



Podcast Transcript

The Data Stream: Episode 11 with Justin Yedor

Date: July 28, 2026

Guest: Justin Yedor, **Host:** David Sherman, Nichole Sterling

Run Time: 33:24

For questions and comments contact:



David Sherman

Partner
Philadelphia
T: +1.215.564.8380 | dsherman@bakerlaw.com



Nichole L. Sterling

Partner
New York
T: +1.212.589.4282 | nsterling@bakerlaw.com



Justin T. Yedor

Partner
Los Angeles
T: +1.310.979.8405 | jyedor@bakerlaw.com

May: Welcome to the Data Stream, the podcast that dives deep into the fast-moving currents of data, technology, and the law. BakerHostetler's Digital Assets and Data Management Practice Group brings you this series, hosted by partners David Sherman and Nichole Sterling, to explore how companies navigate the complex and often intertwined life cycle of data from privacy and cybersecurity to advertising, AI, and other emerging technologies. I'm Charlie May, and you are listening to BakerHosts.

On today's episode, LA privacy partner Justin Yedor joins the podcast to break down the realities behind cookies and the much broader tracking ecosystem companies are actually operating in today. David, Nichole, and Justin discuss what compliance really looks like beyond the cookie banner, whether consent has meaningfully improved, and where regulators are focusing attention. They also dig into implementation challenges, data sharing risks, and practical steps companies can take to better understand and manage their ad tech.

Sherman: Alright, Justin, thanks so much for joining. To start, I'm hoping for those of us, myself included, meaning the non-privacy practitioners listening, can we start with some basic concepts about, for instance, tracking technologies? So, in a business context, what is a tracking technology like? What are we talking about and why should companies care?

Yedor: Yeah, thanks, David. I'm really glad to have the chance to join you and Nichole on your awesome podcast. And I would love to start in on cookies. So, starting from the very basic level from a business perspective, cookies, pixels, other tracking technologies, these are all the things that are on your website that your marketing team is mildly obsessed with. They can actually serve a lot of different purposes.

So, everything from making sure someone can stay logged in, protecting your site against bot attacks, to supporting nice-to-have features like remembering someone's preferences on the site. They also serve many types of analytics purposes, gathering data on pages that are particularly popular, or by inverse, telling you which ones no one is visiting. And then, of course, there is a lot of attention being paid to the use of cookies and pixels and other tracking technologies when it comes to online advertising.

So one very simple example there would be if you have a visitor on a retail website and the visitor is checking out products, you need a way to record the fact that they're interested in a particular product if you want to go and advertise that product to them when they're elsewhere on the internet or perhaps if they come back to your site. So, there is a lot more to it than that. But in a nutshell, these tools serve a whole lot of different purposes. They're extremely common. And ultimately, companies should care both because they're very useful technologies, but also because they're subject to ever more intense regulation under our privacy laws.

Sterling: I'm going to jump in and ask a bit about the vocabulary question, because we talk about all sorts of things when we're really talking about tracking tech. We have a tendency still to default to cookies. And when we say cookies in 2026, are we really always talking about cookies anymore? Is that just the shorthand that we've all fallen into using for this much broader tracking ecosystem? And I know you've mentioned pixels already, but even things like fingerprinting and SDKs, server-side tracking, and all of this other stuff that really doesn't even function like a cookie anymore.

Yedor: That is a great question, Nichole. I think often we are defaulting to using cookies as shorthand for tracking technologies. A cookie actually is technically its own thing. A cookie is a small file that is stored on a user's device to remember information about that device and its interactions with a particular website. You could think about it like the, if you go into a bar and the bouncer looks at your ID and stamps your hand to indicate you're 21. And then you walk out of the bar, you still have that stamp on your hand. If you go across the street, people will see the stamp and theoretically could understand what it means if they're familiar with the bar's practices. Or if you go back in the bar again, they're going to know you're 21 because you've already had this stamp indicating that.

