# EXHIBIT 6

SUPPORT →

GET A DEMO CONTACT US

ARCHIVE360

PLATFORM

SOLUTIONS

CUSTOMERS

RESOURCES

Never miss an episode

SUBSCRIBE NOW

Email*

**Subscribe**

By: Bill Tolson | September 7, 2022

Data Privacy | Regulatory Compliance | Data archiving | Information Management | Information Security | Information Governance | data security


## Description:

In this episode, Bill Tolson and Jane Bambauer, Professor of Law at the University of Arizona and one of the authors of the Universal Data Protection Act, discuss the drafting of a universal data privacy law that could be adopted by all states. The discussion takes a hind-sight look at GDPR, and lessons learned from the EU Privacy Regulations.


## Cyber Risk and Data Privacy Panel Discussion

Adjust cybersecurity strategies in the face of a new threat landscape. Experts in this panel discussion will cover Cloud Adoption, Data Security, and Ransomware.

Watch the Replay

## Jane Bambauer

Prof. Bambauer teaches and studies the fundamental problems of well-intended technology policies. Prof. Bambauer's research assesses the social costs and benefits of Big Data, and how new information technologies affect free speech, privacy, and competitive markets. Bambauer's work has been featured in over 20 scholarly publications including the Stanford Law Review, the Michigan Law Review, the California Law Review, and the Journal of Empirical Legal Studies. Her work has also been featured in media outlets including the Washington Post, the New York Times, Fox News, and Lawfare.

## Bill Tolson

Bill is the Vice President of Global Compliance for Archive360. Bill brings more than 29 years of experience with multinational corporations and technology start-ups, including 19-plus years in the archiving, information governance, and eDiscovery markets. Bill is a frequent speaker at legal and information governance industry events and has authored numerous eBooks, articles and blogs.

## Transcript

Bill Tolson:

Welcome to Archive 360's Information Management 360 Podcast. This week's episode is titled A Daily Privacy Discussion with Jane Bambauer. My name is Bill Tolson, and I'm the Vice President of Compliance and E-Discovery at Archive360. Joining me today is Jane Bambauer, a professor of law at the University of Arizona, and one of the authors of the Uniform Law Commissions Model Privacy Law, the Uniform Personal Data Protection Act. Jane, thanks again for taking the time to join me on our podcast today to discuss this really interesting ongoing topic about data privacy. We really very much appreciate it.

Jane Bambauer:

It's my pleasure. Great to be here.

Bill Tolson:

All right, well, let's get into it. Ever since the passage of the EU GDPR Data Privacy Law, several years ago, many countries around the globe have passed data privacy laws to protect their citizens from personally identifiable information or PII theft and misuse by companies as well as individuals. Additionally, in the last several years, several individual US states, after waiting for our federal government to get their act together, have begun to pass their own data privacy laws. The first being California CCPA, and then the follow on CPRA. In the first quarter of this year, there were approximately 27 privacy bills introduced in state legislators. Most did not make it into law, but so far two have. Both Utah and Connecticut passed data privacy laws. To date, there are five states with data privacy laws, California, Virginia, Connecticut, Utah, and my state Colorado, with obviously I think more to follow over the next year or two.

Bill Tolson:

In 2001, the Uniform Law Commission introduced their model privacy law called the Uniform Personal Data Protection Act. As I said in the opening, Jane was one of the authors of that model law. Jane, some questions around this, and I think it's really interesting, and I've actually read through the law and clients data a couple more times, but Jane, you're a law professor at the University of Arizona. How are you connected to the Uniform Law Commission and can you explain who the Uniform Law Commission is and what they do?

Jane Bambauer:

Yes. The Uniform Law Commission is probably best known for acts like the UCC code. What it does is it promulgates drafts of laws that are appropriate for state law consideration and then helps [illegible] laws enacted across as many states as possible so that there's uniformity across the states. To facilitate that process, the governor of each state actually selects some representatives who sit in the

Uniform Law Commission. Commissioners is what they're called, and these commissioners are put on different committees that are looking at gaps in the law that at least potentially should be filled in the state codes. And if it looks like yes, the Uniform Law Commission can add something of value, then they go ahead and put together a drafting committee. And the drafting committee is made up of commissioners. It also includes observers who are basically stakeholders who are going to have a kind of direct or indirect and significant impact based on the law that's been created, crafted, and then they recruit a reporter.

