Business Better (Season 3, Episode 4): Cyber Adviser – 2023 Preview for Privacy and Data Security

Speakers: Phil Yannella and Greg Szewczyk

Steve Burkhart:

Welcome to Business Better, a podcast designed to help businesses navigate the new norm. I'm your host, Steve Burkhart. After a long career in global consumer products company, BIC, where I served as Vice President of Administration, General Counsel and Secretary, I'm now Of Counsel in the Litigation Department of Ballard Spahr, the law firm of clients across industries and throughout the country.

This episode is part of our Cyber Advisor Series where we discuss emerging issues in the world of data privacy and security. 2022 proved to be an historic year for privacy and data security. In 2023, it's likely to follow suit. With privacy compliance deadlines looming under three state laws, a surge in data privacy litigation, new federal cyber regulations, new state laws governing children's data, and new EU legislation regulating digital services, privacy lawyers will be busy this year. We discuss the main privacy issues that are likely to dominate headlines in 2023. Participating in this discussion are Phil Yannella and Greg Szewczyk, Co-Leaders of Ballard Spahr's Privacy and Data Security Group.

Phil Yannella:

Hi, everyone and welcome to Ballard Spahr's monthly webcast of emerging issues in the world of data privacy and security. This is our first webcast of 2023 and we'll be focusing on what privacy professionals can expect to be the hot issues for the upcoming year. My name is Phil Yannella. I'm a Litigator in Ballard Spahr's Philadelphia office, and I am the Co-Chair of the Privacy and Data Security Group. I'm joined today by Greg Szewczyk, who is also a Litigator based in Denver. He's a Co-Chair of the Privacy and Data Security Group here at Ballard.

Last year was a very busy year in the world of data privacy and security, and we expect that 2023 will also be quite busy. Here's the outline for our discussion today. We'll begin with an introduction, that I just completed. Greg will then kick things off with the discussion of the new state privacy laws coming online in 2023, specifically the Colorado and Utah and Connecticut data privacy laws.

I'll then address litigation trends that we saw developing in 2022 and that we think will continue this year, such as Meta Pixel and chatbot litigation. Greg will then discuss the many new cyber laws and regulations that will become final either later this year or 2024, such as proposed SEC cyber reporting regulations, the new GLBA Safeguards Rule, and breach reporting for critical infrastructure.

I'll then turn to a quick discussion about what we can expect to be going on in the European Union in 2023, and then I'll finish it up with a discussion of ad tech. There are a number of new laws that come online this year that will mandate opt-outs for targeted advertising, and we'll talk about what all of that means for companies.

So let's dive right in with the discussion of how companies will comply with the three new state privacy laws that are going to come effective this year. Greg, want to take it away?

Greg Szewczyk:

Thanks, Phil. As Phil just mentioned, we have three new laws that are going to be coming online later this year, and that's Colorado, Connecticut, and Utah. We also had Virginia and the replacement for the CCPA come online earlier this year already. So we're now facing a world where we have five different state privacy laws that will be in play for some companies.

Rather than go through and try to explain each of these laws in detail, what I'm going to do today is try to hit some main trends that I think we're going to see develop over 2023. And the first one is going to be a continued focus on analytics. And what we're talking about there are the various different cookies, pixels, web beacons, and other tools that companies put on websites and mobile apps to both use them for marketing purposes but also for site analytic purposes.

The focus on analytics is something that we saw pretty uniformly last year. We saw the FTC announce some preliminary rulemaking with respect to what it calls commercial surveillance, which is essentially just the analytics that we're discussing. And we saw the California Attorney General's first public enforcement action against Sephora focus on this as well.

And what I have up here on the screen is one of the more notable allegations made in that late 2022 complaint, which is that according to the California Attorney General, both the trade of personal information for analytics and the trade of personal information for an advertising option constitutes a sale under the CCPA.

Now, Sephora settled this action last year, and through last year we had a cure period for the CCPA. So although the complaint stated that common analytical tools constitute sales, we didn't find out exactly which analytical tools constitute a sale because there really wasn't the incentive for companies to fight it. What we expect to see in 2023 is as that cure period goes away, we expect to see some litigation coming through to actually provide some clarity as to which analytical tools actually require an opt-out as a sale or even a share.