So, a cookie does have a technical definition of its own, and it really is different technology from something like a tracking pixel, which is actually a tiny invisible image that is on a website or sometimes inside of an e-mail, and that can record information about a user's interaction with that page. And it is different from an SDK, and it is certainly different from fingerprinting or server-side tracking. However, this is a lot of terminology, and when it comes to the privacy requirements for these technologies as well, they're all loosely very similar. We can talk about that more. But I think people default to cookies because it is a much nicer name. It is a much more fun name. And it is a lot easier to say than tracking technologies.

Sterling: I mean, it does sound much more pleasant to talk about cookies. I will say that I personally have a tendency to try to default people to tracking tech because it is the broader, more encompassing term. But again, I think that just takes us to, does that outdated label actually matter in practice as long as you're defining it however it needs to be defined.

Yedor: I think that is right. And I also do think a little bit of this is, you could talk a little bit about connotations, I guess, to the extent it matters, but cookies got a very positive connotation. We all love cookies. I mean, who doesn't like cookies? On the other hand, and by the way, I love this quaint 1990s naming convention from when this originally happened and the fact that it is still a technology that is in use today that harkens back to the earlier days of the internet. So, I think, for what it is worth, there is probably a much more positive connotation associated with the word cookie than with tracking technology, which I don't know, implies that like technology is following you around and it is keeping tabs on what you're doing. I mean, certainly that is a use of cookies. It is a use of pixels. It is not an inaccurate term. But I think in addition to the fact that cookie is easier to say in terms of how you pronounce the term, as well as the more positive connotation, I think those are maybe some of the reasons people tend to default to it.

Sterling: We can default to cookies. We can claim it is the 90s throwback. Cool attitude toward them.

Yedor: Yeah, I believe they were originally called Magic Cookies, which is even better. I mean, talk about a great name.

Sterling: Yeah, I believe that is right, actually. So, Justin, back to our point. Client comes to you and they say, they're calling you up one day, they're like, hey, Justin, we've got a banner up. So, we're good on cookies, right? Where do you start with that?

Yedor: Well, so, I mean, look, first of all, I'm always glad when companies are focused on their tracking technology. As a starting point, just making sure, having actively put up the banner, right, indicates that somebody is paying attention to this stuff. And I think that is an important component. However, I would have some questions. And that is because there is no easy solution to how you comply. And at a base level, there is no comprehensive privacy law in the U.S. that actually strictly requires a banner.

And so, if I were to hear, oh, well, we've put up a banner, so we're good, right? Some of the questions I might have following that are, well, I'd like to understand why. I'd want to know if the banner is associated with an opt-in or opt-out approach or maybe the banner is just a pop-up, and it doesn't actually include controls for cookies. Secondly, I'd want to make sure it is working. There are many ways that this technology is actually quite fragile. The technology to control cookies, pixels, other tracking technologies, it often has challenges in actually following through and making sure that trackers are blocked when you want them to be blocked and unblocked when you don't. And so, I'd want to take a look at the site and make sure it is working in accordance with how it was set up.

And then, of course, especially being lawyers, right? We always care about the language and I'd want to take a close look at what it says and make sure that the language looks good and that it is doing the most work to help the client and to inform the user about what is going to happen with tracking technologies, making sure there are clear links to additional disclosures such as the privacy policy, perhaps linking to the terms of use. It is really, if I were to hear from a client who I'm just meeting and they say, well, we recently put up this banner, I would say, great, let's talk a little bit more and learn more about the details.

Sterling: So how often do you think the banner is the least important part of this entire tracking tech compliance piece?

Yedor: It is definitely not the most important part. It is perhaps one of the more visible parts, but I would say often it is actually the least important part because a banner by itself is not particularly meaningful. The banner has to control cookies correctly. And so, I would have, in any given case where you see a banner, I think it makes sense to dig a little deeper and understand whether an opt-out or opt-in approach is being applied to confirm that the tracking technologies have been classified within the tool appropriately so that they are getting controlled when they're supposed to, making sure that it is been implemented in a way where it communicates with a tag management tool, if that is how the company is setting their tracking technologies.