Jane Bambauer:

So the reporter is a subject matter expert, often a law professor, but not always, who helps author the bill. And so part of it is that as a subject matter expert, you're more likely to be on top of the terminology that is consistent with the field in general. But the other advantage to having a reporter come from outside the commission is that they can select somebody who has some depth of expertise or experience in the area, even if the commissioners themselves don't. I was not actually the first reporter on this act, but I was brought in about in the middle and while they were doing a major restructuring. And so I am familiar with this bill inside out, and I mostly, almost entirely **agree** with its approach, which is nice because I'm always happy to explain what the commissioners decided on. But I think with this bill I can not only explain, but I can justify the approach that they took.

Bill Tolson:

That's actually really interesting. Tell me if I'm misinterpreting this, but is the base thought for the Uniform Law Commission to create kind of laws around what the commission sees across the states that would be a law that hopefully all the states would adopt so that the law would not be different from state to state to state. One of the things that I, in dealing with the various state senators and representatives that we've had on the podcast about their bills from Colorado, Utah, Virginia, and so forth, is they follow to a certain extent each other's laws, but then they change it or add additional stuff to it. What that means is for businesses that are trying to follow it, it's not like you can pick a high watermark law and say, well, if I meet California's, then I meet the rest of them.

Bill Tolson:

And I would think with the Uniform Law Commission, the goal would be to have the same law across all the states so that number one, everybody knows it. There's no differences from state to state to state, no different definitions or exemptions or anything like that that really will complicate matters. Am I off base on that?

Jane Bambauer:

You're not, but I'll tell you they have two goals. And the first one is making a good law, and the second one is uniformity. So I'll tell you how we wound up, I'm sure as we talk more, your audience will

learn that the Uniform Law Commissions model bill, I'd call it overall a lower standard for what companies need to do than what is required under California's or say Colorado's law. And there are substantive reasons for that that we'll talk about. However, we have not abandoned uniformity.

Jane Bambauer:

The way that we've achieved uniformity is that any state that would pass the Personal Data Protection Act would have a provision of that act that makes clear that compliance with any state law that is at least as protective as the Uniform Commission's Law would automatically be in compliance with our law. We can't solve, of course, the Uniform Law Commission can't solve the fact that, say, Colorado and California already have two mutually incompatible laws on the books. We can't solve that as the commission. But what we can do is make it no worse. So any state that adopts our law would be as consistent as possible with other states if a company finds that it needs to comply with a higher standard in another state.

Bill Tolson:

Sure, that's a great strategy and way to look at it. I've talked to numerous businesses, corporations, both in the EU as well as in the United States, and obviously, well not obviously, but one of the things they always worried about is in the United States, for example, in four years, are there going to be 50 or 51 state laws that all slightly differ or will there be one, whether it be the federal law that we can talk about later, or the Uniform Law Commissions Model law. Obviously, the business people want one law to follow. It will make their lives much easier. And I think it would probably make compliance of an overall data privacy law much more manageable and probably less costly because I can imagine, I don't know if you've run across this, but in talking to businesses, they're afraid that they're going to have to hire just massive teams, either of people internally or up their law firm spend just to keep track of all of these things.

Bill Tolson:

And you can imagine that as a company, say Archive360 is collecting personal information because we give access to white papers or things like that, and we ask them for their email address and name and some basic stuff like that. Based on the definitions and exemptions and all kinds of things, each one of those data subjects PII is going to need to be tracked with basically active management with real time metadata around it and everything because the company with a right to deletion request or something like that, they're going to need to know based on where this custodian lives, what their timeframe is in responding and what kind of PII do they need to delete, only the data collected directly from the custodian, or any publicly available information the company might have scraped from websites. Two years ago, I was introduced to the Uniform Law Commission. I started looking and I thought, this is a fantastic idea to really simplify but get those laws in place. So I've bee proponent of the whole kind of theory behind the Uniform Law Commission.

Jane Bambauer:

Yeah, I think on the substance it's clearly the best. And so the problem that it has, I think, is the political landscape we're in. But going back to this compliance idea for a second, I think when consumer protection groups hear that businesses are complaining about compliance costs, they tend to kind of trivialize it or minimize it. But these are serious. I mean, the things you describe are really serious costs that wind up, of course, eventually affecting consumers. I mean, to give you a sense, because the GDPR has been in place for longer than any of the state laws, we now have some pretty good data on the cost of compliance there. And we know that the 500 largest firms have spent billions of dollars. That's not an exaggeration. They have spent billions of dollars to prepare for compliance, and the smaller firms simply can't do it.

Jane Bambauer:

So the EU, in fact, I'd say this is true, even before GDPR, when they were under their earlier data protection regime, they've always adopted a sort of law that sounds maximally protective but is actually impossible to comply with. And I think there's a danger that politically that's the expedient thing to do, is to pass a law that's not actually possible to enforce. The other point I'll make is there's also good evidence that GDPR has had negative effects on startup companies and competition in general.

