Digital Planning Podcast (Season 5, Episode 3): Understanding Biometrics and the Impact on Estate Planning

Speakers: Justin Brown, Ross Bruch, and Jennifer Zegel

Jennifer Zegel:

Welcome back to the Digital Planning Podcast. I'm your host, Jen, and I'm with my co-hosts, Justin and Ross. And on today's episode, we are going to be discussing biometric data, which is an emerging and complex subject that impacts us all. Laws and regulations surrounding biometric data and the privacy of biometric data are being enacted or have legislation pending in a growing number of states around the country, which has given way to a variety of lawsuits against employers, service providers, and tech companies for violations on the collection, usage, and storage of an individual's biometric data. Justin will help explain exactly what biometric data is, some current laws and cases, as well as issues and some planning considerations in this area. Justin, with that backdrop, let's start with the basics. What exactly is biometric information and biometric identifiers?

Justin Brown:

Thanks, Jen. Biometric information is a fascinating area of the law right now where it's really expanding into so many different aspects of what we do and how we use our data and how we store our data. And before I go into your question, Jen, I want to talk real briefly about giving a backdrop of biometric information and biometric identifiers. And specifically, in Illinois, Illinois has created the Biometric Information Privacy Act or what some people refer to as BIPA. And BIPA is fundamentally a consumer protection law that's designed to regulate the use and storage and safeguarding of biometric information. So BIPA defines biometric information as any information regardless of how it's captured, how it's converted, how it's stored, and it's all based on an individual's biometric identifiers that are used to an identifying individual.

So what are biometric identifiers? Well, it could be a retina or an iris scan. It could be a fingerprint, it could be a voiceprint, it could be a face scan, a hand scan. It could be any of those things. So BIPA is really designed to safeguard and protect those private biometric identifiers that we all have that are unique to us.

Ross Bruch:

What about DNA, Justin? Does DNA count within that as well?

Justin Brown:

So not to my knowledge because DNA is something that's going to be contained in your blood, and BIPA is focused more on the information and the identifiers that you physically have. So I think the goal of BIPA is that if we all use passwords or social security numbers, and if that information is stolen from us, then we can change our passwords. We might be able to get a new Social Security number, but we can't change our biometric information, we can't change our fingerprints, we can't change our eyes, we can't change our hands, our voice prints. Not that we can change our DNA, but at least right now we're not using our DNA to log into our phones or log into systems. We're using these fingerprints and hand prints and face scans in order to do it.

Ross Bruch:

So rather than just go with the basics, we jumped to step 10 there. Let's go back to the basics of where you're headed and what BIPA means and the implications of that.

Justin Brown:

Sure. So again, as I said, it's designed as a consumer protection law, and the focus here is that a private entity cannot collect or capture or purchase or receive or obtain somebody's biometric identifiers or biometric information unless they first get the consent from the individual. And BIPA goes through steps in what they need to do. So a private entity is going to need to inform the individual of the purpose of collecting and storing the private information, and the individual is going to have to provide a written release of the use of their biometric information. So there has to be this knowing giving up of this biometric information by the user before an entity is permitted to use it and disseminate it.

Jennifer Zegel:

When was BIPA enacted?

Justin Brown:

BIPA was enacted back in 2008. And in response to BIPA, there weren't really a lot of cases, but then they really started to pick up later in like 2018, 2019, 2020. And specifically, there were some cases in Illinois, in federal court, where they analyzed the extent to which biometric information was used and what is considered to be sufficient notice to the individual and a written consent by the individual. So there are a lot of cases, for example, where employers may implement systems that require fingerprinting.

For example, there was one case back in 2020 where an individual was using a vending machine that was provided by the employer, and the employer required fingerprinting in order for anybody to access the vending machine. And once you put your fingerprint on, then that would automatically link to your account, and when you wanted something from the vending machine by putting your fingerprint on, that would then subtract money from your account on the vending machine. So it was a really streamlined mechanism that the employer used and a high-tech mechanism to simply avoid having the need for individuals to carry money around and they can just use their fingerprints to get candy out of the vending machine or a coke.

And in this particular situation, the individual had signed up for it, it was voluntary, it wasn't mandatory, and she signed a waiver. And the issue was whether or not, in this particular case, she experienced a harm in giving her fingerprint to the employer or to the third-party vendor, and whether she gave up any of those rights to her fingerprint and her biometric information. This went through a couple of levels in the court, but ultimately, at the highest level, the court determined that there was a violation of BIPA and there was a harm in BIPA.