Where this will get interesting is if the analytics provider is a service provider under the CCPA, then it would not constitute as a sale or a share by definition alone. There has been some limited litigation with respect largely in the wiretap context or in the BIPA context as to whether or not it is a service provider. Certain types of tools are pursuant to a service provider arrangement. But it's something that really has not been in the courts that much yet. So we expect to see that is one of the more prominent areas that's going to continue to develop in 2023.

And as a note on that, already this year we saw an enforcement sweep late in January by the California Attorney General applying this same concept in the mobile app context. So I think already we've seen that this focus is going to continue and companies should be both preparing right now to comply and stay off the radar of the regulators, but also to pay attention to the litigation and the enforcement actions that are coming out because they may allow companies to take less of a cautious approach, as we see that some of these commonly used tools might be service providers rather than sales to third parties. And Phil, if you could go to the next slide, please.

Another area of compliance that I think is going to be very important in 2023 is privacy policies that comply with these five different states. The only two states that are going to have regulations in 2023 are California and Colorado, and there's been a big issue as to how interoperable these two laws privacy policies requirements will be. We have posted a full post on the blog dedicated to this, so if you're really interested in digging in, I'd suggest you go read.

But essentially, Colorado is taking a slightly different approach than California. Under the CCPA and as carried through to the CPRA, it's really an information-driven approach. Companies have to disclose what type of information they collect and then how they use it and what they do with that information. Colorado has had an evolving set of rules on this, but fundamentally it is a purpose-driven approach. It relates to the purpose for which a set of information is collected, and then there need to be disclosures related to each specific purpose.

And maybe the analogy that I've heard the attorney general give before is think about providing your name and email address to a company. If you provide it for the purpose of signing up for a newsletter or to receive marketing materials, you might have one set of expectations as to how that data will be shared, but if you provide the same name and email address to lodge a customer complaint, you might have a different set of expectations as to how that's shared and used for marketing purposes. So that's really the underlying difference.

Where we have seen a lot of discussion and where things could get very interesting is Colorado has revised its rules over the course of the rulemaking process to try to build in some level of interoperability with the existing California or other framework. And we've seen a lot of commentators essentially state summarily that the California process will be, or the California chart, as we frequently see, will be sufficient for Colorado purposes.

But if you look at the rules closely, I think you'll see that each of these disclosures, although it does not need to be organized by purpose and it can be organized by the category of information, you still need to make the disclosures based on the specific purpose for which the data is provided.

So thinking of the California disclosure that starts with just the identifiers, you wouldn't be able to make all of these disclosures just tied off of that one category of information. You need to end up subdividing the chart further on. And you also may not be able to satisfy the rule listed up here in 1A(i) as to providing a level of detail about what type of personal data

is being processed because the categories that are listed under the California law are often just listed as the statutory categories, which are extremely broad in some cases and may not give this kind of granular level of detail that's required.

So I think what we're going to see in 2023 is we'll probably start by seeing companies take some different approaches. Some may just on a first page of Google see that they think that they're fully interoperable and rely on the California chart to try to comply with Colorado. We'll see other companies try to apply the rule a little more faithfully and under the specific words and what's really required. And we'll see some divergence in how companies try to comply.

When any enforcement might come down or when there might be other kinds of guidance come out, I don't know. But I think eventually, if the final Colorado rules follow what they are right now, we're going to see diverging approaches to privacy policies, one following the California model and one following the Colorado model.

Virginia, Connecticut, and Utah aren't going to have rules come out this year, but their laws more closely align with the Colorado law than they do with the California law. So it will likely be that we'll see companies kind of apply the Colorado model as a more general template rather than the California template. And another reason for that is just vernacular and terminology used in the California law doesn't necessarily mesh up with others. And I'm specifically thinking of words like share, which under the California law has a very specific meaning related to disclosing for the purpose of cross-contextual behavioral advertising, which is not how most people would use the word share, and it's not even how it's used in other California laws such as the California Privacy Policy Law.

So I think 2023 is going to be a year where we're going to see diverging privacy policies across domestic policies. And Phil, if you could go to the next slide, please.

