

International privacy series: episode 1 - Hot topics in U.S. privacy & AI law with Gary Kibel, Davis+Gilbert

Alexander Milner-Smith

Thanks for tuning in to the first episode in our 2026 International Privacy Series. We were delighted to be joined by Gary Kibel, partner at Davis and Gilbert, who explored the increasingly complex legal landscape facing organisations operating in the United States.

He looked at the continued proliferation of state consumer privacy laws in the absence of federal legislation and what this patchwork means for compliance strategies and operational execution. He discussed the uptick in regulatory enforcement activity and the rising threats from class action litigation and beyond privacy explored the rapidly developing regulatory framework for AI, looking at how state level initiatives contrast with the current federal government's approach.

It was an amazing session and I'm pleased to be able to share it with those who weren't in the room. Listen on to hear from Gary.

Gary Kibel

OK, thanks very much for having me here. ~ My name's Gary Kibel from Davis and Gilbert. As Bryony said, we're a very similar firm to Lewis Silkin in the US, similar focus. There are so many things going on in the US right now in this area. It is kind of crazy.

Okay, so privacy is obviously important to consumers. The US, it's getting crazier and crazier because unlike here and in the EU, we don't have one law, like the GDPR or the UK GDPR, that regulates everything. We have on the federal level a lot of different sectoral laws, but the closest thing we have on the federal level to a comprehensive privacy law is one sentence. Under the Federal Trade Commission Act, they have the ability...

to regulate unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful. That's the one sentence they use to regulate the advertising industry, privacy, everything consumer facing. So if you had a car commercial that says the car goes zero to 60 in three seconds and that wasn't true, that would be deceptive. If you had a privacy policy that says we do not sell your personal information, that would be deceptive.

If you had a security breach and information got out, they would argue that's unfair. So this one sentence is really all that the federal regulators can do on a general level for privacy. Now there are many, many sectoral laws in the federal level about children, healthcare, financial services, email marketing, but the states are really getting involved here and that's what's created a lot of confusion which started about ~ six years ago now, well actually eight years ago that the CCPA

The California Consumer Privacy Act was passed, and that was the first comprehensive consumer privacy law in the United States. And it basically codified things that we thought would be normal good

practices that anybody would do. You must have a privacy policy. That wasn't a law in the United States until the CCPA. You have to give consumers access rights, like under the GDPR. And you need to give consumers the right to opt out of the sale of their personal information. And there's a lot to unpack there.

But the important thing to know is that the US, for the most part, is an opt-out jurisdiction, except for sensitive personal data and some other things we'll talk about. Whereas in the EU, it's opt-in. In the UK, it's opt-in generally. You need a legal basis to process the data, usually consent, sometimes legitimate interest, but mostly an opt-in. We're in an opt-out world, so you suck up all the data, but then you need to give consumers all these rights.

When we say in the U.S. about selling data, it's not just setting up a table in Times Square and giving out email addresses. It's any sort of transfer of data for monetary or other valuable consideration. And California requires that in order to allow people to opt out, you must have a very specific link on the website. It used to be that the link had to say, do not sell or share my personal information. Now you can do this alternative link of your privacy choices with that special icon. This must be in the footer of any website that is deemed to be selling information under the CCPA. So if you go to most websites and you scroll down to the bottom these days, there's gonna be a whole series of new links. This is an older screenshot, so it has the do not sell link. And then when you click that, it pops up a process. The link is statutorily mandated. What happens when you click the link is up to the company. But it just needs to be an easy process and not a confusing process. The regulators talk about symmetry and choice, making it as easy to opt out as it is to get in. So regulators are very, very focused on that. And most of the enforcement actions that are coming out of California so far have been focused on these opt-outs. They've been going after companies that are not having a proper opt-out or are making it challenging for consumers. Honda had a challenging one where they were asking consumers for so much additional information to opt out, the regulators felt like this was really a burden to consumers to be able to opt out.

They've also been focused on contracts because the CCPA and some other state laws require very specific contracts, like a DPA, between a controller and a processor. And because this is an opt-out world where it's either a sale to a third party or it's data you're transferring to the processor, you need to have a contract to prove that it's data transferred to a processor. Otherwise, the regulators will feel that you're selling personal information. And their enforcement's getting a little bit more unique. This was about a week and a half ago, maybe two weeks ago. Disney was hit with the largest fine in California so far, \$2.75 million. And their issue was very unique. So Disney, like Disney Plus and all those services are very authenticated. You log in with your ID and password. Well, what Disney was doing is if you logged in on your laptop and said you wanted to opt out, they opted out that laptop.

