Porzio Perspectives: Data Privacy & Cybersecurity - Part 1

March 26, 2024

By: Gary Fellner, Alfred Brunetti

In today's digital age, data privacy and cybersecurity have emerged as hot topic issues, sparking crucial conversations and legal scrutiny.

In a candid dialogue, Litigation Principal Gary Fellner and Data Privacy Principal Alfred (Fred) Brunetti explore the changing and important topics of data privacy and cybersecurity.

This first 30-minute episode discusses data privacy, citing some of the larger cases like Apple's refusal to unlock an iPhone for the FBI, and emphasizes the need for proactive policy development amidst the rise of nationwide state privacy laws and governmental enforcement proceedings. The discussion provides insights for businesses navigating through digital privacy obligations, including creating appropriate policies.

Stay tuned for part two, where they'll delve deeper into cybersecurity issues, offering strategies to help businesses protect against cybersecurity breaches.

Listen to the Recording

A transcript of the audio recording is included below for your convenience.

Transcript

Gary Fellner: Good morning. My name is Gary Fellner. I'm a principal of the law firm of Porzio, Bromberg & Newman, and head the commercial litigation department in Porzio's New York City office.

I'm here today with my colleague and partner, Alfred Brunetti, who is better known by friends and colleagues as Fred Brunetti. Fred is an attorney certified by the International Association of Privacy Professionals and specializes in data privacy. Many issues have recently arisen in this growing field of the law, and a lot has been written about it. Because there's so much out there on this relevant topic, it can get quite confusing.

So Fred and I are going to have a conversation today which is designed to help remove some of that confusion. There's much to cover, so we'll probably wind up doing this in two parts. Today's session is going to focus on data privacy, and we'll pick it up in a couple of weeks and finish off with cybersecurity and data breaches, which we'll discuss at that time.

Fred, good morning.

Fred Brunetti: Good morning, Gary, How are you doing?

Gary Fellner: Good, good. Thanks for coming in and spending some time with me. I want to begin our discussion with these two things that I just mentioned, which are data privacy and cybersecurity.

As I understand it, those things are very much related, but they're also quite distinct. Can you clarify?

Fred Brunetti: Yes, sure. So data privacy and cybersecurity, of course, are the cousins that are always kind of mentioned in the same breath. You really can't have one without the other. But they are distinct.

So data privacy typically is the discipline that focuses on how the data you're interested in is being collected and maintained. Cybersecurity is those measures that make sure that the data that you've collected and are maintaining is only maintained and kept in the way that you've directed. So cybersecurity is the walls that kind of make sure that the data doesn't leave where it's supposed to be.

Gary Fellner: So it's kind of like two sides of the same coin. We don't want certain information getting out. And on the other hand, we don't want people getting it.

Fred Brunetti: Exactly. And it'd be pointless, right, To have one without the other. Why am I taking money into a bank if there's a window open that someone could take the money right back out? Same kind of principle.

Gary Fellner: So, Fred, when we talk about data, let's just start at the very basic premise here of what we're talking about. I mean, when anybody goes on a computer these days or phone or any electronic device, there's going to be some sort of tracking of the information and a data trail. But data privacy isn't directed exclusively to data generally. It's limited to certain types of data. Is that correct?

Fred Brunetti: Right, right. So personal data, personal information, and personally identifiable information are all different terms that are used by different regulatory schemes that are out there. But at its heart, it's information that's used to either identify or enable someone to be identified as an individual.

So you, Gary, go on a website if there's a way to track that your IP address went to a particular website and either by individually just that one piece of information or by taking that one piece of information and layering on top of it other information that's available about you. If we're able to track it back to that visit being done by you Gary, that would in a general sense be determined to be personal information that could identify you.

Gary Fellner: That sounds like a lot of information.

Fred Brunetti: Yeah. Well, that's the thing, right? The more information that's out there in the world about you, the larger your profile can be and the more layers can be built upon it to more specifically drill down and drill down and figure out what you are, who you are, what your practices are, what your likes and dislikes are.

Gary Fellner: So when we talk about data privacy, people I think, tend to think that, “OK, we got to be careful about my Social Security number, my date of birth, my health information.” But you're saying, no, it's much broader than that.

Fred Brunetti: Sure. And it's, it's a risk tolerance for you as an individual, right? Like, absolutely everybody, no question about it, should not want their personal health information, their Social Security number, or their banking account numbers. That's information that you don't want to be shared with someone unless you're purposely doing it.