I just think there is a lot more to it than the banner itself, as well as, you're asking about, is it ever the most significant piece or how often and I think there are also

a lot of questions around, well, what is the opt-out process under state privacy law? The state privacy laws, by and large, require opt-outs. And so even if there is an opt-in consent banner that pops up when the user arrives on the website and it is functioning perfectly and everything is getting blocked when it is supposed to, there is also quite a bit of additional implementation that could be needed in order to make sure that the state law opt-outs are also being respected.

Sherman: So let me chime in here for a second. So, when I think about, and as you just mentioned, we have no federal privacy law, right? So, we're looking at this patchwork of state laws. We have to acknowledge that there is a pain point that we're creating, that compliance here creates for businesses. Do we think that privacy regulation has actually made consent, meaning, I guess in the most direct sense, opt in or opt out, meaningfully better for users, or are we just creating more friction and noise than necessary without actually meaningfully improving control?

Yedor: It is a really good question. I mean, to start with, nobody likes banners. I mean, consumers generally dislike the banner. It keeps them from getting to the site. Businesses don't like them because they want people to come into the site. I'm not going to express opinion on behalf of regulators, but based on the fact that these laws, for the most part, don't require them, I'm not sure that the regulators are specifically looking for a banner. So, there is definitely a degree of this that is creation of friction. And the question is, is it worth that friction?

As I mentioned, the state privacy laws don't actually require an opt-in consent or a banner. These are really being driven by a parallel trend. And that relates to claims about website tracking technology that are based in state two-party consent wiretapping laws, like California's Invasion of Privacy Act or CIPA. And in large part, the banners that we see in the U.S. are mostly an attempt to try to reduce the number of these nuisance claims that plaintiff's counsel are filing against virtually anybody with a website. And not to go too far out on a tangent here, but the complaints generally allege something like there were non-essential tracking technologies that were set without consent. And so, if a business is to try to reduce the likelihood that they're going to see these claims, one approach is to put up a opt-in consent banner and get that consent before the tracking technologies are set.

And so there may be some effectiveness to this. There are some other strategies that can work as well, but I think that is by and large driving most of the banners that we've seen proliferate across the last couple of years on websites for U.S. consumers. And ultimately, I think it is an open question as to whether these banners are net positive or negative, either from a business standpoint or a consumer standpoint. And the devil is in the details. I mean, if it is a highly effective banner and the business stops receiving CIPA claims, well, that is certainly good for the business. And if it is well-designed and the consumer can easily accept or reject and control tracking, well, that is good for the consumer, arguably. But it certainly is a more complicated experience to just go and use the average website now versus even three or four and certainly five years ago when

you would be hard pressed to find a business in the United States that had a cookie banner.

Sterling: I think the other time we tend to see a lot of cookie banners pop up is when somebody from the compliance team went on vacation in Europe. They come back and they're like, why don't we have this banner set?

Yedor: Yeah. I'm glad you mentioned Europe, Nichole. And David, you mentioned the patchwork of state laws. I mean, look, the e-privacy directive and the GDPR, in many ways, they are still stricter on tracking technology than the U.S. state laws. On the other hand, the regulatory regime is simpler. We are dealing with many state privacy laws at this point, upwards of 20, as well as this overlay of wiretapping considerations that has nothing to do with the state comprehensive privacy laws. And so when it comes to knowing what the rules are for these technologies here, ultimately it may not be quite as strict as Europe, but it is, I think, definitely more complicated than if you look at any jurisdiction, including Europe, where there is basically a single set of rules that you could look at and say, well, to be compliant, we need to do that.

Sterling: Yeah, no, I don't disagree. I do think it is funny because we run into sometimes the people that come back from their European vacations and come up with these ideas. I have at least run into that a couple of times.

Yedor: Well, it is great. Travel is meant to open your mind.

Sterling: Yeah. I do have to ask though, because you brought up the friction and just wanting to get to the website thing. And I will say that I know I am slightly guilty of just picking the easiest path to get to a website. Do you tend to click yourself, accept all, or do you actually go in and manage your settings on a regular basis, or you just ignore the banners?