But then when you logged in on your iPhone, you were not ~ opted out from the iPhone. But Disney was linking the devices for targeted advertising purposes. So the regulator said, well, you can obviously link the devices because you know how to do it. So why are you not opting out the consumer when they opt out on the laptop, opt them out on the iPhone as well? It's the same account. It's the same person. So I think that's having a lot of companies look at the way that they do linking between different devices.

The opinion talked about probabilistic targeting, because that's a little different. Disney was deterministically knowing that this was the same person on the laptop and on the phone. So the CCPA was very complex, and then California amended it a few years ago with the CPRA, the California Privacy Rights Act. And it did a couple of very important things. Number one, California is now the only state privacy law that regulates B2B data. So it applies to employees as well.

Every other state that has implemented a comprehensive consumer privacy law only has it applied to what you would think of as consumers. But California applies to B2B. So if you have offices and personnel in California, you need to issue them a privacy policy and give them the rights to access their data. Also, the biggest thing that happened with this change in CPRA is California established the California Privacy Protection Agency, the CPPA.

There's so many different acronyms, gets very confusing. But the CPPA is the United States' only standalone privacy regulatory agency. Now the FTC, which I spoke about earlier, the Federal Trade Commission, they regulate so many different things in advertising and consumers and manufacturing and antitrust. But there's no federal agency and there's no other state agency that has one mission to regulate privacy. California has it. So as you can expect, they're getting very active in terms of enforcement. Some things that the CPPA is doing is they're issuing lots of rulemaking about different areas, automated decision making, cybersecurity audits and risk assessments. I think this is going to be a big thing in the industry in the US. They have now passed a rule that for businesses that are processing data that represents a significant risk, and that's based on the volume of data processed, you will need to have an annual independent cybersecurity audit.

The first ones kick in in April of 2028 based on revenue and then other companies are going to be pulled in in 29 and 30. And then you also need to do risk assessments if you're engaged in high risk processing activities and that includes targeted advertising. Now you're not going to submit those risk assessments but you're going to have to attest that you have completed them. So I think there's going to be a whole new industry here of auditors and risk assessors who are coming out of the woodworks to offer new services here.

Okay, I like to be educational here, so little known fact. There are 49 other states in the United States besides California. And they all wanted to get in on the act. And they have. And so we now have 19 states in the United States with a comprehensive consumer privacy law. There are other types of laws we'll talk about through this presentation, but these are sort of the ones that mirror CCPA the closest they can. Problem is, they don't line up with each other very well. And I often get questions from ~ clients saying, well, you got all these different laws, just tell me the strictest one and I'll just comply with the strictest one. It's gotta be California, right? And the answer, from my opinion, is no, I don't think California is the strictest law. I think it's the most comprehensive law. They have the most regulations and most detail and... the most enforcement, but I don't think it's the strictest laws I'll show you in a moment. but just to say firstly, there's a threshold test in every state as to whether or not the law even applies to your business. Most of them are based on the number of records you're processing. Some of them are based on the revenue of the company, and some of them are based on the percentage of revenue you earn from selling personal information.

Another disconnect, opt-out preference signals. This is a big issue now in the US. So browsers can send automatic opt-out preference signals like a DNT, do not track signal, or a GPC, a global privacy control signal. Well, by law, some states are saying you must recognize those signals that are sent automatically and treat them as the consumer's request to opt out. Even though the consumer may have done nothing and it may have been on by default, you have to treat that automatically.

as the consumer requesting to opt out. The California regulators, when they reach out to companies, have been asking, how do you honor GPC signals? Because they want to know that you've built in the technology to do that. One of the other biggest disconnects is in sensitive personal information. And this is really one of the hottest areas for regulators they like to go after, sensitive personal information. Firstly, it's defined differently in all the different states. But these are common themes.

precise geolocation, racial ethnic information, biometric health, children. I mentioned that California is not the strictest state. California is one of the very few states that has an opt out for processing sensitive personal information. Nearly every other state requires an opt in to process that data. But there are differences in these definitions here. The way sexual orientation is defined is often different. Precise geolocation is even defined differently.

California defines it as under 1,850 feet. Most other states define it as under 1,750 feet. So it's different. There are so many disconnects. I just picked out a few here and there. Oregon, a very unique requirement. If a consumer reaches out and wants an access request, not only do you have to tell them the categories of third parties to whom you shared personal information, you have to tell them the names of the third parties.