I think another area where we're going to see emerging as a big issue in state compliance is data minimization. All of the 2023 privacy laws have some form of expressed data minimization requirement, and it's something that is addressed in the rules for both California and Colorado to a degree. Where I think it will get interesting is how this privacy side of a statutory and regulatory requirement gets carried over into other areas. We already started to see that happen at the end of 2022, and what I'm thinking of right now is the FTC settlement with Drizly, which is in the data breach context.

Now, in many ways, the Drizly data breach was a fairly standard data breach and it was a fairly standard settlement with the FTC, but where things got a little different is the FTC brought a specific claim for failure to minimize data, essentially under the thought that you can't lose what you don't have. And that's kind of a new approach.

So we expect this to be something that becomes more and more prominent in the state regulatory context, especially if a company suffers a data breach, it might expect to see some compliance actions against it for failure to comply with the state privacy laws as well.

So I think this is going to be an area that we continue to see evolve, it's going to be an area that we continue to see a focus on, and companies are going to have to not only minimize data in a way that they may not have been doing before, but they're going to need to find a way to document it, both as a policy matter and as an execution matter so that they can show their compliance if they're ever under the regulatory scope. With that, I'll turn it over to Phil to talk a little bit about litigation trends.

Phil Yannella:

All right. Thanks, Greg. Data privacy litigation has been trending upwards for many years, and we expect this trend is going to continue in 2023. One of the more surprising trends in 2022 is a resurgence in class action litigation under the Video Privacy Protection Act. This rarely enforced law was passed in the late 80s in the wake of congressional outrage over media reports of Judge Bork's video rental history which emerged during his Supreme Court confirmation hearing.

The law has a very specific purpose. It requires consumer consent for the disclosure by videotape service providers of a consumer's video viewing history, and it provides for liquidated damages for a violation of the law. For decades, plaintiff's attorneys have been trying with limited success to apply this antiquated law to internet streaming activities.

In 2022, a new variant of VPPA litigation emerged. The new claims focused on website usage of Meta Pixel, a tracking cookie that enables the sharing of a consumer's website activity with Meta. The typical VPPA complaint alleges that a website that shows videos shares the plaintiff's video viewing history without consent with Meta via the pixel. Now, as many websites have

thousands of daily visitors accessing videos, the potential statutory damages for a class of website subscribers can quickly reach seven or even eight figures.

There have been at least 70 VPPA class actions filed in the last eight months. Media and news organizations which often embed videos on their websites have been a particular target for plaintiff's lawyers. Most of the recent class actions are still in a pleading stage and only a few courts have thus far ruled on motions to dismiss. Until there is a clear consensus among federal courts on the viability of these claims, we can expect to see continued stream of VPPA litigation in 2023 and maybe beyond.

The use of Meta Pixel also gave rise in 2022 to a number of class action lawsuits under state wiretap claims. Plaintiffs in these cases allege that Meta Pixel allows Meta to intercept consumer communications with a website while in transit. A major driver for these claims are favorable rulings by the Third and the Ninth Circuits, both of which permitted wiretap claims to go forward against companies based on their usage of certain kinds of website tools.

At least 60 wiretap class actions have been filed since August of 2022 in the states. Many of these claims focus on Meta Pixel, recently however, plaintiff's lawyers have been asserting claims based on usage of chatbot, session replay software, and insurance quote tools. An even more recent variant of wiretap litigation focuses on hospital's alleged use of Meta Pixel on patient portals, which plaintiffs allege results in the unauthorized sharing of EPHI with Meta.

As with VPPA litigation, most of these wiretap class actions are still in the pleading stage, but given the broad way in which courts are reading wiretap laws, it is highly likely that we will continue to see a steady stream of wiretap class actions in 2023. We also expect that plaintiffs will expand the focus of these allegations to include other pixels other than Meta Pixel, other tracking cookies and embedded website technologies operated by third parties.

For at least half a dozen years, the number of data breach class actions filed each year has slowly been trending upwards, and we again expect that trend to continue in 2023. Now, this trend is somewhat surprising in the wake of TransUnion versus Ramirez in which the Supreme Court held that plaintiffs could not establish federal standing for monetary damages based on the mere risk of future harm.

