The Our American States podcast—produced by the National Conference of State Legislatures—is where you hear compelling conversations that tell the story of America's state legislatures, the people in them, the politics that compel them, and the important work of democracy.

You can subscribe through iTunes or Google Play.

The Latest in Online and Digital Privacy Laws | OAS Episode 67

Gene: Welcome to "Our American States," a podcast of meaningful conversations that tell the story of America's state legislatures, the people in them, the politics that compel them, and the important work of democracy. For the National Conference of State Legislatures, I'm your host, Gene Rose.

In this episode of "Our American States" we take a look at how state legislatures are addressing the topic of consumer and digital privacy. Later in the program we talk with Utah State Representative Craig Hall. He successfully guided legislation that was signed into law that requires search warrants for electronic documents, treating digital documents the same as printed ones.

We start off the program discussing what is considered landmark legislation in California that addresses online consumer privacy. The California Consumer Privacy Act of 2018 was signed into law last year, and we start out this episode with a conversation on proposed changes to the law in 2019.

We have returning to our program California Assemblymember Jacqui Irwin. Welcome back.

Jacqui: Thank you very much.

Gene: Last year the California State Legislature approved the California Consumer Privacy Act. It's considered a landmark bill, but I know you and some of your colleagues felt that changes need to be made. And let's talk about one of the bills that you've introduced to address this: AB 873, that addresses the definition of the types of personal information that are protected in the act.

Time Marker (TM): 1:36

Gene: Can you tell us what is meant by personal information and de-identified information in the current act, and how or why your bill would change that definition?

Jacqui: Certainly, and I will go a little bit into depth on this. I think everybody understands that when you're asking about the details of these bills, it's definitely complicated.

Gene: Right.

Jacqui: Hopefully we are getting to making sure that CCPA is workable and maintains consumer privacy. So personal information is what CCPA covers. It's a threshold question to see if the data you have as a business is subject to a right to transparency, disclosure, deletion, opting out of sale. And the way that the definition is currently in CCPA is all-encompassing and it uses a string of verbs that is quite broad, and it makes almost any data point personal information, and it's because of the phrase "capable of being associated."

So if you don't modify "capable," it's a future-looking exercise that almost ends with: Yes, everything is capable of being associated. That's a problem for people who are trying to exercise their rights under CCPA because when businesses are trying to honor your request, they have to try and associate data with you that they normally wouldn't, but have to do so, so that they can honor the request, let's say, to be deleted.

And so the first part of 873 is that we added "reasonably" before "capable" to reduce the lengths considered within a business' ability to associate data with a consumer. And what this basically does is bring the scope of personal information to a much more workable breadth while still covering vast amounts of truly consumer information.

The second part of the bill is talking about de-identified information, so that's personal information that's gone through some pro-privacy techniques of data processes and management to remove most of the identifiers, but still allow some association within the data to maintain our ability to gain insight.

The identified information in CCPA also comes with controls about its use to prevent it from being re-identified and the problem with CCPA, again, that passed last year with de-identified is that it doesn't describe data that's within the scope.

So my bill refocuses the definition on the Obama Administration's FCC guidance and that's where de-identified data can do many things, just not identify or be reasonably linkable to a consumer. And with this change businesses can be pro-privacy and de-identify their datasets and safeguard them against requests for deletion, but still be bound by CCPA's limitations on de-identified information like not attempting to re-identify.

So that is AB 873 and, like I said, it's probably pretty in the weeds.

TM: 4:34

Gene: Tell us what kind of reaction have you had to this bill so far; are people getting onboard?

Jacqui: Oh yes. So what we did very early on is we spoke to the author of the initiative. What happened in California was Alastair Mactaggart had funded an initiative that had qualified on the ballot and, of course, the problem is once it's passed, it's very difficult to amend it until you go back to the ballot.

So we spoke very early on about what we saw as some items that were inconsistent, might make CCPA unworkable, or actually had the opposite effect of what he was trying to do; like what I was describing before when if you don't add "reasonably" to "capable" in order to delete information, that you have to get much more information about the consumer. So it's sort of working in the opposite direction of what you wanted to do.

So because on both of these bills he was either in support or neutral on it, none of my colleagues in the assembly have had an issue with it.

TM: 5:33

Gene: So let's talk about another bill that you have, AB 874, that would change the definition of publicly available information to include any items that are lawfully made available from government public records. Why are you taking this change on?