Jane Bambauer:

So there's an eagerness right now to simultaneously be very strong on privacy rights in the United States and also to be very strong on sort of antitrust and pro competition law affecting big tech. But they're not a resolvable function, but they are, at least at the popular privacy laws, the GDPR style laws really do have an anti-competitive effect. Google will be able to comply and smaller firms will. So that was on the commissioner's mind. These are I think, considerations that really do have consumers interests at heart that tilt toward a more pragmatic approach. And so this is the pragmatic alternative.

Bill Tolson:

That makes a lot of sense. And as I've talked to the state senators and to organizations that worked with the state representatives to build along, there's always outside help from corporations and stuff. I don't think they take like you and the law commission does, they don't take the big picture into their thinking. And I constantly remind people this, but these privacy laws, GDPR, Canada's PIPEDA and their new one, C-27, if it makes it through, our federal one, all of the state ones, they're all global in nature. They come up with these, I don't want to describe this wrongly, not weird, but in some cases, complex requirements that they don't take into effect that there could be 30, 40, 50 other state laws that have their own complexities. And then you're looking at companies in the EU that might be collecting on me here in Colorado. And in reality, they're under the requirement to meet Colorado law, correct?

Jane Bambauer:

Yeah, right.

Jane Bambauer:

Almost nobody understands that who's not submerged in this topic, but the state senators just don't take that into account. They're working in their own little domain there. You mentioned GDPR. Now I actually have some interesting data, and one of the things I'm writing about now is this idea about data subject access requests. Bill Tolson can fill out a form or send an email to Archive 360 and say, Well, what data do you have on me? How are you using it? Are you using artificial intelligence with it? And oh, by the way, I want you to delete all of it.

Jane Bambauer:

Now those DSARs, I'm kind of future casting now are going to be one of the biggest costliest issues that organization has in the next several years because of the amount of new spending companies are going to have to do just to be able to meet those timeframes. It has to be responded to in 30 days or 45 days. You need to be able to find all the information. In fact, a couple of very large market analyst firms looking back in the EU in 2021 a little bit for the California but is almost all EU. They determined that, and at the end of 2020, the average company in the EU was receiving 147 DSARs per month and each DSAR was costing the company $1400 to respond to equaling about 200 grand per month.

Jane Bambauer:

The interesting thing is you're focusing on the cost of the company, which is significant, but we can also look at it the other way that we have this enormous legal apparatus because in theory, the consumers are demanding a right to access and delete their data, but in fact, those rights are not exercised all that often.

Bill Tolson:

Oh, absolutely. Part of my point is that was just a smaller number. What happens if the world in the near term or in the next couple years is educated on their rights and there are 50 state laws and then you have the other 145, 150 country laws, all of a sudden the burden, and I'm not thinking that companies are the oppressed here, but the burden on companies of tracking all of these laws responding to all the... I mean, you could be getting thousands of DSARs per month. And then the other thing that I'm starting look at is if the idea of a DSAR is weaponized by groups. Gee, I want to cause IBM a lot of issues, so I'm going to start putting all kinds of DSARs in. And even going further, what if the AI and ransomware starts to generate these DSARs automatically and starts hitting a com with those things, they won't know which ones are right and which ones are legal and which o aren't.

Jane Bambauer:

So let me tell you, we thought about this somewhat at the Uniform Law Commission. We do have the structure of our law for those who are not familiar with it, does match to some extent what the kind of global trend is. And so we did incorporate a limited right to access and correct personal data, but because of exactly the problems that you're describing, we limited that access right to only a subset of the data controllers. And those are the controllers who already have basically a credentialing process system with the data subject. And so even though we recognize it doesn't give you a complete view of where your data is throughout the entire ecosystem, it does though allow you, anytime you have a direct relationship with a company, you can ask that company to identify what data they have, who they've shared it with.

Jane Bambauer:

And so that solves some of the security problems that you're describing unless there's a hack where a bunch of passwords are used and exploited for this attack, it just makes it a lot harder to attack the system. It makes it harder for someone to impersonate someone else to get their data. It has some security built in.

Bill Tolson:

Yeah, I'm probably could be termed as paranoid by even thinking of this stuff, but I've been following the whole ransomware extortionware techniques and technologies and stuff. And I can imagine sometime in the near future extortionware actually getting into a system through phishing or something like that and finding those repositories where all of the PII is kept potentially if it's not encrypted and it should be encrypted, but a lot of it isn't. And then using that data to start generating SDARs to throw against the company. I know I'm reaching out on a limb here, but it's interesting to potentially kind of model and then maybe write about. Are we going to get to that point? No, but I think the idea of companies being somewhat overwhelmed with these SDARs I think is probably going to show up in the near term. And like you said, your model law really took that into account. And the others that I've talked to never thought of that. I think that's great that you took that into account.