The other aspect of data privacy though, is in the largest sense, what we deal with ad tech and the way things are sold and shared in the online ad industry is that you might not go onto a website and punch in your Social Security number, right, but you might go to a website and click around it for a while. And the policies of that particular website might be that, hey, listen, every single person who comes onto our website, we're going to analyze what website they've been to prior. And we're going to analyze what website they're going to next because we're going to stick a tracker on them. And that tracker is going to allow us to build a profile. Some people like that. Some people don't like it.

It might make it easier for your shopping, right? Because the next time you go to look for another pair of sneakers at another store, that ad might pop up and say, hey, we have a sale on the kind of sneakers you like. Some people don't like that. They don't like the idea of being tracked or traced around unless they're aware of it.

Gary Fellner: But the idea, I guess, is to let people know.

Fred Brunetti: 100%. Transparency is always the touchstone, no doubt.

Gary Fellner: Well, that brings us to a gentleman by the name of Steve Jobs who pretty much foresaw that this was going to be a hot area, and he summarized it very succinctly. We have a sound clip from 2010 where Steve Jobs is saying the following:

[Steve Jobs Audio] Privacy means people know what they're signing up for. In plain English, and repeatedly. That's what it means. I'm an optimist. I believe people are smart and some people want to share more data than other people do. Ask them. Ask them every time. Make them tell you to stop asking them if they get tired of your asking. Let them know precisely what you're going to do with their data.

Gary Fellner: So that was Steve Jobs in 2010. Here we are in 2024 and the world is just starting to come around and adopt what he was saying and enforce the rights that seem pretty fundamental. Apple is certainly no stranger to privacy issues. I know there was a case that came to mind in 2015 or 2016 when the FBI took the suspect's iPhone and they wanted it unlocked and Apple refused. That went to litigation, didn't it?

Fred Brunetti: It did. Yeah, horrible shooting that took place back in San Bernardino, CA, where 14 people were killed. And to condense it down, essentially what the FBI was looking for at the end of the day was they wanted to be able to access the information in the shooter's, the defendant's cell phone. Apple had given essentially the information that it had, but it didn't have access to the actual phone itself. It couldn't crack the phone itself. So what the FBI was looking to have Apple do was to create a tool to backdoor in and be able to access the cell phone.

And that you're right, turned into quite a bit of litigation where Apple took the position of saying we're not going to create that tool. Because when you sign up for an iPhone and you purchase an iPhone, these are the terms and conditions. The terms, the conditions are the only person who's ever going to be able to access it with your password is you.

And I think it was a two-part concern. One is the notice and consent issues of saying this is how the product was established and put into the market. But two, I think probably a more pragmatic aspect of it was Apple was saying we can't trust that the tool that we're going to create to do this is going to remain a one-off because God forbid it becomes available on the dark web or other places where it gets misused by authorities. We can't allow that to happen to our product because it's so widespread and so widely used. So I think that was essentially why they were at loggerhead.

Gary Fellner: And ultimately, as I understand it, Apple refused to produce that type of software that would theoretically be very helpful in criminal investigations and ultimately I think the government wound up getting the information that they sought so the matter was dropped.

Fred Brunetti: You're right. It came to light unfortunately with another shooting a few years later where similar issues came up just as you said they wanted access to the phone. Apple continued to refuse and the FBI and its professionals and experts were able to find a way in without the help of Apple.

Gary Fellner: So Apple you know true to Steve Jobs's vision stood its ground and said no, we value privacy and we're not going to see to the government's demands. So that was an earlier case and it shows that privacy was taken very seriously back then. Now, I know that there's a lot of litigation out there, particularly class actions where there are data breaches and we're not going be talking about data breaches, as I said earlier, talking about the data privacy rights. But there have also been several class actions over the past several years involving violations of people's data privacy rights. And one of those ways that the rights are being enforced is through class action litigation. One of them was the large class action in the Northern District of California against Facebook that was settled in 2023, right?