Now there is a carve out for trade secrets. So don't have to reveal your trade secrets. But by Oregon law, unless it's a trade secret, you need to tell the consumer all the third parties that you've sent their personal information to. Minnesota has a similar one. Rhode Island has a really wacky one that they actually require that you put into your privacy policy the names of the third parties that you transfer the personal data to. And there's no trade secret exception.

Every client I've told this to so far has said, hell no, I am not doing that. Because the idea of putting all your customer names into your privacy policy is something nobody ever thought of doing. ~ We'll wait to see what happens when Rhode Island regulators reach out about this. I mentioned earlier about DPAs. Some states require that you have a data protection agreement. California is very prescriptive about the type of language that's in the agreement, whether it's a processor or it's a third party to whom you're selling the data. It's very different language and it's very specific language and the regulators ask to see these contracts because if the right language is not there, for example, for being a service provider or processor, then they're going to believe you're selling the data because you didn't get the right language into your contracts. Data privacy impact assessments, some states require them, some states don't.

Alright so, I've mentioned a couple times that I don't think California is the strictest state in the US. I think Maryland is the strictest privacy law on the state level in the US. Maryland has a prohibition on selling sensitive personal information. It's an outright prohibition. You can get consent, you can't do it. You can get consent from the the minors' parents in a sworn statement, you cannot do it. You cannot sell the sensitive personal information at all. And that's very unique.

They also have codified a data minimization requirement. We always talk about data minimization. Don't collect more data than you need. California talks about purpose limitation. Only collect what you need for a purpose. But Maryland put this very strict requirement in place that says a controller shall limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. So think when you go to a website and you want to go to a news website, but there's 12 tracking pixels in the background for targeted advertising. Did the consumer request that those tracking pixels collect data for a specific product or service? Probably not. You may have a cookie banner and they said yes, but it didn't identify all those parties. It's going to be interesting to see what happens when Maryland starts to dig into this. They haven't yet, but I think they're going to step up enforcement. Okay, let's go to another topic, children's privacy.

This is even getting crazier in the United States. We have so many different standards. It used to be very simple in the United States. We have a federal law that still exists, the Children's Online Privacy Protection Act, pretty straightforward. You don't collect personal information from children under 13

without parental or guardian consent. That was very simple. Then the state started to say, well, under 13 is not enough. We need more. So now...

I put things into multiple buckets here. There's probably 10 different buckets amongst the states in terms of processing data of teenagers. In some states, you need opt-in consent from the teenager in order to use their data for targeted advertising. So I mentioned how the US is mostly an opt-out jurisdiction. So you may have a website with tracking pixels. If you have actual knowledge or reasonable knowledge that children are accessing that service, you need consent from those teenagers in order to collect data for targeted advertising. Some states, like Maryland, you can't do it at all. So there is no way you can do targeted advertising by collecting personal information from anyone under 18. And some other states are now starting to consider similar prohibitions. Just like you have in the ICO here in the UK, there are age-appropriate design codes. And these are laws designed to...

specifically target the way that advertisers are processing personal information and targeting children. And you probably often hear in the news here about the US, red states and blue states. Everything is divided in the US between red states and blue states, Republican and Democrat, right and left. Well, as you can see from the list of states here, it doesn't make a difference whether it's a red state or a blue state with these laws. South Carolina is the most recent one to pass an age-appropriate design code.

They are probably the most red state we have in United States. So it's coming into play in every state in the United States. The way that these age-appropriate design codes work is that you're only supposed to be processing data in the best interest of the child, not in the best interest of the business. And if a service is reasonably likely to be accessed by children, then you need to configure all default privacy settings to a high level of privacy.

So that probably means you need to opt them out of everything automatically. And again, this law is currently in effect, but there's not been any enforcement yet. I'm going to fly through this. Just look at the heading. Age verification laws, another new area that's becoming hot in the US. They need to verify the ages of the consumers so you know whether or not you're processing the information of children. Now, there has been a lot of move to make the age verification happen here.

Shouldn't Apple and Google just verify the ages of everyone? That would be a lot easier than making every website and every app verify the ages. That is a positive thing, although if they then pass that data down, going back to one of my prior slides, if Apple and Google are verifying everybody's ages, then every app and every website definitely knows the ages of their consumers. So there's positive and negatives, but these laws are being passed all over the place. Okay.

I'll go to data brokers. So data brokers are a hot issue in the United States because processing data is how you make your business valuable and bad data leads to bad business results.