The court looked at whether or not the harm was specific to this individual or generalized, and the court ultimately said that with biometric information, it is such important information that we want to safeguard that the harm is very specific and we need to be protecting this protected information. We need to be protecting our biometric identifiers and our biometric information because if it gets stolen or if it goes into the wrong hands or if it is disseminated without the individual's knowledge, there's really not a lot that we can do to fix the problem.

Ross Bruch:

In that case, was the company using the biometric data for anything other than access to that vending machine or similar products?

Justin Brown:

In that case, no. There was another case in 2020 where there was a company that was scanning the internet for pictures and taking these pictures and creating a database with people's names and addresses, and I think their jobs, their employment. And what that company did was they never contacted anybody to let them know that they were doing this, so nobody knew that their pictures were being stored in this database. And they then sold that database to the police. So the police then got this database of people's faces, their biometric information and identifiers so that the police could then run that information through their system and they would have names, addresses, jobs, and all of that stuff.

So, Ross, good question. That's two different cases where the biometric information was used for two entirely different reasons. One, to make a profit, the other to streamline the process for employees. But in both situations, the court in Illinois believed that these were BIPA violations.

Ross Bruch:

So what would you have advised the first entity, if you were representing them, to have done beyond the waiver that they already collected, beyond the notice that they provided, to comply with the law?

Justin Brown:

Yeah, good question. And I think that's probably a good place to start with, the most recent case that came out. There was a case in February of this year where there was an individual who was a manager at a White Castle restaurant in Illinois. And similar to the other case, when she started back in 2004, White Castle created a system where the employees were required to scan their fingerprints to access their pay stubs or to access their computers. And White Castle hired a third-party vendor that was responsible for verifying each fingerprint scan in order to authorize the employer's access to their pay stubs or their computers. What was happening was there was a scan that was stored someplace, presumably by White Castle, and then this third party would then verify this new scan against the old scan to confirm that it's the correct individual.

The issue in that case is that the individual started working for White Castle back in 2004, so this system went into place in 2004, but BIPA didn't go into place until 2008. And the individual never came forward and contested anything or claimed a BIPA violation. The question was, has the statute of limitations run on this? If the individual got that initial scan in 2004, then was there really a BIPA violation and if BIPA wasn't created in 2008? And if there was a BIPA violation, has the statute run on it? And this was a pretty big case because the court ultimately decided that not only was there a scan in 2004 that violated BIPA, but every single time that individual scanned her fingerprint, that was a scan that triggered BIPA. And if the mechanisms that were in place were not proper and appropriate and compliant with BIPA, then every single one of those scans for that individual and every single employee during that time was a separate BIPA violation.

This is a significant case because before we thought that maybe there could be one BIPA violation per person, but here it could be a lot of BIPA violations. Think of every single time you log into your computer at work, and if you're doing that with scanning of your biometric information, then that's a lot of scans and a potential lot of BIPA violations and more importantly, a lot of damages that employers and, in this case, White Castle, were subjecting themselves to.

Ross, going back to your question of how should we be acting with biometrics? The first thing I would say is the easiest thing is don't use biometrics if you can avoid it. Yes, it makes things easier, but you could just use a password to log into your computer or to log into a vending machine program or the pay stub program. So that's the first line of defense. That's the easy answer.

If you're going to use some type of biometric information, then I think there needs to be clear delineations for the individual whose biometric information is being used to say, first of all, that this is entirely voluntary. I don't think it makes sense to create programs or procedures that are mandatory, which would require individuals to give up their biometric information and their biometric identifiers. So first step is give people an out so that it's not a mandatory program. And then, once you have done that, it's going to be very important that you give written notice of exactly what you're doing and have people provide written consent of the ability to use their biometric information for a specific purpose. And I feel like, especially in Illinois, it's got to be more than a I agree type page where you just click it and say, "I agree." I think there probably needs to be some greater explanation so that employers are not going to have problems later on with arguments that they didn't notify people.

Jennifer Zegel:

Going back to that case that you just discussed, do you know if it has gone up on appeal or if they've begun that process?

Justin Brown:

So this case was in the Illinois Supreme Court, so it was the highest level of Illinois.

Ross Bruch:

Is there a difference between an employer who might mandate, or in your case of what you just talked about of giving them an option to use a written password to get out of it, versus a third party where you're voluntarily employing them? So I'm thinking back to our conversation with Joel Revelle of Two Ocean Trust Company, and he mentioned a biometric trifecta of fingerprint, voice, and face ID as a heightened level of security access to an account. If I were to create an account with Two Ocean, is that going to be viewed differently from the courts than my employer saying, "Ross, you have the option," or, "You must provide us with this biometric data."