Fred Brunetti: It was. And that was if you remember back in the day with Facebook biometrics information is a hot topic and always one of concern. The allegations of that lawsuit were the individual who is bringing the lawsuit against Facebook was saying hey I didn't give you my photo with my permission. What you're allowing these individuals to do who post photos, on Facebook is you're allowing them to make what was called back-in-the-day tag suggestions. So you and I and a couple of other people from work, you're in a photo, and you decide to post it to your Facebook page. I all of a sudden look at it and say, hey, why are you telling Gary you might want to tag Fred in this photo? Why are you telling Gary you might want to tag Joan in this photo? They didn't consent to their picture being put there. So that was kind of the crux of the litigation battle there that took place between Patel and Facebook.

Gary Fellner: That was Patel v. Facebook under the Illinois biometric law, right?

Fred Brunetti: BIPA. It'll turn your blood cold if you're a litigator because, unlike the vast, vast majority of the privacy laws that are out there today, BIPA has a very specific private right of action which is why class actions and a significant litigation docket and specialties will be built around it not only to prosecute it but also to defend those types of actions. There's a mandatory penalty that goes along with it. And recently within the last year, the Illinois Supreme Court essentially came down with the ruling saying that each penalty can be cumulative. So for example, if you are an employee scanning your thumb click pred to your employer because that's how they track their employees in their movement. And you do that say four times a day, clocking in, clocking out, doing the same thing for lunch. Each one of those clock-in procedures, if it's not properly noticed and if the data that's collected is not properly maintained, could be a violation. And those violations at $5000 a pop could add up pretty quickly.

Gary Fellner: Do folks in New York, New Jersey, and Connecticut where we practice mostly, do they need to be concerned with the Illinois biometric statute?

Fred Brunetti: They do if they have any relation at all to Illinois and to the practices that are taking place in Illinois. So if you have a couple of different offices and one of them happens to be in Illinois and to any degree touches upon biometrics, you need to make sure that you have the proper practices and protocols in place there.

Gary Fellner: There's also being, in addition to the class faction, the Federal Trade Commission weighing in on data privacy, correct?

Fred Brunetti: Yes. So in the absence, as you know, in the absence of an overarching comprehensive federal data privacy law, the FTC has been the de facto federal enforcer of privacy rights nationwide.

Gary Fellner: I think that one of the largest settlements ever in this area from the FTC was Facebook settling for $5 billion in 2020 for allegedly deceiving users regarding their ability to control the privacy of their personal information. And of course, that whole proceeding has spawned off into further litigation, which I believe is continuing.

Fred Brunetti: Right. Yeah, that was kind of the watershed moment, or at least that to that point it had been for the FTC. That essentially was like one-quarter of Facebook's profits that they were being hit with a penalty for. And it was the, the settlement terms that were kind of groundbreaking because not only was it, you know, the eye-popping financial number, but also as part of the settlement, Facebook had to open up their corporate compliance structures and allow new boards, new audits, new regulators to come in and be able to simultaneously direct the operations of their business. And it all arose at its base because Facebook essentially said you have certain rights, this is how you can exercise them. But in reality, they weren't giving those privacy-related rights to the users. So it became a large deceptive action.

Gary Fellner: So we've been talking about Facebook a lot. But the FTC is not, of course, limited in its proceedings to protect the privacy just to Facebook. As I understand it, there have been several other companies in the last year or two that have been the subject of action by the FTC under Section 5. Many of them seem to be targeting health organizations. Is that fair?

Fred Brunetti: Yeah. So as you know, FTC has two major hammers at its disposal, right? They have “unfair” and they have “deceptive” under Section 5 of the FTC Act and they can wield both of them equally effectively. The sensitive data has been a new focus topic of this regime of the FTC led by Chair Lina Khan. And they've been using all the tools that they can accumulate to be able to go after data privacy. Again trying to gap fill because there is no specific comprehensive federal data privacy law for them to use.

So the one that probably took the most press recently was the GoodRx decision because it was the first time that the FTC was again in a settlement, but it was the first time the FTC was able to use its health breach notification rule to go after GoodRx. Essentially what GoodRx was doing was allowing certain information to be shared even though it had made the representation that it was not being shared. So the health breach notification rule, although it's sometimes very closely tied to HIPAA is really separate and apart because it regulates folks that are not regulated by HIPAA. So here's GoodRx, which is an online vendor being able to be brought in by the FTC under the health breach notification rule for the first time.

Gary Fellner: So you're talking basically about pharmacies that are being swept into these regulations separated apart from HIPAA.