Okay, so data's very important to drive businesses. The data brokerage business has become very, very big. Who are data brokers? Those are parties that are collecting data when they do not have a direct relationship with that consumer, and then they are selling that data. We have four data broker laws in the United States right now, Vermont, California, Texas, and Oregon. And the way they generally work, which is pretty straightforward, is that you register on the website, you pay some money, you're listed as a data broker and they'll link to your privacy policy. That's about it. Texas has a couple of wrinkles. But in California, I think there's about 600 registered data brokers. If you wanted to opt out from all of those registered data brokers, I think it would probably take you two weeks working full-time, eight hours a day. Because you would literally have to go to the list and go, all right, data broker number one. I'll click on their privacy policy.

I'll read their policies, see what their opt-out process is, go through their opt-out process. Now I'll go back to broker number two and go through all seven or 800. Well, California says, let's take that two week process and make it down to maybe five seconds. So they've implemented the DELETE Act. The DELETE Act will allow consumers to opt out in one click from every registered data broker. And they've taken care of the dirty secret in the industry that data brokers always knew that, well,

Delete the data, I'm going to get your data again someplace else. I'll find it someplace else online or from another party. This requires the data brokers to refresh deletions every 45 days. So basically the data stays permanently deleted and the fines are going to be absolutely outrageous. So currently under the DELETE Act for failing to register as a data broker, you can be fined \$200 per day. Starting in August,

when it goes live for data brokers, you can be fined \$200 per day per registered California consumer. So right now their system has opened up. It's called the DROP, the Delete Request and Opt Out platform. It opened up in January, January 1st for consumers to sign up. They have not advertised this at all, and they already say there's about 240,000 California consumers who have signed up. They're going to do a... actual advertising campaign this summer to get consumers to sign up. I think they're going to have two, three or four million people. And by August 1st, data brokers are required to process the opt-outs. Going back to what I said about fines, \$200 per day per registered California user. you're not registered, you're not doing it properly for one day. It's \$200 times four million consumers. So I mean, it could be outrageous in terms of the fines.

The way the drop is going to work is that consumers sign up on this website in California. California will verify that they are a California resident. The data brokers don't need to do that. Then there's going to be different lists inside the drop. Every registered data broker is required to download at least one list every 45 days and process opt-outs. They need to go through a standardization process for their data so that there's not... you know, a hyphen in the first to last name or a period, need to tighten it all up. It's really going to be quite a burden for data brokers. Data brokers were required to sign up for the drop by January 31st, so they're technically in violation if they've not done so yet. Consumers are signing up. California has not given a lot of details about how the APIs are going to work in this system, but by August 1st, that's when data brokers are to have to process opt-outs. And, um...

I was at a conference last week in California where some regulators were speaking and I got to ask a question and kind of embarrassed them in front of the room. I said, if all a data broker has is their own cookie ID, they're definitely a data broker because they're collecting, you know, cookies in the back of websites and selling that data. How do they allow consumers to opt out through this system? Because there is no list of that data broker's own cookie ID in the system. And the regulator kind of nodded her head and she goes,

Yeah, there's nothing for them to do. I'm like, oh, that's good. She goes, but you still need to download one list every 45 days to make sure there's nothing to do. I said, so you have to log into this system, download a list of like email addresses, and then say, well, we have no email addresses and do nothing and do that every 45 days. And she said, yeah, that's unfortunately the way the law works. You must do something every 45 days.

So, it's going to be an interesting system. They're explaining to consumers how to upload their mobile advertising IDs, their IDs. ~ And we'll see what happens, how many consumers sign up for this. OK, I'm going to go through a whole series now of sensitive personal information and then some unique privacy laws before we get to AI. And then I run out of breath by 5 o'clock. So health information. There are some discrete laws about consumer health data. Washington, this is Washington state, not

Washington, D.C. They have a law called My Health, My Data Act. They do not have a comprehensive consumer privacy law. This is just about health data. But we're all lawyers here, and we always focus on the most important thing down at the bottom. The Washington law has a private right of action, meaning individuals can sue, meaning class action lawyers can sue, which is always the big fear.

They define consumer health data extremely broadly. If you had a website where you're, you know, it says, do you have headaches? Click here and you pixel that party. They may argue that that's consumer health data and you have to get an opt in for that data. You have to have a separate standalone privacy policy for that data. There's a lot of obligations. When this was enacted, we thought we'd see a rash of class action lawsuits. It hasn't happened yet, but this law is still out there and I think some other states are going to do things similarly.