Yedor: Oh, you want to know the really guilty answer? It is that I use my BakerHostetler laptop. I click whatever is easiest, and I'm like, you know what? It is on the firm network.

Sterling: I will say that I have a tendency to, and this is where I think you do really see the friction thing, is that if I am actually presented with an accept all reject all type button situation, I will click accept or click the reject all. If it is accept all or go and manage settings, I will click accept all because going into manage the settings always requires so much scrolling and toggling. And it is just, yeah, extra effort. So yes, that is where I am.

Yedor: Yeah. And I think that is where this newer trend around equivalent choice and dark patterns comes in. And it points to the fact that none of this is as simple as just put up a banner. I mean, even when we're talking about what buttons need to appear on the banner, you have considerations around making sure that you are providing an opt-in or opt-out choice that those two require an equivalent number of clicks. But then there are also plaintiff's firms out there that have brought claims, claiming that a reject all button is misleading because it does not

in fact reject every single cookie on the website. There may be some cookies that are essential for the site to operate or that are set by service providers or data processors that don't require an opt-out. And so, the language can be really important. The buttons are important. The whole thing, it is a very delicate balance amongst all these different requirements. And ultimately, I mean, it is like poetry, right? There is more than just the few words that are on there. There is a lot that goes into how this should look and operate.

Sherman: And a big piece of this originates from a 1960s California statute designed to preclude wiretapping. Is that, am I correct about that?

Yedor: You are correct. Yeah. So, strap on your tinfoil hat and let's all pretend for a moment that the interaction with a website is actually you making a phone call to someone. CIPA is our state wiretapping law. It is an all-party consent law. And in broad strokes, plaintiffs tend to allege that tracking technology, if not set with consent, is illegally intercepting a communication between them and the website operator. And so, by putting up a banner and obtaining consent, you're a little bit taking that argument by the horns and saying, okay, well, fine, if you say that this is a phone communication and consent is required, well, we're going to use our banner to obtain consent. So that is the general idea. There is definitely more nuance to it than that. And you have to buy the premise in the first place that this 1960s telephone recording law is actually even intended to apply to cookies and pixels. But yes, that is the general concept.

Sherman: Fascinating. So, when we, I'll spare the jokes about eating magic cookies to try and understand how we get from wiretapping to tracking, but nevertheless.

Yedor: They'd hurt your stomach, anyway. If it is a magic cookie, you got to let that one be. I wouldn't eat that one.

Sherman: No, I'm with you. I'm with you. So, but it is an interesting point when we think about how, again, how laws are being, whether they're stretched, twisted, contorted, hallucinated, who knows, whatever. But when we think about the regulatory landscape today and we look at for instance, interpretations in case law under CIPA, I'm really curious to know or to think about how regulators are, where we're heading from a regulatory perspective and how regulators look at tracking and where their focus is shifting towards. Are we moving towards greater attention to issues like signal handling and global privacy control and opt-out mechanics, or are regulators still at this point really spending most of their energy on other subjects?

Yedor: No, I think the opt-outs are particularly important. So, opt-outs from so-called sales of personal information, that would be transfers of personal information to third parties where those other parties have not agreed to be a service provider or data processor under state privacy law, as well as targeted advertising. Issues around targeted advertising and sale opt-outs have been the most enforced issues under our state privacy laws. And it doesn't tend to matter too much which state we're talking about. Regulators definitely care about those.

To the question about signals layered on top of that are requirements relating to opt-out preference signals, so signals like the global privacy control header signal, which is intended to essentially indicate to a website operator that a consumer wishes to opt out the second they land on the site. So instead of having to click into the website footer and open up a consumer interface and click a toggle and opt out, the global privacy control or GPC is meant to signal that automatically. And so, the consumer saves the step of having to click to opt out.