Jane Bambauer:

Thank you. That's good. So the other thing by the way, although we did recognize again a limited right to access and correction, we did not adopt the right to deletion. So I could explain that logic if you think that's...

Bill Tolson:

Yes, please. That is really interesting because all the other bills as well as laws that I looked a obviously have the GDPR is the right to be forgotten, the right to erasure, but the right to delete PII if it

doesn't need to be held because of regulatory or litigation. But yes, please.

Jane Bambauer:

The reason we did not incorporate a right to deletion, there are two explanations. One is that the theory of the protections that we used in the model law is not one of absolute control by the data subject. There's more mutuality. So we're looking for types of uses of data, including disclosures of data that either could be risky or could be beneficial. And we're trying to preserve the sorts of data usage, data practices that are beneficial. We call it a compatible data practice. So we're allowing a company to continue to do compatible data practices without the consent of the data subject, as long as it's either totally consistent with the relationship that they have with the data subject already or is in the clear best interest of the data subject. And those are separate. They're overlapping, but not exactly identical. At the same time, we also recognize some prohibited data practices.

Jane Bambauer:

And so these are data practices that are so risky that we don't think that a company should do them even if they have consent. One problem with the kind of property approach or the control approach is that when you vest control in the data subject and they're just not sure of the downstream risks and benefits, they might withhold the data when they could instead get a benefit. But the other problem is that they might release the data when it is in fact not in their best interest and is likely to harm them. So we have compatible data practices that can keep going, prohibited data practices that can't be done no matter what, and then a middle category that does require some form of consent, either opt in or opt out, depending on the sensitivity level of the data. So I wanted to explain all that because that's kind of the heart of the kind of competing interest between a business and its customers.

Jane Bambauer:

And it explains why we don't want deletion. The whole idea is we're trying to preserve that there are these unexpected but very useful and valuable future repurposing of data that we don't want to cut off prematurely. And also at the same time, we don't want to put this burden, this probably an excessive burden on data subjects to go out and opt out of everything that might be risky. And so instead we go back to a kind of more traditional torts approach where we're looking at risk and saying you just can't do unjustified risk.

Jane Bambauer:

The second reason though, that at least a subset of the commissioners thought that a right to data deletion is not appropriate in the United States is because of a clash with the First Amendment. And this is something that I have not seen discussed enough and with enough rigor when we are talking about whether it's the federal data privacy bill that's being considered or will be probably taken up again next term, or whether it's say California's law, we have at this point Supreme Court precedent that

pretty strongly suggests that, I mean it definitely says that even dry data that's just like a database of personal information even that is considered speech.

Jane Bambauer:

And so you can regulate it, but you have to do so within the constraints of free speech scrutiny. And I think some of these privacy bills, most of them would probably be analyzed under intermediate scrutiny. We don't need to get into the weeds here, but one of my main research areas is on this clash between privacy and free speech. So I could probably go into too much stuff on this, but the point is that courts will have to look at whether there is a tailoring of the law toward a real and concrete harm. And so a right to deletion irrespective of any possible risk or damage to the customer seems to me not even likely to pass intermediate scrutiny. The idea was, well, good policy anyways doesn't require deletion because in fact we might want a startup company to do something novel with data that's helpful or we might want it to be obvious and clear that businesses can retain records that need to be kept for legal or public policy reasons. All of that, they're good policy reasons, but also why court a conflict with the First Amendment?

Bill Tolson:

I've never heard this put the way you just did around it's potentially a freedom of speech argument that PII that's been collected by company A, if they've collected it, they have a right to use it, not misuse it. And that's where you get into deletion. But first I talked to Senator Kevin Thomas in New York who has authored several privacy bills and one of his privacy bills from two years ago, none of them had been passed yet in New York, but one of his privacy bills specifically called out this idea that the data collector had to act as a data fiduciary. And that obviously, was one of the sticking points and probably one of the reasons why it did make it into law in 2021. But I've heard others kind of renamed that. In fact, I think it's even sort of adopted in the federal bill right now.

Jane Bambauer:

Loyalty.

Bill Tolson:

Duty of loyalty or duty of loyalty and care. And I think that's really interesting concept. I would imagine that companies having to figure out if I'm going to use this PI in a certain way, is it beneficial to the data subject or not? I mean you're going to get in some, I think a lot of probably lawsuits over that. I thought it was in talking to the senator, he was very passionate about it. And I thought it was a really interesting concept about that. But you mentioned, you don't include the right to delete, which I understand and I think that's really interesting. Like the other data privacy laws that are out th PR and the various five states and all kinds of stuff, is there a series of basic rights that the comm s

model law does include like the right to query as to what kind of information that somebody might be holding on you, that kind of stuff, and what are those basic rights?