Jacqui: Well, this is very important for many industries that rely on government records to provide services, so for instance, you know, realtors or any sort of business. Right now, the exemption only allows the business to use the government records in line with the reason that the government collected the information in the first place. So this is publicly available information, but we have to acknowledge that business uses and government uses for records are rarely the same and it makes this exemption useless.

So my bill deletes the requirement that the data be used for the same purpose and basically what we're addressing is we think a first amendment issue—people should be able to use information that the government already has publicly available regardless of the reason that the government collected it.

TM: 6:34

Gene: I'm sure you've heard the expression: There's no privacy without security. Do you think that the California Consumer Privacy Act will change security practices of businesses?

Jacqui: I'm not sure if CCPA is a motivational force for security. I think that the motivations have been around for a while. You know, businesses want to protect their IP, their ability to stay open, their marketplace reputation, and throughout the states and in California also, if you have a breach, it's very, very costly for businesses. So I think that they already have a pretty big motivation to make sure that they protect their data.

I think the biggest thing that we should be looking at, whether we're looking at CCPA or looking at cybersecurity, is making sure that we educate more people in tech, specifically more cybersecurity professionals. There are over 300,000 open cybersecurity jobs in the U.S. and especially here in California, we have a lot of businesses that are competing hard for these individuals. So, of course, that makes it very difficult for government to be able to hire what they need.

So it's really important that as legislators we focus on doing everything we can to expand the education for these professionals.

TM: 7:53

Gene: And there's also been considerable attention given to the large social media companies at the federal level in regard to consumer privacy. How do you think the nature of information collected by these firms may change in the future?

Jacqui: So with GDPR and CCPA and the other privacy bills being considered, we're going to see consumers engage with social media about privacy and what they feel comfortable sharing with them. I think it's about finding the right balance.

I can talk personally; I am very concerned when I see the amount of information that's being gathered by companies. They know where you've been and where you're shopping, and that is of great concern. At the same time there are a lot of conveniences that we gain when they have certain insight. So, for instance, I do like it if I am looking to buy a dress that I am given ads about dresses or suggestions about restaurants that are in the area.

So I think we've become very dependent or comfortable with the advantages of some of the information that technology companies are using to feed us the information we want. But I also think that we need to allow every consumer to decide: How much privacy do they want to give up to receive that information or to make their online experience better?

TM: 9:10

Gene: It makes me wonder what Europe has done. Do you see the United States going to that level of protecting privacy?

Jacqui: Right now, the latest information I've had about GDPR is that there are not that many companies completely complying with it and we have a lot of companies that are able to make investments, large companies that are able to make the investment, but certainly there from what we understand right now is that smaller companies are having issues with this.

I think that we all see privacy as a basic human right, but as I mentioned before, if we start to go down a direction where people are not getting what they're used to having fed to them information-wise or making their lives easier, I think that there's going to be some pushback. And we have heard that GDPR, some people think it has just really clogged things up.

TM: 10:04

Gene: Well, let's get back to the United States. We've seen several other states introduce comprehensive privacy bills similar to the California Consumer Privacy Act. Why do you think this issue is gaining traction in state legislatures this year and do you have any advice for your colleagues across the country looking at this issue?

Jacqui: I think a lot of it has been driven by what we're hearing in the media about the amount of information being collected. I'll just talk about one specific situation, which is the issue with the cellphone companies selling your geolocation data to, let's say, bounty hunters was a story in The New York Times, that these bounty hunters now have the ability real-time to track people.

And I think as people living here start to see those stories, we wonder if we've allowed too much information out without enough regulation. So it is the reason I think that the issue is gaining so much traction this year.

Personally, I think California leads on these issues and we really have an ability to export our work to other states. And so with CCPA, we have a lot of work to do to make sure that it is completely workable and that we've gotten rid of what the inconsistencies are, and part of that is driven by what I mentioned before, that we were given the choice between an imperfect bill that we could fix, or a ballot measure.

And so we chose the path to give us time over the next year to look at: What are the fixes that might be needed? And hopefully other states are looking closely at the things that we're fixing. I think it's really important that we all align the bills as closely as possible to CCPA, the other states also, because the big concern for us has always been that there could be federal preemption if it turns out that it's become a complete patchwork of different laws in different states. Then you have an opt-in or an opt-out. If you have no consistency at all, then it makes it much more likely that industries will call on Congress to preempt all of us.