This has been a little bit more common, geofencing prohibitions around healthcare facilities. So if you follow US politics and the Supreme Court, the Supreme Court overturned a law, a court ruling last year called *Roe v. Wade*, which allowed a woman a right to seek an abortion. That was a right, a privacy right under the Constitution. They took that away and set it up to states. And then there was a fear that companies were gonna start to geofence around women's healthcare facilities and send them targeted messages to harass them.

So states, and this was mostly blue states, started to pass laws that says you cannot geofence around a healthcare facility. So that's an issue for advertisers. If you have pharmaceutical clients that want to target ads to healthcare facilities, because that makes sense, they can't do it in certain states. So what's the industry doing on the self-regulatory? We have all these new privacy laws. There are still self-regulatory programs out there. And ~ you're probably familiar with a number of these names.

So, you know, the IAB, the ANA, NAI, these programs are still out there. So the Digital Advertising Alliance, they had their different principles for opting out of targeted advertising.

Then there's a network advertising initiative, the NAI. They used to have their own opt-out program, but they sunset their opt-out program because they realized the self-regulatory program doesn't ensure compliance with applicable law, so why do it? You should just do what complies with applicable law. But the NAI, think, is a great organization, ~ really good membership, and they give guidance to their members about how to comply with the law.

The one self-regulatory program that I think is very helpful, and it is designed to help you comply with the law, is the IAB's Multistate Privacy Agreement, the MSPA. What the MSPA does is it helps you do a number of things. Number one, it helps you process opt-outs when there's multiple parties you need to pass opt-out signals downstream, because that's very challenging, because you may have pixels on your website, but they're bundled with other pixels, and they're calling out to other parties as well.

And so this will pass an opt-out signal down to all those parties. The second thing that's really valuable is what they call their springing contracts. I mentioned earlier that some states require you have a written contract with all the parties to whom you share data with. Well, if you've got all these pixel providers on your website and they bundle with other pixels, you may not have contracts with all those parties. What the MSPA does is it makes every signatory a third-party beneficiary to other signatories. That way you actually have a contract with every party in the ecosystem. And it is a very complex system. This is the flowchart of data and permissions under the MSPA. It's not easy, but most consent management platforms, the CMPs, will help you comply with the MSPA if you're a signatory. Okay, biometric laws, another sensitive area in the U.S. The most significant biometric law is in Illinois, the Illinois Biometric Information Privacy Act, or BIPA.

The reason it's the most significant private right of action, individuals can sue. So if you are processing biometric information in Illinois, such as you have a warehouse and employees come in and they do a fingerprint, or you're doing some facial scan or retina scan, there are specific requirements and they're kind of nuanced about having a written retention policy, about getting consent, about saying how long you're going to retain the data. If you don't do these things, you could be subject to a class action lawsuit and there have been many, many class action lawsuits over this law. I mentioned it's not a red state or a blue state issue. Texas has one of the most significant biometric laws and they've been very aggressive in enforcing it. They got 1.4 billion out of Meta. So their attorney general who is currently running for US Senate, I think, he's bragging about how much money he's generated for Texas by going after the big tech companies. There are additional biometric laws elsewhere.

But the challenge is when there's no law applicable. So ~ my firm's in New York, Madison Square Garden, one of the most famous arenas. I go there for Knicks basketball games. And the owner of the Knicks, not a very popular guy amongst fans, and he set up a system to do facial scans of every patron coming into Madison Square Garden. And if you even worked for any law firm that was suing any of his companies, they would ban you from entering Madison Square Garden.

And when that happened, yes, I see jaws dropping. Everybody was like, this has to violate a law. But there is no biometric law in New York State. There is no comprehensive consumer privacy law in New York State. There's nothing that it violated. There is a new law about signage if you're doing biometrics in New York City. actually, I took a picture of this back in December when I went to the garden for a game. They now have new signage. But this does not violate any law.

New York State was trying to find an angle to make them stop doing this. So they were trying to go after the liquor license for the garden because if you're a place of public accommodation, you can't discriminate against people and have the liquor license. ~ But they are still doing this today. ~ For what I understand, it's now no longer that you work for any law firm, but that you're a lawyer for that law firm. But think, if you're in a thousand person law firm and you're in the Oregon office,

You have no idea someone in New York is suing one of his companies and you're there on vacation with your family and you want to go see the Knicks or the Rangers. You walk in, they scan your face, they go, nope, you can't come in, get out. And so this is what happens when there's no laws. Class action lawsuits. ~ The bane of our existence in United States. It's bad and it's getting worse. So there are class action lawyers, look for money. That's all they're looking for. They're not looking for corrective action for consumers and protecting consumers. They're looking for money. They're looking for a quick hit. And what they always do is look for a law that they can latch onto that will generate a lot of money. One law that was a good cash cow for them was the Video Privacy Protection Act, the VPPA. Now, you might sit to me and say, like, you videotapes. This is, ancient stuff. And for anybody, like, under 35, let me explain. There were these plastic things with little circles. You can look it up online. ~