Jane Bambauer:

The basic rights are a right to access, a right to a copy of your data. Again, as I mentioned before, it's a right that applies to data controllers that already have a relationship with you so that they can verify easily that it's you. The right to correction through the same channels is also included. There's a right to notice. So very much in the style of California law, we included a requirement that there's a publicly available privacy policy that describes not only who would have access to the data to the extent that it's shared with business partners or whatnot, but also the compatible data practices that the company expects to make use of.

Jane Bambauer:

In that way, if there is a challenge over whether a data practice really should be considered compatible, there's clarity for watchdog organizations to see what companies are doing. There's a right also to data security, which we can talk about. There's a requirement to do kind of like a privacy risk assessment. I mean, it is a privacy risk assessment, but our law is a little different because a lot of the laws that incorporate this, it has to be a kind of public document or at least discoverable. And we worried that it would wind up becoming a not very serious kind of CYA.

Jane Bambauer:

We require an assessment, but we designed it to be non discoverable. So the fact that you did it needs to be verifiable. But what it is, we wanted candor, we wanted a real self-reflection exercise.

Bill Tolson:

I think that's really an interesting point because impact assessment or a privacy impact assessment or whatever the various names I've seen it called could actually contain competitive information that on companies competitors might like to get their hands on. So you're potentially putting a company at a disadvantage by making that a public document versus discoverable if beginning the litigation. But if you're doing it now, I think some of the laws say it has to be done on an annual basis, but having done it but then you use it with your customers or your potential customers to prove that you're up to speed and all that kind of stuff, I think is an interesting way to look at it. And I've looked at all of these all the way through GDPR and all the rest, and I never thought, geez, this might be a competitive disadvantage for a company to have that out there. Not that you shouldn't do it.

Jane Bambauer:

Right, exactly. And then also it's the sort of thing where a company might be aware of a risk but wouldn't want to commit it to paper because then there's proof of knowledge. But otherwise the privacy rights are protected through this idea of compatible versus incompatible versus prohibited data practices. So everything else that's done with data is going to be categorized into one of those three categories. And so either you just can't do it, period, you can do it and you don't need to go through the cumbersome process of consenting, or the middle category which is I think the boundaries between the middle category and the compatible category is probably going to be the most contested.

Jane Bambauer:

And by the way, for that reason, another thing we did that is somewhat unique, although the federal bill has incorporated something very similar now, we with the help of some very important observers who were part of our process, we incorporated what we called a voluntary consensus standard where industry and members and stakeholders can get together and can basically propose some kind of clear guidelines that if the state attorney general agrees is consistent with the privacy law, the state privacy law, then those compliance with the guidelines is the same as compliance with the law.

Bill Tolson:

Oh. Wow.

Jane Bambauer:

So that it allows a company to go ahead and sort of get pre-verification that what they're going to do is not going to put them at risk of liability.

Bill Tolson:

Yeah, that's actually pretty neat. I like that idea. You probably have gotten the question before, but so far the model privacy law hasn't been adopted by any states. Why do you think that is?

Jane Bambauer:

Yeah, this gets back to the political comments I made earlier. I think the easiest thing that the Uniform Law Commission could have done is just basically write up something that looks very similar to California's law, and then have it get adopted with maybe minor tweaks in a lot of states and then claim victory. So I am glad though they didn't do that. I mean probably I would not have been the right reporter if that's the route that we wanted to go. They didn't do that because I think they thought of this as a longer term exercise that the privacy bills that are politically popular right now are not actually workable.

Jane Bambauer:

We're going to see that play out. We're starting to see it in Europe I think already. We're going to see that. And it could be that what is politically kind of a bill like this one that looks superficially like it's too wimpy will turn out to have a lot of virtues because it actually identifies the worst harms and has a practical approach to limiting them, but is not so costly and so kind of impossible to enforce that it winds up being kind of a kabuki theater sort of.

Bill Tolson:

Well, I think the way you just explained that, the commission looked at it as what would get the point across, what would get the main focus done, but also be workable. And I think a lot of the state people that I've talked to, they're responding to obviously political interests to shut this business down, and nobody should have my information and all this other kind of stuff, but they all want free apps and things like that. But to think about it from that point of view of what's workable, we don't want to put companies out of business. We just want to protect PII to the extent that we can, but not throw up a roadblock so that costs go up, companies go out business, all kinds of other things happen.

Jane Bambauer:

Services get worse.

Bill Tolson:

Exactly. I really thought that the way you explained that was really illuminating. I really liked that. I hadn't thought of that.