We had, and I think I might have spoken to you about the bill we had last year, which was an Internet of things bill, and we worked with industry to get a bill to basically look at making sure that every Internet of things device had basic security procedures, so making sure that, for instance, you have to change the password.

It was a very collaborative bill and when I went to my cybersecurity NCSL meeting I presented the bill and everybody around the room was saying: Hey, can we copy the language? And you see that same type of language in a lot of other bills throughout the states this year.

But I think that that's really a better way to go than having a big patchwork of bills that are completely inconsistent and then allowing the federal government to come up with something that might not have the same type of privacy measures that we think are important.

Gene: We've been talking with California Assembly Member, Jacqui Irwin. Assembly member, thank you for letting us know about how your state is addressing consumer privacy.

Jacqui: I certainly appreciate the opportunity. Thank you so much, Gene.

Gene: Right after this short break we will talk with Utah State Representative Craig Hall about the Electronic Information or Data Privacy Act signed into law this year.

MUSIC & Female VO

Gene: We're talking with Representative Craig Hall from Utah who has passed what is considered to be the first law in the nation for a state to have a digital privacy law. Representative Hall, welcome to the program.

Craig: Yeah, thanks for having me, Gene. I appreciate it.

TM: 14:14

Gene: So tell us about this law which again, we assume, is the first in the nation. What are you hoping to accomplish with it?

Craig: So traditionally our current laws have done a decent job of protecting our physical communications and our physical data, our physical papers. But of course, now we live in a time where such a high percentage of our communication and information is in electronic form.

I noticed that the state of Missouri, they passed a change in their state constitution, which would protect electronic data and electronic information and put that specific provision within their state constitution. And that bill passed the Missouri legislature; it went to the voters; it passed the voters. So that is actually now within the state constitution in Missouri.

So back in 2018 during the legislative session here in Utah, I tried to do the exact same thing that they did in Missouri, which is to change the state constitution. Our Utah state constitution, like many other state constitutions, it has a provision where it says, and I'm paraphrasing here, that the right of the people to be secure in their persons, houses and papers and effects against unreasonable searches and seizures shall not be violated without a warrant. If you want that information, law enforcement needs to get a warrant.

So I tried to add electronic data and communications into our state constitution. I ran up against some opposition in that respect, particularly from law enforcement, and we ended the 2018 session without being able to pass a change to the state constitution. And law enforcement, during that process, they actually suggested: hey, we may be able to do the exact same thing by statute.

And so that's what we decided to do in 2019 was make this change by statute. So very simply, the law has not kept pace with new technology and, as a result, state and federal governments, they claim broad authority to track people's movements or purchases or reading habits, and sometimes even private conversations and data, all without a warrant.

So our correspondence and other quote/unquote papers – they don't become less sensitive simply because we store them in electronic form. So what we started with was it's very clear, for example, if I sit down with my laptop and write a document, draft a document and store it on my hard drive, if law enforcement wants that document that's stored on my hard drive, it's very clear that they need to go ahead and get a warrant. Right?

But it becomes less clear if I sit down at my laptop and happen to save the document in the Cloud with Dropbox or Google Drive, and the reason it becomes less clear is because of the third-party doctrine. There is lots of case law out there that says hey, if an individual voluntarily transmits information to a third party, they lose their privacy rights in that document because you transmit it to a third party.

So what this bill did is make sure that all of the protections that we have in the paper world, we continue to have those protections in the electronic world.

TM: 17:56

Gene: And you mentioned law enforcement, that they actually have been supportive of this measure?

Craig: It took a while to get to the point where law enforcement was fine with the 2019 bill. And actually, I think we had five substitute bills before we actually passed the bill. We did a good job of starting early in the session, so we had enough time; our legislative session here in Utah is 45 days and then after the 45 days were done.

So we were lucky that we started early in the session. We had enough time to make revision after revision after revision, and we finally struck I think the right balance where we provide sufficient protections and still allow law enforcement to do what they need to do.

TM: 18:44

Gene: And as I was researching this, this also follows a Supreme Court decision*, Carpenter vs. the United States*. Can you talk about the relationship between this bill and that decision?

Craig: Again, going back to the third-party doctrine, back in the '70s the Supreme Court issued a pair of decisions; this was *U.S. vs. Miller, Smith vs. Maryland*—they said hey, these documents, these records … and in those two cases I believe it was bank records and phone numbers, dialed phone numbers … In both of those cases the court ruled that defendants' Fourth Amendment rights were not violated because they didn't have a quote "legitimate" expectation of privacy since they had voluntarily given up their information to the third parties.