This law was passed in the 1980s when there was a hearing for a new Supreme Court justice. His name was Robert Bork. And Democrats didn't want him to get nominated. He was super conservative. And a reporter got his videotape rental history from Blockbuster. now, there was nothing shocking there. He was not renting any questionable videotapes. But you can imagine the members of Congress, and they were like, people can get my videotape rental history, they pass this law really, really fast. And it's been amended and it applies to digital media and online. So it applies to Netflix and other systems. And it applies to anyone with ~ pre-recorded videos. And there's a lot of different wrinkles there about collecting personal information from a consumer who's a subscriber to a videotape service. There's lots of ways to dig holes in the arguments.

But the class action lawyers have jumped all over this. The quick takeaway, if you have any videos on your website, do not attach tracking pixels directly to that one video to identify the consumers having watched that one video. It's okay to identify them as having landed on the page, but don't identify them as having watched one video. This is the one, and maybe some of you are familiar with this, CIPA the California Invasion of Privacy Act. This is an absolute disease in the United States right now.

Class-action lawyers are sending out thousands of letters. They are filing thousands of lawsuits. This is a wiretapping law from the 1960s, which prohibits intercepting communications. Now, why do you think this was passed in the 1960s? It was for unscrewing the telephone, putting in a bug and screwing it back in and then listening to a phone call. Well, courts in California opened the door to the belief that tracking pixels on a website, collecting data, is intercepting a communication in violation of wiretapping laws. There, as I mentioned, is thousands of cases pending in California courts. There have been cases that are favorable to plaintiffs and cases that are favorable to defendants. But as we all know as lawyers, people don't want to litigate because the cost is outrageous. There are class action firms in California that are very sophisticated in this area and they will file lawsuits and they are sending out nonstop letters to every website they can find if there's any sort of tracking pixel on the website and it's not on an opt-in basis. Remember I mentioned earlier, there's no requirement under the law for opt-in. They've basically turned the wiretapping laws into making everything opt-in in the US. And a client gets the letter and I have the same conversation with them. say, look, we can litigate. I say you probably have an 80 % chance of winning a motion to dismiss that may cost you \$50,000 to \$100,000.

or you can settle with these guys for 10,000 and they'll go away. Endless companies are settling and these class action lawyers, their motivation is to keep going because from their point of view, send out 30 letters, maybe four go to court, they lose three times, but those other 26 companies settle. So they keep sending out the letters, they're perfectly willing to go to court and lose because it makes the threat real. So talk to anyone in the US, CIPA has been an absolute nightmare. We've probably helped settle 50 to 60 of these. It's just nonstop. That's why in the US now we see cookie banners all over the place. They're not required by law. It's to put a speed bump to prevent the class action lawyers are coming after you. This is the number one piece of advice takeaway. I would say that if you have a website targeting US consumers, geotarget California and make your cookie banner strictly opt in. Other states.

less risky to opt out. There are wiretapping laws in other states, but it's California. And unless you're willing to just, you know, as a cost of doing business, pay out these class action attorneys, make it opt in in California. Okay. New and pending legislation. ~ And ~ it would be helpful if there was federal legislation to resolve these issues. Well, we don't have a new federal law. We just had the FTC Act, which I described to you previously. And the FTC is focused on a lot of things. Sensitive data, AI, antitrust, dark patterns. And they're also concerned about data brokers. They're concerned about bad data. This is a real example. Office Max sent out a flyer that said, Mike said, daughter killed in car crash or current business. And, you the regulators thought this is outrageous. We have to regulate data brokers. So they're trying to regulate data brokers through just the deceptive and unfairness prong of the FTC Act.

I experienced this myself. This wine catalog, showed up at my house, and it was addressed to my son. And I thought that was kind of weird, because my son was really not interested in wine when he got this catalog. But that's just an example of bad data. Some of the FTC enforcement, again, I'll skip some of this, because I want to get to AI, they've been focused on location data in the ad tech industry. ~

They're very concerned about that, and forgive me for skipping. We don't have a federal privacy law. The closest we got was two Congresses ago.