Jane Bambauer:

I think there's also sort of a selection effect problem. The people who are really focused on a privacy law and getting it passed, they are generally speaking, I think they would invite and be perfectly okay with a big upheaval in the internet economy. And so just taking behavioral advertising as an example, I travel in privacy law circles. My colleagues, they understand that by cutting off behavioral advertising revenues, the content creators, so I'm not talking about Google and Facebook and the ones that serve the ads, they're the middle men. They're going to be okay no matter what.

Jane Bambauer:

But it's the content creators whose revenues are going to go down, and that if your privacy sensitive, that's okay. But it's not clear that that's what a fully informed and more typical American, it's not clear to me at least, that that's actually what they want. And if it is, I'm happy to be proven wrong. And if I'm the weirdo that actually just likes having free services that are really frictionless, if I'm the weird- I'm happy to be outvoted. But right now I think we're at risk of having a minority position that sor superficially seems to be serving the general public making its way into law.

Bill Tolson:

Yeah, I think you mentioned that for example, that current state laws, the five may be in the long run unworkable. Did I hear that right?

Jane Bambauer:

Yeah.

Bill Tolson:

As they amend them from session to session, then my guess is they're going to amend them to be more complex and burdensome just based on the input they're getting from organizations, the big corporations you've mentioned many of them that have their hands in this stuff. They're trying to create these laws to better their business or at least make it easier for them versus what's good for the business environment as well as the individual data subjects.

Jane Bambauer:

I have on occasion been very cynical about why some of the biggest companies, Microsoft and whatnot, are very happy to push, Google too, are very happy to push some of these privacy bills. To give a specific example, I believe it's the Colorado bill, correct me if I'm wrong, but I believe it's the Colorado bill that was the first to incorporate a kind of universal opt out signal.

Bill Tolson:

Yes.

Jane Bambauer:

So that's in the proposed federal privacy law too.

Bill Tolson:

And that they're also, I've listened to a webinar today by David Stauss. You probably know who he is, Byte Back law and it went through the ADPPA, but they were talking about having this universal opt out kind of consolidation so that you don't have to go to each corporate website to opt out. You go to a registry that says opt me out of everything. Or you even build it into an internet browser that you can set. I thought that was just tremendous.

Jane Bambauer:

It is tremendous in terms of facilitating control, but if a consumer who feels annoyed at these giants goes ahead and gets on the unified opt out list, sort of like the do not call list.

Bill Tolson:

Yeah, that worked.

Jane Bambauer:

And then at the same time, and I think many would given the option once it's made clearer what your rights are, I think many would at that point, I think we're going to be in a role sort of crisis situation where the content companies are then going to have to either strong arm their own consumers into changing their settings, which California law, a lot of the laws try to prevent the companies from even being able to do that, or the content that they get is going to be worse in some way, either less of it. There is empirical evidence showing that differences in default settings of the law affect literally the amount of content that's produced. So it could be the amount of content, could be quality of content, it could be that you get the same content, but now you're seeing more advertising because they have to make up for the revenue loss.

Jane Bambauer:

I think that we can talk in a way, the privacy conversation has not totally consciously made use of the fact that very few people bother opting out and so therefore you don't really see these seismic changes in the services we have available. But if everyone did opt out, we would see those changes. I think consumers would not actually be happy with that in the long run.

Bill Tolson:

That makes sense. On a hopefully related subject, a while ago you mentioned data security and your model law as well as all of the bills and laws that I've looked at, at least in the states and Canada as well as the EU, they all approach data security in almost exactly the same way. They all basically use the same terminology for data security. The data collector or data processor must use reasonable security practices.

Bill Tolson:

Even the GDPR. And being more of a technical guy, first thing that occurred to me is define reasonable. Is there a basic definition, legal definition for reasonable? Because I thought, geez, what lawyer couldn't get out of a complaint that you didn't use reasonable security practices? Define reasonable. Is it industry standard, those kinds of things. And I've been somewhat educated on that, and I notice also your model law does talk about provide reasonable data security measures, so on and so on. And they all do. And I'd just love to get your thought on that. Do you think either now or eventually the laws need to be a bit more prescriptive? Like all PII must be encrypted while in transit and at rest?

Bill Tolson:

Something as simple as that because encryption is a technology everybody knows it's not owned by one company. Lots of applications already do it. And I've put that question to many of the senators and representatives at the state level and say, well, why wasn't it more prescriptive? And very nice people by the way, but they didn't really know. It was more of this is what our advisors told us to put in. And by the way, GDPR does state that.

Jane Bambauer:

That it must be encrypted. It's specific.