Fred Brunetti: So GoodRx, is a telehealth online service and essentially what they were doing is connecting the patients to the pharmacy. So GoodRx to be able to confirm billing codes and coupons and all that kind of information had its finger on PHI on the protected health information that's from pharmacy. But good, GoodRx itself as a vendor is not HIPAA regulated, so they can't go after them for violating HIPAA. However, the health breach notification rule reaches beyond HIPAA. It kind of follows the information and it requires that if you have access to health records, you have an obligation if those health records are being breached and shared. If there's a breach of those health records, you have an obligation to notify certain folks. And that was the allegation here that Good RX didn't do that. They were allowing this protected information to be shared and they didn't tell anybody that it was happening.

Gary Fellner: But again as we spoke earlier, the scope of the information or the data is not limited to health information. It could be any personal information that identifies you. Just seems though that the FTC has been focusing more on large corporations like Facebook and health-related companies. Is that is that a fair statement or do people who have data in the form of personally identifiable information, do they have to be concerned as well?

Fred Brunetti: Yeah, so really a renewed focus of this FTC has been really kind of two things: sensitive data and kind of part and parcel of that is, is children's related data, which is also by most regimes viewed as a sensitive form of data. And I think the reason they're focusing on that is because it's such a wide playing field, they want to be able to kind of take their risk-based analysis, right? Is it more risky for you to have your email address out in the public domain or is it more risky for you to have your medical condition, your genetic records, or your biometric information out in the public domain? Of course, it's more dangerous and much riskier to have that type of sensitive health information, biometric information out there because A, it really kind of speaks to you as an individual and B, it's something that you can't change. If your email address gets out there, or your phone number gets out there, you know, of course with some pain in the neck you can go through the procedure to play to change it.

Gary Fellner: You can't do that with a fingerprint.

Fred Brunetti: 100%, right. Exactly. So that's one of the reasons why I think the FTC is focused on making that a real priority. They want to make sure that if there's going to be safeguards that we're going to enforce, we're going to start with the riskiest stuff first.

Gary Fellner: Well, Fred, we've been talking about class actions and regulatory proceedings by the federal government. As I understand it now, there has been a wave lately of legislation that has been passed and is being passed, as we speak, in many states in the United States. All of which follow on the heels of the European Union's General Data Protection

regulations, which seem to be the gold standard. But let's talk about the United States. Here we are in the Northeast. I'm in Manhattan, you're in New Jersey, And we are witnessing all of these laws that are being passed. Tell us about some of the main laws that are being passed in the United States.

Fred Brunetti: Sure, so as we're talking now in early 2024, there are five separate comprehensive state privacy laws that are in effect: California, Colorado, Connecticut, Virginia, Utah, to varying degrees, they were passed some time ago and they all came into effect before this year.

There are a handful more that are going to come into effect during 2024. And in addition to those state comprehensive privacy laws as they're called, because they're essentially industry agnostic, right? You have HIPAA which regulates health information. You have Gramm Leach, which generally regulates financial information. But when we talk about comprehensive state laws, those are laws that regulate across borders, typically across sector borders to regulate the information itself. So each state has now kind of taken upon itself with some exceptions and exclusions to regulate the data in their state.

So by the end of this year, there will be a handful more that have been passed and will become enacted. Essentially by the end of 2026, there will be 14 different states that have enacted comprehensive data privacy laws, which of course means for us and compliance and, you in litigation. Those are 14 different schemes that you need to be able to track. I need to be able to understand not only the scope but also the information, and the data that they would be covering and concerning.

Gary Fellner: Did you say at the end of 2026?

Fred Brunetti: Yeah. So some state laws have already been passed, but their effective dates are not until 2026. Indiana, for example, was passed a while ago, but it's not going to become effective until 2026.

In my home state of New Jersey, late last year, really early this year, they finalized and passed its state of privacy law. It was passed in early January of this year. It will not become effective until January of 2025. There are handfuls more that are going to come online and that number sometimes gets blurred because Florida, perhaps not surprisingly, did its own thing. It has a date of privacy law, but it only applies if your gross annual revenue is over a billion dollars. So most companies are not going to have to concern themselves with it, but it is a comprehensive law. It goes across sectors and industries so we kind of group it in there together.

Gary Fellner: Well, it certainly makes it hard for companies to comply with these laws that are a patchwork of different regulations or legislation throughout the United States when they're doing business on the national level, it's not easy to follow which law applies. I mean, we're not talking about selling widgets from state A to state B. We're talking about data. It's rather amorphous, right?