The American Privacy Rights Act, covered all the major issues we would want to cover in privacy law. ~ This would have done everything and it got close to passing, but then there were some disconnects between left and right about preempting other state laws and about private right of action to sue. So, all right, let's spend the last 15 minutes talking about AI.

And maybe I'll leave some time for questions. Of course, you can always ask me questions afterwards at the cocktail party. So legal consideration when using generative AI. We have all the IP issues that we worry about when using AI. The United States Copyright Office has said in this statement, not a law, just their guidance statement, that original works of authorship generated by a computer are not subject to copyright protection. Because copyright protection in United States protects works that are created by humans, not works that are created by AI. So think in the advertising world, use an AI platform to create a commercial, and it's a fantastic commercial. The copyright office would say, you don't own that agency or client because a computer created it. You don't have copyright protection. Now that may sound like a novel idea, but it's actually not. plays on something that happened a long time ago. Great story.

Back, you know, more than 20 years ago or whatever, there was a photographer, very well-known photographer named David Slater, who would go out into the jungle and take pictures of animals. And he was taking pictures of gorillas and monkeys. And a monkey grabbed his camera and took a selfie of itself. And it's known as the monkey selfie. You can look up online and see stories about the monkey selfie. Well, it became very popular because it was such a funny thing. And the photographer started sending copyright claims to people saying, hey, that's my photo. That's my copyright. I own it. And went to court and tried to register with the United States Copyright Office. And everyone said, you didn't take the picture. Nerudo took the picture. And so you don't own the copyright in that photo, David Slater, even though it came from your camera. And it got funny because PETA, you know, for the know, people for the ethical treatment of animals sued on behalf of Naruto to try to get the copyright for the monkey. But the court was like, yeah, no, that's not going to work. So big thing in AI, I always do, is look at the terms and conditions and see what you're getting. So if we look at ChatGPT, I think it's really important to read those terms and conditions. So it says, may provide input to the service and receive output from the service based on your input. Together, the input and output are content. You are responsible for the content.

So they're saying you're responsible for the output. They've got no liability for it, including ensuring that it does not violate any applicable laws. You represent warrants that you have all rights, licenses, and permissions to provide input to our services. And then I love this part. As between you and OpenAI, you own the output. But they're saying, as between you and the rest of the world, good luck. But between the two of us, you can own it. And so they're saying that it could be similar to other output.

So you got to pay attention to those terms. The regulators are starting to pass privacy laws, but on the federal law, on the federal level, since we don't have laws on many things, the federal regulators have said, we don't really need a new law because we have the FTC Act, which regulates deceptive and unfair practices. And this FTC commissioner, who was since fired by our new leader, said, there is a very powerful myth out there that AI is unregulated, yet in fact, unfair and deceptive trade practices apply to AI.

Actually, the new chairman of the FTC has also said that. He said, we're not an AI regulatory agency. We don't need new AI laws, but if it's deceptive or unfair, we will regulate it. So that's not enough for the

states. The states started to say, let's get involved in this. Since the federal government is not enacting laws, we will enact AI laws and we'll fill up the chart just like the privacy laws. So this is starting to get just as complex as privacy.

Not as many yet, but it's getting there. The most significant law that was passed was the Colorado Artificial Intelligence Act. And that had a lot of similarities to the EU AI Act. ~ Some good news, at the event that was at last week, a regulator from Colorado was there and basically said we can ignore this. She didn't say that exactly, but she said, we're probably gonna amend the law during the summer.

They're also concerned about being sued by the Trump administration, which I'll explain in a moment. And they've paused drafting new regulations. So not much is happening. We were all getting very concerned about this because this was basically the EU AI Act in America. But it sounds like not much is going to happen there. But then going down to real specific issues, there are a lot of laws about using AI in employment because the concern is consequential decision making through AI.

There was an interesting case where an individual who was not hired by a company who was a minority sued the company for not hiring them based on their resume. The company said, we never even saw your resume. That's because it went through Workday's AI platform and was filtered out somehow and never even made it to the company. But it's a pretty good claim from the individual to sue the company to say, hey, that's your vendor that filtered me out, maybe for discriminatory purposes.

If you ever come across someone using AI in employment, it can be done. I was talking to a client yesterday about that, and I'm saying, you can use it, but we really need to dig deep into what this AI platform does. Is it helping you just to classify information and organize it in a better way, or is it actually screening people out? And it may screen people out unintentionally in a bad way. There are some state laws that prohibit considering someone's personal bankruptcy in a hiring decision.