Bill Tolson:

Well, no, must use reasonable security practice. But I'm glad you said that because with the GDPR, it doesn't mention a specific technology or anything. And I'm not saying it should, but I think the basics should be there. But the GDPR also states that a PII is encrypted and a breach occurs, then the breach notification requirement's not triggered.

Jane Bambauer:

So there's a carrot.

Bill Tolson:

And I love the fact that they did that. But just love to get your opinion on do we need to go further in specifying I guess, base reasonable security practices or is that terminology, does it fit into the law and how it would be described? By the way, I've actually had a person on my podcast couple of weeks ago who was actually one of the authors of the Sedona Conference commentary on the reasonable security test, which actually boils down to they built an algorithm that attempts to measure incremental burdens and benefits on security. So it's still really interesting discussion. Really interesting guy, and I absolutely respect the Sedona conference and what they do, but I just wonder, could we be just a tiny bit more prescriptive?

Jane Bambauer:

It's possible that we should be more prescriptive along the lines that you're suggesting, having a clean rule that is at least a baseline, a bottom floor. I'll tell you the two reasons that we probably didn't do it. One was that especially when you're doing a broad privacy law and omnibus privacy law, it doesn't draw security experts in the room as often. And so we simply, I think a lot of lawmakers and drafters are nervous being too specific about something they don't understand. That might be the practical explanation. But I think also, and I'm curious if the Sedona Conference came to a similar conclusion, I think another concern is that much like negligence law itself that uses this reasonableness s

and doesn't bother, then let's kind of more specific cases or bodies like the FTC kind of define what we mean. I think one advantage might be is that there could be some uses of data.

Jane Bambauer:

Let me give you a scenario. Let's say that you have a database that is probably not scrubbed enough to be considered de-identified and so therefore it's PII, but it's not really usable for attacks. It would take a lot of effort to actually re-identify someone or to make it usable to phish or whatever. Something like that, maybe there is an encryption burden or maybe there might be some burdens that are not worth it in a cost benefit sense. I'm not sure though, again, my first answer is the correct one, which is that I profess ignorance. So that's probably the main reason we just relied on reasonableness. And we also felt like, well there's now a body of quasi case law from the Federal Trade Commission because they've enforced lax security more than anything else in their privacy caseload. So I think those kind of gave us a chance to punt but it is a punt. I'll acknowledge that.

Bill Tolson:

Just lately in the last couple of weeks, this gentleman, Chris Cronin, who was co-author the Sedona Conference right up on it, he pointed me to a very recent settlement, basically a multi-state settlement, six states with a company called Wawa Incorporated. I guess they're kind of a convenience store place that had had a data breach with 34 million payment cards and all kinds of other stuff. And the main argument was that the company Wawa did not provide reasonable security protection. So under the **agree**ment, the six states basically listed some very specific security requirements for them, which is getting into more prescriptive stuff. And Wawa **agree**d. And basically they wanted to actually list out some very specific security safeguards with respect to logging and monitoring, data access, access controls, file integrity monitoring, firewalls. But they also list encryption as one of the directives and then others like comprehensive risk assessments, penetration testing, things like that.

Bill Tolson:

But I thought this six state **agree**ment with the company that had been breached that listed a series of more prescriptive security requirements, which included actually encryption. I thought that was really interesting, and that actually might prove to be maybe a precedent going forward for others. I thought that was interesting. I never would've found that unless this guy pointed it out, and I read through. I'm wondering if you've had any time to look at the federal bill in the House, the ADPPA, what you think of it, what do you think the changes are of it getting through, those kinds of things?

Jane Bambauer:

Well, I mean there's going to be a lot of pressure next year or next term in getting it through. I so this bill has managed to kind of create a kind of coalition of people who are ready to argue thi od

enough. It is being described as a kind of compromise bill. I don't really see it that way. The reason it's being described as a compromise bill is because it preempts California and all other state laws.

Bill Tolson:

Yes, the preemption and the private right action are the two biggest problems.

Jane Bambauer:

And the private right of action, there is one, but it doesn't start for a while and it's somewhat limited.

Bill Tolson:

And it's like two years. Yeah.

Jane Bambauer:

Preemption I think is good. I mean, after our whole conversation, I think the audience will not be surprised. The preemption's good. The private right of action, this might surprise people, but I actually have no problem with even a strong private right of action if the substance of the law is good and predictable and advanced. So my problem really is the substance. And when people talk about this being a compromised bill, they almost never talk about what's actually required in it, and what's actually required in it is excessive, in my opinion. So not only do you have the data minimization and loyalty duty and right to deletion and right to access and right to direction, there's also, I mean they're experimenting with things like right to algorithm, transparency, that sort of thing. This has so many rights in a space where we should not be thinking about rights. We should be thinking about conflicting interests and how to manage them through risk management. So I actually do not like this bill despite the fact that it has some procedural stuff that I think is good.