Fred Brunetti: No doubt about it. And it's more than a full-time job because, to keep track of not only the bills that are out there and pending but also the enacted ones and how they're going to be enforced. It's a significant concern. And I think it's scalable depending on the size of your company, right? If you're a relatively small company with a relatively small consumer base. Let's say you have a lot of repeat customers, but you're under a certain threshold, you might not have to be concerned with every single different state regime that's out there. But if you're a growing, ambitious company that again like you said, operates across borders with certain information and has contact information, personally identifiable information of consumers in various states, you need to keep informed and you need to establish good practices early on so that you're not at the short end of the stick later on trying to explain yourself to a regulator. The best position for you to be in is to always know where your data is. This way, not only can you steer clear of the regulators and the bad stuff that can happen to you and your company, but you can best inform the strategic decisions that your company makes as to how best to use that type of data.

Gary Fellner: What does this mean to say a company in New Jersey or New York or Connecticut where they're selling services on a nationwide basis? You've got these flows that are coming down on the pike. One thing obviously that they need to be concerned about is having good policies in place, correct?

Fred Brunetti: Yes. So you have to kind of work back end to front end, right? You want to make sure that you have the proper operations on the back end and your privacy policies. That's the stuff that everyone always sees. Now it's, you know, it's hard to avoid when you scroll down to the bottom of every landing page for a website, at the very bottom you see a hyperlink that says you know, privacy policy. Well, the reason that's there is to harken back to your pal Steve Jobs is because you want to be able to give people notice of what's happening to their personal information, to their data. So you need to have back end structure so you know what you're doing with the data so that then you could properly and accurately put together a privacy policy which is outward facing to the consumer telling them this is what we're doing with your data and these are the rights that you have and these are the obligations that we as the, as the collector, as the controller of the information have.

Gary Fellner: Are you seeing that many companies are gearing up as they should to develop these policies?

Fred Brunetti: Yes. And I think some folks are going to kind of off-the-shelf solutions of trying to get a very boilerplate one and sticking it on their website so that it's there. But I think the more sophisticated businesses, the ones who kind of see down the road to develop their strategy are really before they put a privacy policy on their website, are sitting closely with the business development folks, are sitting closely with the technologist, are sitting closely with marketing.

Gary Fellner: Are sitting closely with you?

Fred Brunetti: With me, sure. And it's important to be involved in those conversations early on because certainly, we can help them to avoid some problems. But they need to have a clear business plan initially because once you come and sit and talk to me or talk to you, it's good when the company knows this is what we have, this is what we'd like to do with it. This way we can have a more informed conversation of saying, OK, this is what else you can do with it, or these are the kind of things that you have to avoid. So every company, regardless of where your customers or where your users are located, should have a privacy policy on their website. But just as important as having one is making sure that it accurately describes exactly what's happening with your data. Because as you mentioned, in a lot of those other cases, it's going to be one or two things. Forget about the AGs and the private rights of action that can come after you, FTC very clearly had said it better be fair and it better not be deceptive. So the easiest way to get tripped up is to say you're going to do something and not do it. That's textbook deceptive and you don't want to be doing that.

Gary Fellner: And this is a concern that I guess faces all companies. We're not talking about the Facebooks of the world or the GoodRxs, all companies, big and small.

Fred Brunetti: Sure, yeah, there are certain thresholds for each of the different state regimes. But essentially if you're looking depending upon the size of your state and the smaller the state, it's usually scaled to how many consumers are in that state. But if your website is drawing traffic from typically 1-2% of folks from a regulated state, you're going to be in the scope of their data privacy laws. So you need to make sure that you have the proper protocols in place. And like we had talked about, some companies are doing it a different way, right? Some are small enough that they could say, OK, we have our list. We know there are 14 states that we have to look out for now. We can make sure that we're compliant and kind of hopping in the right direction. Other companies perhaps with a longer view are saying, you know what, we're going to establish ourselves to the high watermark. We're going to take the most restrictive standards. We're going to give that those rights and obligations across the board, whether or not you're technically in scope and we're going to move forward with our business objectives there.

Gary Fellner: Well, Fred, we're out of time. I thank you very much for stopping by and chatting with me about data privacy. I look forward to our next conversation where we'll dive into the fighting world of data security breaches, where there's a slew of lawsuits that are being filed and we'll pick that up then. So thank you.

Fred Brunetti: Thank you, Gary. It was good talking to you.