with personal information as part of their business, and there are different thresholds under some of the statutes that exempt certain organizations in certain jurisdictions from compliance with these new requirements.

Kattman: Elise, can you tell us what types of entities are the new acts applicable to?

Elam: So, each of the new acts has a threshold that must be met for the act to apply to an organization, and it is important to understand the distinctions between the various states' laws. We'll start with Connecticut. The Connecticut Act applies to entities that conduct business in Connecticut and either process personal information of 100,000 or more Connecticut consumers, or process the personal

information of at least 25,000 Connecticut consumers and derive 25% of their revenue from selling personal data. I will note that conducting business in Connecticut is not a defined term under the statute, so it is not entirely clear the scope of what that would entail. It could be very broad, or it could be more narrow.

It is important to note, too, that this act won't apply to all organizations. Most entities are not engaged in the sale of personal data for profit and having the personal data of 100,000 Connecticut residents will likely restrict the applicability of this act to larger businesses operating in Connecticut. Some examples would be businesses in in the insurance industry, market research firms, and social media companies. Colorado and Virginia's laws are very similar to the Connecticut Act, have the same or similar applicability requirements.

The Utah Act, though, is a little bit different because it applies to businesses conducting business in Utah or that produce products or services that are targeted at Utah residents. It also has different thresholds that apply compared to the Colorado, Connecticut, and Virginia Acts. The Utah Act applies to entities with an annual revenue of $25 million or more and that annually control or process the personal data of at least 100,000 Utah residents or the controller process the personal data of at least 25,000 Utah residents and derived more than 50% of their gross revenue from the sale of personal data. So, that is a lot to unpack, but it emphasizes the point that it is important to understand the sort of nuances between all of these laws.

Kattman: Thanks, Elise. David, let's talk about how these organizations should address these new obligations, given that they continue to change and vary from state to state.

Potter: Sure, Amy. Fortunately, or unfortunately, depending on which side of the coin you're on, California since the very beginning and continues to be the innovation leader when it comes to data privacy protection and enforcement. Entities that have implemented processes and strategies to address the requirements under CCPA and CPRA will have a leg up on other organizations that were unaffected by those acts. Those are really the models for these new acts, and I think will continue to be the model for other states that enact similar comprehensive statutes. Organizations in the states that have enacted these new acts should pay attention to the requirements and the thresholds that Elise just went through that subject organizations to the acts and ensure they are in compliance with the requirements relevant to their organization. They should also develop internal processes to address the various requirements related to consumer rights.

Kattman: With these new acts, it seems we're really looking at consumer rights, entity obligations, exemptions, and enforcement mechanisms. Can you talk about what companies need to be aware of regarding these four areas? David, let's start with you.

Potter: Sure, Amy, we'll take these one at a time, and really the consumer rights is the big highlight here because like the California Act, these new laws give

consumers a right to confirm whether our business is processing their data, obtain a copy of the personal data being processed, correct any inaccuracies in that data, and also ask that their data be deleted. And the entity obligations really go in line with those consumer rights, and what entities are required to do is they're required to provide consumers with a privacy notice, maintain reasonable data security practices to protect the data, and in the case of Colorado, the act also requires entities to enter into specific data processing agreements with any entities that process data they control that includes consumer information.

In Connecticut, there is a separate requirement that entities must conduct assessments that weigh the benefits of processing the data against the risk of the rights of consumers, and also requires controllers to take reasonable measures to ensure that any deidentified data cannot be reassociated with an individual.

Kattman: Elise, do you want to talk a little bit about exemptions and enforcement?

Elam: Another thing to understand about these new privacy acts is that they all contain various exemptions that apply to different sorts of entities and activities, and these exemptions vary by state. However, all four of the statutes include exemptions for entities subject to HIPAA or to the Gramm-Leach-Bliley Act, or the GLPA, and there are also types of activities that are exempt, such as activities in the context of employment. The Colorado and Connecticut acts also exclude government entities, non-profit organizations, and higher educational institutions, so those privacy acts in those states would not apply to those types of organizations.

Another thing that is important for entities to understand as they prepare for these laws to be in place is the enforcement mechanisms that are built into these acts. Unlike the California acts, none of these new acts contain a private cause of action for consumers. What that means is that under the California act, a consumer whose rights under the privacy act have been violated can bring a lawsuit against the offending entity for a violation. However, in Colorado, Connecticut, Virginia, and Utah, that is not the case. Instead, those four acts are enforceable only by the attorneys general in that state.

In the case of Colorado, county level district attorney offices can also enforce the act. So, what that means is that only the government can enforce these acts against the entities to whom the acts apply, and it is important to understand the various penalties involved with each of these acts. They range from $7,500 up to $20,000 per violation, but it is important to understand what a violation is. A violation could be any time an individual is not provided with the proper notice about the processing of their data, or any time an individual is not provided with the information about them upon request, or each instance of a failure of a company to comply with some other aspect of these acts. Any single instance of that type of violation could be enforced as a separate and distinct violation. What that means effectively is that the penalty of $7,500 up to $20,000 per violation can be stacked on top of one another, and that can really add up quickly to a much larger penalty.

Kattman: David, as we wrap up today's program, let's talk about what is on the horizon. Are other states going to follow suit and will these laws ever be settled, or do you foresee more meddling from legislatures?

Potter: Amy, this trend from state legislatures opting for comprehensive acts that address the rights of consumers, responsibilities of entities processing and controlling personal information, and the means of enforcing them, is absolutely likely to continue. If the past is prologue, there will be a day when 50 states have their own comprehensive data privacy acts similar to CCPA and CPRA. Whether there will be further meddling from legislatures and the public regarding these types of privacy protections will depend on how effective the new acts are in changing the behavior of enterprises that control and process personal information. After 16 years of the original breach notification law in California, it is likely apparent to everyone that simply notifying individuals about data security incidents isn't adequate to effectively protect personal information.

The penalties being assessed are becoming more severe, the causes of action are expanding, and the obligations of entities that are subject to these acts are increasingly focused on strategies to actually prevent these types of incidents in the first place. That is the big take away, and where legislators are likely to go in the future, protecting personal information on the front end before an incident and penalizing entities that failed to take steps seen as reasonable by the public.

Kattman: Thank you for joining us, Elise and David.

Elam: Thanks for having me.

Potter: Thanks for having me, Amy.

Kattman: If you have any questions for Elise and David, their contact information is in the show notes. As always, thanks for listening to BakerHosts.