And I'll add that I think this is very relevant because for years now I've been reading and seeing and hearing that passwords will one day no longer exist, and we all know we forget our passwords, they're imperfect, they are hackable to some degree. So it seems to me, I almost don't love the direction that this is heading of limiting this so much. I understand the importance and why because of the heightened level of security that the courts are so stringent on this observation or on their rulings of how information was collected, stored, shared, used. But to me, it seems like it's a better path forward than physical written passwords.

Justin Brown:

Let me take a step back first to say that BIPA is an Illinois law, and it is designed to protect consumers in Illinois whose biometric information and biometric identifiers are being used, without their their knowledge or their consent. There are similar statutes throughout the country in various states, not exactly the same as BIPA, but I guess the focus today on BIPA is because it is one of the more talked about statutes and has some of the most case law developed around the statute. There is no nationalized form of BIPA yet. There is a bill in Congress that has been in Congress for a little bit, but it hasn't moved.

If we go back to the Two Ocean Trust episode where we talked about the security procedures in place using biometric identifiers; that was not in Illinois; that would not be subject to BIPA unless the action occurred in Illinois. So in that situation, if you had an individual who was one of the people whose biometric information was being scanned and that person was physically in Illinois at the time, then BIPA would be implicated, but it wouldn't unless the person was in Illinois at that time.

But Ross, I hear where you're going. BIPA applies to private entities, so that's pretty broad. To me that includes everyone except for state or governmental entities. In that situation, those scans for accessing private keys, those would all be subject to BIPA. And I presume that when you're setting up those scans and those security procedures, there is some kind of notice and informed consent that is being provided to the third-party that is scanning. Now, I think a big question is what are these companies doing with the biometric information once they scan it? I talked about one of the cases where the private entity took that information and sold the information to third parties. In that situation, it was the police. That is a huge risk because I don't want my biometric information sold, because once it's sold, I can't get it back.

Jennifer Zegel:

So I think, and correct me if I'm wrong, Justin, it's important to recognize that with the different legislation that's enacted or pending at state levels, BIPA does give a private right of action for an individual to directly bring an action against violations of BIPA with their personal biometric information, but not all states allow for a private right of action. In other states, it's up to the discretion of the attorney general. And so I think that's going to have very different outcomes because the attorney general may decline really pursuing violations of BIPA in certain cases where there is no private right of action.

Justin Brown:

Yeah. The states are free to create their statutes however they want and to create causes of action however they want. And Illinois has specifically given individuals a private right of action because they have wanted this statute to be so protective of individual rights that they felt like the only way to do that was to give individuals the private right of action.

Jennifer Zegel:

And because of that, with the situation of Two Ocean Trust, and I'm not familiar with any form, whether pending or enacted legislation, where Two Ocean Trust is located, but if a client of Two Ocean Trust is physically in Illinois, uses their biometric

data that does not conform to BIPA, but conforms to the law of the state where Two Ocean Trust is, I think we have some real conflicts of law issues, too, that are likely to emerge.

Justin Brown:

I think you're right, and I think you have that issue in entities that are operating in multiple states and create one uniform policy on how they're going to be dealing with biometric identifiers and biometric information. We are all trust and estates attorneys. I guess a question for you guys is how does this impact the trust and estates world? Why do we as trust and estates attorneys care about a privacy case in Illinois?

Ross Bruch:

Well, to me, there's a great deal of overlap between your property rights and your personal data rights, personal data meaning your biometric data. Is it the equivalent of a digital asset? It seems to me we care about our client's security from a monitoring their Social Security number, in the case of an identity theft, we've all dealt with clients who have been victims of identity theft, and this is just one more avenue into that. So from a security standpoint, we certainly care, but I also think that back to the property issue, it is something that they are knowingly possessing and possibly giving away, knowingly or unknowingly, and thus, it's within our purview to help advise on that proper use and understand what the law is so that they can make better and more informed decisions.

Jennifer Zegel:

Absolutely, and to take that one step further, I think, as this technology advances and consumers are more aware of it, there's going to likely be an ability to commoditize personal data, and some people may want to do that for monetary gain. The other thing to think about is right now there's no postmortem privacy right to this type of biometric information and data. And do we want to plan for that in estate planning documents that that type of information can continue on if somebody is creating databases or storing their DNA for potential future cloning or some other wild technological advancement that they're properly allowed to do that and their executors and beneficiaries are allowed to continue to use that data, or are they prohibited? Should that information be deleted? Should the executors and personal representatives take active steps to find out where biometric information may be stored with various tech companies, service providers, employers, and seek to actively make sure that that information is destroyed?