Although courts within some circuits have dismissed punitive breach class actions based on TransUnion, a number of courts have held that breach plaintiffs do have federal standing to proceed with their claims. One line of reasoning used by these courts is that the breach itself gives rise to a present harm, such as emotional distress, that is separate from the risk of future harm. Plaintiff's lawyers have also been very adept at finding plaintiffs who have suffered out-of-pocket expenses arising from a data breach.

Given the huge number of breaches that occur every year in the US, we can confidently expect that data breach class actions will continue to trend upwards this year.

Last but not least, BIPA. 2023 could be a truly momentous year for BIPA litigation, which is already one of the most common litigations, privacy litigations in the country. We're waiting on some key rulings from the Illinois Supreme Court on significant issues that could expand or perhaps constrict BIPA litigation.

One recent ruling already came down with the Illinois Supreme Court finding a five-year statute of limitations applies to BIPA claims as opposed to a one-year statute that have been applied to certain kinds of claims. This is obviously going to increase the number of filings that we can expect to see. The Illinois Supreme Court will also address in this coming year whether certain BIPA claims accrue only once upon the initial collection of biometric information or whether disclosure of biometric information occurs each time a company collects or discloses biometric information. That could have another significant impact on litigation.

So let's turn to predicting the next kinds of privacy litigation. Privacy litigation in the past has often tracked issues of federal regulatory concern. And now using federal regulation as a guide to privacy litigation, here's some areas where we might see increased litigation in 2023.

Children's data. Over the past several years, the FTC has been very focused on children's data. The recent settlement with Epic Games for 245 million relating to deceptive practices to collect or share children's data in game suggests that we're going to start to see some privacy class actions that are focused as well on children's data.

Data minimization. Greg talked about this already. It's been another focus of the FTC. The Drizly consent decree that Greg just discussed requires that company's delete, or that Drizly delete unnecessary data. I would look for breach class actions that will start to include allegations that defendants fail to delete consumer data in a timely manner.

Data dark patterns. This is a focus not only the FTC but state regulators as well. The CPRA regulations, for example, include very detailed examples of illegal dark patterns that may steer consumers into making choices that they otherwise would not have made.

Earlier in 2022, we saw the District of Columbia bring an action against Google for its alleged use of dark patterns in connection with location tracking. It would not be surprising at all to see plaintiff's lawyers in 2023 begin to assert claims that certain online disclosures and consenting mechanisms wrongfully misled consumers into purchasing decisions.

Artificial intelligence may be the holy grail of privacy litigation. Artificial intelligence contains two key hallmarks that plaintiff's lawyers love. First of all, it operates largely in the dark surreptitiously, to borrow a favorite allegation, and it also has the potential to negatively impact consumers.

Thus far, there has not been much AI litigation and there's not been really a lot of granular regulation concerning AI, but that may be changing. Many of the new state privacy laws that we've already discussed seek to regulate the usage of AI. And we expect to see regulations in California and Colorado that may develop some legal guardrails. These regulations may also provide greater transparency around the operation of certain AI tools and provide the legal basis for consumer fraud or even UDAP claims.

So that's what we expect to see in 2023 for litigation. Let me turn it back over to Greg.

Greg Szewczyk:

Thanks, Phil. The first area I'm going to talk about for new cybersecurity laws and regulations is the GLBA's updated Safeguards Rule. So the Safeguards Rule under the GLBA which regulates financial institutions has for many years been fairly generic. In December of 2021, the FTC issued its updated rules that have much more specificity.

Most of the real meat around these rules was set to go into effect in December of 2022, but in the fall of last year, the FTC announced a six-month extension until June of 2023. So what we're seeing right now is after companies got done with their CPRA push for financial institutions, they're now really cracking down on trying to make sure that they can meet the Safeguards Rule June 9th effective date.

The specific requirements of the updated Safeguards Rule are fairly expansive and they come in a lot of detail. This is a pretty big departure from the framework that most financial institutions were used to in the past. Many financial institutions will have a GLBA policy or a GLBA compliance policy that in many ways just mirrors the requirements of the old safeguards. Those types of policies will just not be sufficient. And to comply with the updated rule, there will need to be execution on some pretty significant operational changes.