Bill Tolson:

Yeah. I've heard so called subject matter experts or pundits basically say it's the US trying to out GDPR the EU.

Jane Bambauer:

Well, I'm glad that they're saying that because at least in a lot of mainstream media and then even in the law circles that I'm in, the discussion really isn't on what it would require. The discussion is about California. I think it's focused on how exactly California's just set up this new agency, and now this agency will become moot. It's like that is so irrelevant to the question of what should privacy law be.

Bill Tolson:

Right. California's obviously fighting the preemption. They're trying to add the little tiny bits in here and there to make California sit down, but that's not going to happen. But I thought what you mentioned also the whole idea of data minimization. I mean, in the business that I'm in with data management and archiving, stuff like that, even with general counsels in companies, the idea of keeping everything forever kind of went away 10 years ago because of the risk and the liability and smoking guns and all kinds of stuff. So the idea within the records management community of data minimization, get rid of stuff you don't need or doesn't have value to the company anymore, also doesn't have liability as well, I think is an interesting thing.

Bill Tolson:

And the fact that they included in this bill really surprised me. I thought that was really, in my mind, interesting, but totally unexpected. Jane, I think we've reached the point where we need to wrap up this edition of the Archive 360 Podcast. I really want to thank you for this really insightful, fun discussion I had today. I love talking about this stuff with people and especially you. You really made me see some things that I hadn't seen before and I really appreciate that.

Jane Bambauer:

That's really an honor to hear because you've talked to the best of them. You have a really great podcast here. So thanks so much for having me.

Bill Tolson:

I appreciate that. And hopefully we can do it again. Maybe if the ADPPA passes, love to get you back on to get some more opinions from you. But we'll look at that if it actually gets through. If you have time, we can talk about the Canadian bill. It really has some interesting stuff in it, but I know you haven't looked at it yet, so I appreciate it. If anyone has questions on this topic, Jane and I have been talking about today or would like to talk to a subject matter expert, please send an email mentioning this podcast to info I-N-F-O @archive360.com or directly to me, Bill.tolson T-O-L-S-O-N@archive360.com. And we'll get to soon as possible. You can also email Jane with questions. Jane Bambauer, J-A-N-E B-A-M-B-A-U-E-R@Arizona.edu.

Bill Tolson:

Also check back with the Archive360 resources page for new podcasts with leading industry experts like Professor Bambauer, or diverse subject matters, experts, more in depth on data security, information management, archiving, records management, regulatory compliance, all of those kind of things. Also, all of these podcasts, which are on our resource page are also published up into iTunes, Spotify, the Google Podcast platform as well as many others. So you can find us anywhere, b keep publishing podcasts around these topics. And with that, I will close it. But Jane, it was ve y fun for me to have this discussion. I very much appreciate it.

Jane Bambauer:

Likewise. Thank you so much, Bill.

# Questions?

Have a question for one of our speakers? Post it here.

First Name**

Last Name**

Email**

Questions?**

SUBMIT

## Related Posts

SEPTEMBER 21, 2022

## Episode 31: Discussing Data Privacy Regulation with the CPO of NC

Bill Tolson and Cherie Givens, Chief Privacy Officer of North Carolina discusses this newly created position and the current data privacy strategy.

By: Bill Tolson | Data Privacy | Regulatory Compliance | Data archiving | Information Management | Information Security | Information Governance | data security

**LISTEN NOW →**

AUGUST 24, 2022

## Episode 29: What is "Reasonable Data Security"?

In this episode, Bill Tolson and guest Chris Cronin discuss the term *reasonable data security* found in many states' privacy regulations.

By: Bill Tolson | Data Privacy | Regulatory Compliance | Data archiving | Information Management | Information Security | Information Governance | data security

**LISTEN NOW →**

## Contact Us to Learn More

### Contact Us

ARCHIVE360

+1 (212) 731-2438

info@archive360.com

Microsoft Partner
Gold Cloud Platform
Gold Application Development
Gold DevOps
Gold Security
Gold Application Integration

**PLATFORM**

- Open Archiving Archive Migration
- Zero Trust Security

**SOLUTIONS**

- Enterprise Vault Migration
- Journal Archiving Microsoft Teams Archiving
- SharePoint Archiving
- Salesforce Data
- Archiving Legal and eDiscovery
- Records Management
- Email Archiving Supervision and Surveillance

**RESOURCES**

- All Resources
- Case Studies
- Blog
- Podcast

**COMPANY**

- About
- Leadership
- News
- In the Media
- Become a Partner
- Microsoft Partnership
- Customer Support
- Careers

© 2022 Archive360. All Rights Reserved | Terms & Conditions