While biometric data can't necessarily change because that's part of ourselves, what if somebody's in a horrific accident and has plastic facial reconstructive surgery or their hands get burned and their fingerprints change? How is actually accessing accounts information going to be able to be updated to have new biometric data with the facial recognition software changed as a result of the surgeries or deformities?

Justin Brown:

Yeah, I agree. I think you've got RUFADAA issues of how do we access this biometric information when somebody's incapacitated or when somebody's passed away. We have storage issues. We have custodial issues. How do we make sure that the people who are holding onto this information are safeguarding it? I go back to our discussion we had one time about holograms where we were talking about creating holograms post-death, and you would need to use biometric information and biometric identifiers to create those holograms. So who would be creating those holograms, and who would have access and the legal right to be creating those types of things? Michael Jackson, post-death, did a show all through hologram. How was that information used?

Ross Bruch:

So that's an interesting question because if your voice is your biometric data, and obviously during life you possess your voice, you own it, it is yours, and I think there would be some sort of intellectual property violation if somebody copied my voice through a deep fake and then used it to sell something. But after my death, who owns my voice, especially if I didn't give it away? Does it automatically become a property of my estate, and then it just flows through every other intangible asset? Do I

need to specifically give it to my beneficiaries or a beneficiary? Can I give it to multiple people? There's a financial interest in a famous person's voice, or take it one step further, you said no to DNA, Jen mentioned cloning, though, but in 10 years, maybe DNA is a biometric data point that needs to be monitored and secured.

Or maybe my personality, we talked about AI in a recent episode, and ChatGPT is really good at mimicking the voice, meaning the type of writing or speaking style of famous individuals. So is that something that can be protected, and is that something that needs to be planned with? And even though we can't do anything with it now, does that need to be addressed at any point in the future, at any point in the near future, I should say, of documents of how your clients are protecting their estate and interest in it and their beneficiaries, especially when you're dealing with somebody who is famous?

Justin Brown:

And how do famous people protect this information? If you have put out a CD or somebody wants to impersonate us, all they have to do is go to the podcast and take excerpts of our voice and presumably take some biometric information from there and recreate us later on.

Jennifer Zegel:

Are you inviting someone to do that, Justin?

Justin Brown:

I don't know that anybody wants to right now.

Jennifer Zegel:

But it's a very scary concept. And taking advanced AI even further, I've read articles that from just a partial picture of somebody's fingerprint, an AI can recreate it and actually get into the systems with that recreation of the fingerprint totally usurping the security protocols and some of the reasons for biometric data, which is horrifying and gives it an even deeper meaning to deep fakes.

Justin Brown:

Well, and should there be the ability to use somebody's biometric information after their death? If I have a picture of somebody's fingerprint, what stops me from using that later on? Now, there might be computer fraud and abuse laws that I'm violating, but with technology, this information is going to become more accessible and we're going to be able to use it in a much easier manner.

Jennifer Zegel:

A lot of food for thought and future planning considerations here, which are likely going to change and evolve as more and more states enact this legislation and, of course, if there's federal legislation. And we haven't even discussed or dipped our toe into the water as to how this could be violative of the GDRP or other European laws, nor have we even talked about how China already regularly uses biometric data of its citizens, and this created a national registry, I believe, of male individuals in China. So there's a deep rabbit hole here.

Ross Bruch:

So I raised the question about planning within and where it fits in a document and maybe we're years away from talking about whether it belongs in a will or in a trust. But since both of you are in private practice right now, I'll ask you, what about a power of attorney? Should power of attorney documents reference the use of biometrics? Because I can imagine my incapacitated principal and their agent wanting to use a retina scan or wanting to use their fingerprints to access something on their behalf and acting as their fiduciary, and totally within the grounds of the law, but needing that biometric data, should they be able to gather it? And can you foresee updating your documents and your forms to reference this at any point in the near future?

So futuristic world, right? Well, year 2025, and the principal is incapacitated in a coma on the hospital bed, but has an account at some trust company, some bank account, some financial institution where the only way to access, because passwords have been a thing of the past, the only way to access is through a facial scan and a thumbprint, and you need both of them. Should that agent be able to go to the hospital with the phone in hand, scan that individual's face and put their thumb onto the iPad and access that bank account because they need to access it on behalf of the incapacitated principal?