Regulators care a lot about these issues on the mechanics of opting out, whether that is via GPC or whether that is in a process of clicking buttons. But they also then get deeper than that. I mean, that is really, that is very visible to the front end, right? Anybody who is on a public website can tell whether there are the appropriate controls there. And if you're a regulator and you're looking to see, well, are companies following our law, it is pretty easy for you to check that issue. Sometimes that is just an entry point for deeper questions about what is happening with this opt-out and is this just a front-end set of controls that don't go anywhere? But those issues on the mechanics, I think, remain pretty important. And they do come up. They come up all the time in the regulatory investigations and sweeps that our state AGs and the California Privacy Protection Agency undertake.

Sherman: So, I guess in a somewhat related sense, thinking about the level of visibility that the public has or that a regulator would have, do you think companies are underestimating just how much purview regulators now have into actual data flows and not just what is written into the policy, but what is actually happening under the hood?

Yedor: Yeah, I think that is likely the case. You can't overestimate it because when we're talking about a website, it is, I mean, it is generally open to the public. I mean, there is nothing to prevent anyone who chooses to take a look from looking at it, as well as it is as simple as a right click in Chrome or any other browser to be able to see what is happening with network transmissions, cookies, and so forth. And so, certainly, it is very visible, whatever is happening with the tracking technologies, with the consent modules that may be on the site, whether that is a banner or a pop-up cookie preference center. Basically, anyone who chooses to take a look and is willing to spend the time doing it can see whether the site is turning on or off most of these technologies in accordance with the controls that are presented. And it is also that much easier to see if there are not controls being presented in the way they should be. So, I think it is a very visible issue. I think that does have something to do with how much it has been enforced is that it is, sometimes it is just an entry point to other issues. But the reason it is an entry point is because it is so easy to see.

Sterling: So based on what you're telling us, Justin, sounds like a lot of these are really legal issues in that lawyers are advising on them regularly, but a lot of them are really these implementation problems as well. And so really when we're dealing with them, we're looking at a lot of things that have to function between legal, product marketing, et cetera. One of the things you've been really working on to

develop as a service that the firm can offer now is this Smart Cookies service. Do you want to tell us a little bit about that?

Yedor: I would love to, Nichole. I could talk about this one all day. So Smart Cookies is a better way of keeping tabs on the cookies that are on a client's website, what those cookies do, whether an opt-out is required under the state privacy laws, what the terms are that apply to a vendor relationship associated with a given cookie, and much more information. And the reason I thought it was important for us to build out this service is really multifold. There are a number of common issues that we see over and over again with implementation of cookie management systems on websites.

A couple of these really are technical. So sometimes there are issues with the blocking of cookies, either because of something like where the script is placed, or a second issue that comes up all the time is relating to communication between the cookie consent tool and the tag manager tool if there is one in use. But then the third issue we kept seeing was that within a given tool, either there were cookies that were not categorized, so meaning that the tool didn't recognize what the cookie was or under what conditions it should be turned on or turned off, or we would have clients who would come to us and they had been relying on information provided by the vendor that provides them with the cookie management tool. And the classifications weren't really taking account of the legal requirements.

So, the classifications might loosely relate to what the cookie does. Is it essential for the site to operate? Is it a nice to have feature that is supported by the cookie? Or is it used for advertising? But they weren't accounting for the legal question that is really significant under U.S. state law about, is it a sale? What do the terms say with this party? And can we appropriately classify this particular relationship as one with a service provider or a processor? Or do we need to provide an opt-out for that reason? That is a legal question, and it is based on interpretation of a contract, and that is something we as a law firm that focuses on privacy and data security, we're well equipped to do. But I also noticed another trend when we did this. And that is that the vast majority of companies are relying on vendors' standard terms and data processing addenda in order to facilitate the relationship that they have for tracking technologies on their site.

And so, we kept seeing the same vendors over and over again. And so Smart Cookies is really a smarter way of serving our clients in this space. It is a low-cost, fixed-fee service where we leverage our institutional knowledge about these terms, as well as information about what these cookies are. We now maintain a comprehensive database of roughly 1,300 different cookies and all of the associated information, so that when we have a new client that comes to us, we can very quickly scan their site, append the information that we already have about the cookies that are on the site, our attorneys review it before we deliver a report to the client, and if we're missing anything or if there are updates needed, we use this process to fill in those gaps. And then we also maintain the information internally. So, this gets better every time we use it. It is constantly kept up to date. And I think it is a key component of a cookie compliance

program so that clients not only know what is on their website, but they know what to do with these things.