Some of these are designed towards better corporate governments and more accountability, such as designating a qualified individual to oversee the program. Others are more in line with what companies were already doing, but requires things to be in writing, such as with a risk assessment, an annual risk assessment that has specific components and a written incident response plan that also has specific components.

But where we've seen companies have the biggest difficulties are some of the specific safeguards that at first sound like they might not be quite as big of a deal, but when you actually start cracking down into how to execute them across organization wide, it gets much more difficult. And the two that we've heard the most about are multi-factor authentication or MFA and encryption for data in transit and at rest. These are both areas that simply require technical changes and can be a big issue both within a company from a technical standpoint and from a user experience standpoint.

On the MFA, I think it's worth noting that when you look at the FTC's comments and responses to comments that it received, it's clear that the MFA requirement is supposed to occur every time anyone accesses non-public personal information that's regulated by the GLBA. This would apply to both consumers and to employees. And so if you just think about putting that through in the context of an organization, it can lead to employee dissatisfaction with how much more time it may take to log onto a system and the same way for consumers when they're logging on.

The encryption aspect is also something that we've heard a lot of clients saying it is difficult. Figuring out how to make sure that all MPI is encrypted both in transit and at rest is not so simple and it can require some real operational technical changes. So we expect to see companies working for the first half of 2023 really trying to make sure that they can hit their compliance deadline.

We also expect to see a lot of these requirements get pushed down to vendors. So beyond just financial institutions, we expect to see this start to be something that percolates through the vendor world and have major impacts on both DPAs that are attached to vendor contracts from the legal side of things and the requirements that are pushed on a technical side down to the vendors across various different industries, so not just in the financial realm.

We also expect to see any time that we see one of these types of very prominent cybersecurity rules come out, it's necessarily going to impact to some degree the definition of reasonable that is governing companies outside of these specifically regulated industries. Pretty much every state except for Massachusetts that has a data security law applies a reasonableness standard. Having this type of a specific Safeguards Rule that applies to so many financial institutions will inevitably impact the argument as to what constitutes reasonable for purposes of those state law compliance that impacts so many more companies outside of the industry.

So that's something that we expect to see start being teased out both through data breach litigation and other types of arguments that we see, whether from the regulatory or litigation standpoint. So keep an eye on that as you're trying to develop what constitutes reasonable for reasonable security guards. Phil, if we could go to the next slide, please.

Another big area to watch on the cybersecurity regulatory side is the SEC's proposed cybersecurity rules. These rules were issued last year in March. If they're finalized in 2023 in their current form, the reporting requirements are going to have a significant impact on how public companies manage and disclose both their cybersecurity program and their cybersecurity incidents.

One of the biggest areas would have the biggest significant impacts on companies is the first point up here. It would be the requirement to report a material cybersecurity incident on an 8-K within four business days of the event.

Now, obviously, when you are in the midst of responding to a security incident, the quick timelines are always difficult. And it's hard enough when it's going to be going to a supervisory authority or an attorney general, but it's not going to be public. Reporting it on a public filing within four business days is going to not just be very difficult from a compliance standpoint, but it's likely going to throw up the potential lightning rod for class action litigation from shareholders. So on top of the investigation, companies are going to have to start really preparing for that litigation front right off the bat.

That type of an exposure's also could potentially have some impacts on things like is the breach response investigation subject to attorney-client privilege or work product? We've seen the court's trending against finding privilege or work product over the last few years, but if the public reporting is done within four business days, that could arguably change the position of whether or not litigation is reasonably anticipated, and therefore extend that work product protection across the investigation.

Another area that this is going to impact is how incident response is staffed from the legal standpoint. As it sits now, you essentially have your breach response counsel who's kind of running the investigation and preparing to provide notices. A lot of times that breach response counsel might not be the best position to also prepare your 8-K. You're going to want to work with your securities attorney. But you're also going to want to work with a securities attorney or another privacy or data security expert because there is a growing body of case law and enforcement actions out there about improper reporting and misleading reporting. So the specific disclosures are going to be very important and how you're going to staff those incident response is going to be very important.