So this third-party doctrine really opened up a massive loophole that bypasses the Fourth Amendment and lets the government collect reams of very personal information. So last year the U.S. Supreme Court, they narrowed the third-party doctrine in *Carpenter*—it was a 5-4 decision. This case dealt with cell site location information.

Justice Roberts was the individual who authored the opinion and basically said that a person doesn't surrender all of his Fourth Amendment protections by venturing into the public sphere. So they stated that when the government tracks the location of a cellphone, it achieves perfect surveillance of an individual, just as if it had attached an ankle monitor to the phone's user.

So Roberts acknowledged that this third-party doctrine, the court tried to really narrow the decision to sell phone location information, but the Supreme Court acknowledged that look, you cannot use that information without getting a warrant. And so what we did in this bill is we basically codified the holding in the *Carpenter* case and tinkered with some of the language in order to get all of the stakeholders involved.

One of the great things about the process of this bill was I received really good help from two different groups. One was a Libertarian organization here in Utah called Libertas. And then the other group that I received a lot of help and support from was the ACLU of Utah.

And so when I had both of those groups working on the bill together, we were able to come up with great language, we were able to come up with language that law enforcement was okay with, and after five versions of the bill, we finally got the bill in a place where we were able to get it passed.

This is really a first-in-the-nation type of bill and it really takes into account this third-party doctrine and what happens to information when it's transmitted to third parties. We're not saying that law enforcement can't use that information; what we're saying is hey, if you want to obtain and use the information, then just go ahead and get a warrant.

TM: 22:00

Gene: And have you had public reaction to this? Does the public understand what was at stake here?

Craig: Just like any other bill, it takes a little bit of time for the public to understand exactly what was passed. But we really have had good reception of this bill, particularly because we spent a lot of time working with the groups that were really concerned about liberty interests, both on the left and the right, and also we worked a lot with the attorney general's office, with the county attorneys in order to get the bill to a place where they were fine with the bill as well.

So remarkably, after all of that work, we got the bill to a place where it passed unanimously both in the House and in the Senate. So to answer your question: yes, we have had really good public perception on this bill and, of course, the public, any time that their information receives more privacy protection, they generally support that idea.

TM: 23:02

Gene: What haven't I asked you about this bill and what would you like to tell other state legislators across the country if they're considering such legislation?

Craig: Yeah, I think that it's a fantastic idea. You know, one thing we were concerned about was: What would be the reaction of the technology companies? And frankly, it does not affect the technology companies all that much. It doesn't put an additional burden on the technology companies and because the technology companies mostly stayed out of this fight, that was helpful.

And this issue, case law does not do a great job of keeping up with technology. And one statement—this is from Justice Alito—Justice Alito wrote this statement in 2014 in *the Riley vs. California* case, and this is kind of the theme of this particular bill and what was the motive of this bill. He said: In light of these developments … and he's talking about whether law enforcement can get to a phone and look at the contents of a phone, he said: In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment.

And then he goes on to say: Legislatures elected by the people are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.

So this is a perfect place for the legislatures throughout the country to go, is look at the code that you have in your states: Has it kept up with technology? Does it provide the same protections in the electronic and digital world that you have in the paper world? Are documents that are saved in the cloud, do they have the same protection as documents that are saved on

your hard drive? And sometimes the answer to that is no, and sometimes it's ambiguous, leaving this interpretation up to the state and federal courts.

So this is a fantastic direction. We have gone through so many revisions of this bill. We feel like we have struck a great balance. Really appreciate the good work of the Libertarian group that helped us out and the ACLU of Utah that helped us out, and also really big props to law enforcement that pushed back, but pushed back appropriately so that we could strike a great balance between making sure that we keep these liberty interests, keep these privacy interests, and also allow law enforcement to do what they need to do in order to help keep us safe.

Gene: We've been talking with Utah State Representative Craig Hall on his digital privacy legislation. Representative Hall, thank you for being on "Our American States."

Craig: Yeah, thanks for having me. Appreciate it.

Music and Gene VO:

And that concludes this episode of "Our American States." We invite you to subscribe to this podcast on iTunes and Google Play. Please rate our podcast or leave a review. Until our next episode, this is Gene Rose for the National Conference of State Legislatures. Thanks for listening.