Sherman: Justin, before we wrap, I have to ask a non-privacy question. I understand you've taken up skateboarding with your son, which feels fun, maybe a little dangerous, but awesome. Have you found that sharing a hobby like that changes how you experience something like a solo hobby?

Yedor: Oh my gosh. Okay, so it is definitely dangerous. I'm a battered old man over here, David.

Sherman: Wrist guards, man. Wrist guards.

Yedor: So yes, I have recently taken up skateboarding with my son. The rumors are true. This year I visited a skate park for the first time. I've dropped in on a ramp with him. I'm doing ollies, which is where you go up in the air on your skateboard. And this is different from what I think the experience was like when I was, I don't know, 12, the last time I was on a skateboard.

But here is what is great about this. I actually, I love it so much because my son, he is seven and we are learning this at the same time. And, as a parent, there are lots of things that you teach your kids and you of course want to share all the things that you've learned and your experience in doing these things. And that includes other hobbies that I do with my son. But I love that this one is new and we're both learning it together. And there is something really fun and special about, we're at the same level. We are equivalent level skateboarders. This is not like, this is not like dad is going to teach you, right? Because I don't actually know. Instead, we are developing together and we're learning the terminology and we're dropping in on a big ramp is pretty scary for both of us. And we're there together.

So yeah, the rumors are true. If you see me with bandages or I hobble in on crutches, it is going to be pretty obvious why that is happening because I don't have the rubbery body of a seven-year-old and I don't bounce back quite as quickly as he does.

Sherman: Well, I admire it and wish you all the best. As I said, I would like bubble wrap myself before I even tried these days. Although I have to say there was a time and maybe we'll find a photo and show notes or something with, at the point where I could chew on my hair and definitely had a couple inline skating years, but That was to your point.

Yedor: I can see it. Also a big believer in safety equipment.

Sherman: Oh yeah.

Yedor: I got my knee pads, I got my elbow pads, I got my helmet, I got the whole old man setup.

Sherman: Hey, safety first, man. That is, dude, it is everything.

Yedor: Absolutely. Yeah. It is good to take risks, but you got to do it with appropriate caution.

Sherman: You know what? And to that end, that is probably the perfect segue to the final question I have, which is what is the one thing that you would tell all in-house counsel to pay attention to these days from a safety first, risk aware, whatever.

Yedor: Oh my gosh. So, there is so much, and privacy is, in some ways, it has become such a complicated field because there are so many new laws, things are changing so rapidly. I mean, I always come back to the core, I think, which is understanding what you're collecting and why. And we could apply that to tracking technologies and say, well, you should know what technologies are on your website and what they do and why you're using them. But I think it is a broader point. And I think if you're going to anchor to just one thing in privacy, I think knowing your data is still the key that unlocks a lot of the answers on what you need to do from a compliance standpoint, from a best practice standpoint, and sometimes can help your product teams too. So, I'm going to go with that, David. I'm going to say know your data is probably the top thing to pay attention to and just making sure that you really have your hands around exactly what you're collecting and what you're doing with it.

Sterling: I feel like that is the answer to pretty much everything, because I feel like when we talk to people who are on David's side of the house dealing with the cybersecurity side, that is what they always say as well.

Yedor: Yeah, absolutely.

Sherman: I couldn't agree more.

Sterling: Thank you for joining us, Justin. It's been a really fun conversation and I enjoyed hearing more about Smart Cookies, although I've heard about it quite a bit already, but I feel like I learn more about it every time we talk.

Yedor: Well, thanks, Nichole. Thanks, David. I mean, yeah, I can't stop talking about it. I tell everyone in the skate park all about it.

Sherman: That is awesome. And they should know. The world is a better place for it. So can't wait to learn more about it and see how Smart Cookies evolves too.

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

Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.