Another area that the proposed cybersecurity rules would really change things is describing the board's oversight and expertise in cybersecurity risk and risk management. So as part of public company's disclosures, they're going to have to explain the board's expertise in the area of cybersecurity. The makeup of boards and how you select who is going to be on the board will likely change.

Companies are also going to have to disclose their risk management and their strategies, which again, is going to lead to the need to have better documented from both not just the technical side, but from the legal side to be able to back up and ensure that your disclosures are accurate. It's also going to probably weigh in favor of having not just your securities counsel involved, but also your privacy and data security counsel involved to make sure that these statements are accurate and not misleading.

And with that, I'll turn it over to Phil to talk about some happenings that are going to go on in the EU.

Phil Yannella:

All right. Thanks, Greg. So looking across the pond, 2023 is likely to be another year of large fines for US tech companies operating in Europe. In addition to the more traditional actions that have been brought against tech companies under the GDPR, operators of online platforms, hosting services, and providers of network infrastructure are also going to have to comply with the requirements of the EU Digital Services Act, which is a new law that just came online last year.

The requirements of this act vary depending on the size and business practice of an organization, but they generally include new transparency and disclosure requirements, as well as new controls for the dissemination of illegal content. With fines reaching as high as 6% of annual worldwide turnover, large US tech companies are likely to be a continuing lightning rod for new enforcement actions in the EU.

In somewhat brighter news in 2023, we may see a finalized US adequacy decision through an updated version of the Privacy Shield Framework. While the new framework will certainly be subject to challenge, it was specifically designed to avoid being invalidated under a Schrems III type analysis. Assuming a best case scenario, we may see a finalized framework, an adequacy decision in the next six to eight months. And further, in the event of an EU-US adequacy determination, the UK-US determination would likely follow shortly thereafter. So if the Privacy Shield comes into play, again that will provide a new mechanism for US companies to begin moving data from the EU to the US.

Over the last few years, since Schrems II, companies have been relying heavily on standard contractual clauses, which anyone's had to deal with them knows that it can be real compliance nightmare. So the Privacy Shield could offer a new mechanism for bringing data into the US that will be a lot easier to comply with.

Let's turn lastly to ad tech. This coming year is likely to be an active year for ad tech. All of the new state privacy laws, certainly the California law and the Colorado law that we've talked about in depth this afternoon, they all mandate opt-outs for behavioral advertising. That is going to make cookie management tools almost a virtual requirement for companies.

Lots of companies have been working to operationalize this by January 1st of 2023 to deal with the new CPRA regulations. Lots of companies still don't have opt-out tools in place. I would expect that for the next really five months, you're going to see lots of companies start to put those cookie management tools in place because, again, it's really going to become a requirement for pretty much any company that's got any kind of significant online presence.

Another big issue in the coming year will be Google, dealing with the announcement from Google that it's moving towards eliminating cookie tracking in Chrome. That's been pushed back a little bit, but currently the elimination of cookies in Chrome will begin mid-year. So it's likely we're going to start to see a shift towards more contextual advertising for companies that are looking for ways to access their customers.

While it's unlikely the cookie is going to disappear entirely, we may see it become irrelevant as replacement forms of tracking become the norm. And of course, as those new forms of tracking come into play, we'll have to see how privacy regulators view those.

In the meantime, companies should be cognizant of their tracking activities, and those that continue to engage and target advertising will need to incorporate opt-out mechanisms into their business practices or incorporate alternative tracking technologies to satisfy advertisers and applicable legal standards.

So that brings us to the close of the webcast this afternoon. Before we leave, one last word. In addition to speaking and blogging about cyber litigation, we've written a book on it. It's called Cyber Litigation. It's published by Thomson Reuters. And it covers a wide range of data breach, data privacy, and digital rights litigation, everything from retail data breach litigation to online tracking litigation to website accessibility claims. Check it out. It's available at the URL on this slide.

Thanks for joining us today, and we'll talk again next month.

Steve Burkhart:

Thanks again to Phil Yannella and Greg Szewczyk. Make sure to visit our website, www.ballardspahr.com where you can find the latest news and guidance from our attorneys. Subscribe to the show in Apple Podcasts, Google Play, Spotify, or your

favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.