Justin Brown:

I would say no, because, in that situation, that's not the proper mechanism for a power of attorney to access the information. And in that particular methodology, the power of attorney's impersonating the principal and using the principal's biometric information and not the power of attorney's biometric information. And that would be a potential violation of the Computer Fraud and Abuse Act. So in that specific example, the power of attorney should be going through the normal mechanisms.

Jennifer Zegel:

So slightly changing that fact pattern, Ross, say they're not trying to access a bank account, say they're just trying to unlock the incapacitated person's smartphone and the incapacitated person has set the smartphone to only open upon fingerprint and facial recognition. So now the incapacitated person is on hospice, they're still alive, agent under power of attorney has authority through the power of attorney under RUFADAA, can the agent take the phone to hospice and go through the procedures just to unlock it? Because under RUFADAA, if the person was deceased, I mean, separate apart from access issues, the executor, if it's the same person as the agent, could go into the phone. We're not talking about connecting the apps that go to third-party service providers. And I think a power of attorney could do that while the person's alive as well.

Justin Brown:

If the power of attorney explicitly provides that.

Jennifer Zegel:

If the power of attorney explicitly provides that. So in some ways, by having RUFADAA authorization and powers of attorney, does that then extend in a limited situation to what Ross is saying about more robust language? Is that a placeholder for now? Do we need to go deeper?

Justin Brown:

I think that's a tricky question because I'm still on the Computer Fraud and Abuse Act. And again, you can't impersonate somebody, but if you would be able to access it when the person died, again, not by impersonating the person, but if you were able to access it when the person died, and if you had the authority to access it while the person is living through the power of attorney, then one could say that you should be able to access it by whatever means necessary in order to fulfill your obligations as power of attorney. If the only mechanism to fulfill your obligations under the power of attorney and access it is in violation of the Computer Fraud and Abuse Act, where do the two, when you've got two conflicting statutes or two conflicting purposes, which one ultimately prevails?

Jennifer Zegel:

But it does open my thoughts as to how and if healthcare powers of attorney should be revised or include provisions specifically allowing the agent to collect biometric information of the principal. That brings in a whole other different kind of angle here. And then, what could the agent do with that information if they are legally allowed to collect it in some fashion? Is it limited to a specific purpose, use?

Justin Brown:

I think that's a good point. And we had talked, in one of our episodes, about wearables and the data on wearables and who owns that data? And it's now biometric information that is going to be stored on these wearables as technology improves. So

what's happening with that data? What's happening if you provide access to that data to, say, a life insurance company and they are using that data to maybe determine what your rate should be? Is that a potential violation of, say, a BIPA where the data from my wearable is now going into a company that is using the data to come up with actuarial calculations for their product?

Ross Bruch:

Okay, Justin, so lot of complicated things going on here, a lot of different moving pieces. Uncertainty about what the future of the law brings, not only in the case of BIPA, but where it's going to apply if it's going to apply in other states. What are some major takeaways that you want to impart on the audience?

Justin Brown:

I think we, as trust and estates attorneys, need to be aware of these types of laws. And I think we need to be aware of how our clients are potentially using their biometric information and their biometric identifiers because it is the Wild Wild West out there. And there are going to be cases where individual's information is taken or disseminated or transferred without their knowledge. It's important that we impart upon our clients the need to protect their biometric information. Are we going to have the answers right now? Absolutely not. And is this an evolving area? Absolutely. But I think with a lot of things that we talk about on the Digital Planning Podcast, we've got to have it in the back of our minds, because it is an area that is going to be impacting all of us and all of our clients.

Ross Bruch:

I think that's well said. I am maybe naively willing to give up some of my privacy for convenience, and I can't be the only person who does that. It makes me more cautious to think this, but I would gladly give up all of my physical credit cards, my pass into my office, anything else, my physical passwords, my written passwords where I could just scan my retina or upload my fingerprint or talk to the computer and give me access to what I want. I want to give my employer access to my fingerprint so I can get to the candy machine as per the first case you referenced before, because it's an ease of access. It's, to me, administratively, so much easier and eliminating one of the hassles and burdens of modern life.

But you raise excellent points because how do I know how that information's being used and stored, and what have I really given up? And in the case of if I was a famous person, what are the implications there? So a lot that I am naively not thinking through when I say, "Yeah, I want to give this up in order to have a simpler life," but I think that I am not the only one who's doing that and going to be subject to those trade-offs. And that's where we come in in being able to help our clients understand the implications.

And with that, this has been another episode of the Digital Planning Podcast. A special thanks to our co-host, Justin, for his expertise on biometric data and the ins and outs of the future of this field. So thank you, Justin, and on behalf of Jen, Justin, and myself, thank you for listening and we'll catch you on the next episode.