What if some AI platform using for employment is searching out on the internet, found that somebody filed for personal bankruptcy five years ago, and decides to pull them out of the candidate pool? You don't know what the AI is doing, so you really need to stop when it comes to employment and really test the waters with that provider. AI transparency laws, as you can see, my slides are getting smaller and smaller, because there's more and more laws I got to shove in here. These last few slides are just like a boatload of random laws that are coming up in the US.

Transparency is a big issue. There are a number of laws that require disclosing to the consumer that some service is generated by AI, whether it's a chat bot or something else. California has a new law that requires publishing online information about your training data so that consumers know when they use a generative AI service, where is it training to develop the output. ~ New York has a new law about synthetic performers and advertising.

This was one that was lobbied by the advertising industry, that if you have an advertisement with the AI-generated performer, you need to have a disclosure conspicuously that says, this is not a human, this is an AI-generated performer. Because a lot of ad agencies and advertisers are looking at AI saying, wow, I don't need to spend \$2 million on production, I need to have my high school interns spend a half an hour just playing with ~ Sora and get me a commercial.

So there's gotta be disclosures.

Algorithmic pricing, another new one about AI. There's a lot of concern, just like in the AI and employment context, about using data for negative consequences. And there's a concern that AI platforms are using personal information to do what they call surveillance pricing, or some call it

discriminatory pricing, or other sort of targeted pricing, to give different prices for goods and services to people based on their personal information.

So New York passed a law prohibiting that. And I mentioned about the White House. So ~ President Trump, ~ he issued an executive order, which he basically said states cannot pass their own AI laws. Now firstly, I don't know how you issue an executive order that's an override state law that would violate our Constitution. And he took it a little further and he says, if states pass AI laws, we're gonna take away your subsidies for rural broadband internet access. But this was passed, so states are a little cautious right now, and that's what I mentioned about Colorado. They're worried that if they start enforcing their AI law, they're gonna be sued by the federal government. There was a Wall Street Journal article about this last month where I was talking about this, thinking that, you know,

States are still interested in regulating AI, but they're concerned they don't want to be in a battle with the administration. Last three slides I'll talk about, since we're all lawyers here, think. Lawyers need to be very careful about the use of AI. As there's probably been here, there's been a rash of cases in the United States about hallucination and attorneys submitting briefs and filings to courts with hallucinated cases or hallucinated parties or hallucinated judges.

This was the very first one that happened and it became a big issue. This is happening nonstop. And judges are getting really mad about this and they are issuing sanctions because if you go into just a regular platform like ChatGPT and say, find me a court decision about the following issue, a lot of times it gives you information that may have a real judge's name and fake parties or a wrong decision. And that's actually the worst fact pattern when it's a real judge and it's the wrong decision.

So you've got to be really careful because ~ the lawyers are doing this nonstop and they've been fined. The fines are not huge, but then you get a disciplinary hearing and it's certainly not fun. ~ In the United States, we have rules of professional conduct and they're different in each state, but this is from New York and it can apply to AI, and this is a rule that's been in place for decades and decades. A lawyer should provide competent representation to his client. This includes keeping informed of the benefits and risks of the technology the lawyer uses. So what they're saying, and the bar associations have emphasized this, that it's the lawyer's job to understand how the AI platform works. It is not acceptable to go into a court and say, I'm sorry, Judge, the AI platform made a mistake, it was not me.

It is your job to understand how it works. ~ There's been some recent cases where a defendant put information into Claude to try and help their attorney with information and the court said that was not privileged. So lawyers do need to be careful. I there are certainly great AI platforms out there to use. know, we're testing them and we're piloting them, but you need to be very careful. Like we prohibit our attorneys from using chat GPT. And.

All right, last slide. I always ask the question, has AI jumped the shark? I don't think so, but it's really getting crazy. It's like, those are my golf clubs on the left. I have AI smoke golf clubs. I have no idea if they're better than normal golf clubs, but I'm a typical gullible consumer and said, AI, these have to be better. I got to buy these. So I bought the AI smokes. And our new washing machine has an AI wash mode. I have absolutely no idea what this does.

But my socks are AI washed socks. I have no idea what that does. But this is literally on my washing machine at home. Don't know.

Well, thank you very much. I appreciate everyone coming.

Alexander Milner-Smith

Thank you for listening. hope you found Gary's insights into the U.S. privacy and AI landscape valuable as you navigate your own compliance challenges. If you did enjoy the session, please share the episode with colleagues and friends. And if you have any questions or would like to discuss how these developments might affect your organization, please do get in touch with our And we look forward to spending time with you in the rest of 2026 as our International Privacy Series continues.

Thank you.