35TH ANNUAL SYMPOSIUM: HUMAN RIGHTS AND CROSS-BORDER DATA FLOWS

March 1, 2024

Connor Glendinning:[1] Hello, everyone, and welcome to the *Florida Journal of International Law*'s annual symposium. This year, for the first time post-pandemic, the *Journal* is returning to an in-person format, and for that I have to thank and acknowledge the Levin College of Law and Dean McAlister for the funding to do so. As a direct result of that, the *Journal* was able to invite our two esteemed guest speakers today to talk about cybersecurity, privacy, and a hint of Artificial Intelligence (AI) on the global stage. Thanks also to Ruth McIlhenny for all her help in planning for today. This event is going to proceed in three parts—each guest speaker is in turn going to give sort of a mini-lecture on a topic of specialty before we proceed into a panel conversation that is going to be moderated by Professor Lidsky. Afterwards, there is going to be official time for questions, but there will be time for questions along the way as well. I now have the pleasure of introducing our first speaker, Trish Carreiro. Mrs. Carreiro completed her undergraduate studies at Duke University before earning her J.D. at NYU. She began her career in the tri-state area in New York and is now a partner at Carlton Fields in Miami where she is the chair of the firm's cybersecurity and privacy practice. She has numerous certifications from the International Association of Privacy Professionals and is co-chair of its South Florida chapter. She also has extensive experience litigating complex privacy cases and advising companies as outside privacy counsel, so she is the ideal person to speak to us about managing business interests in the privacy landscape today in the United States. So, without further ado, Mrs. Carreiro.

Patricia Carreiro, Esq.: And you can all just call me Trish.

Connor Glendinning: Trish, I'm going to provide some questions to get things going. First, could you give us an overview of the major laws governing data privacy in the United States and particularly the newly enacted laws in the past year?

Patricia Carreiro, Esq.: Sure, so for any of you who haven't taken privacy courses, this year things are already getting a little more complicated in the privacy world. We have some privacy laws, typically sector specific—things like [the Health Insurance Portability and

1. Connor Glendinning is a third year law student at the University of Florida and Editor in Chief of the *Florida Journal of International Law*.

Accountability Act (HIPAA)], Gramm-Leach—that have been around for decades, but last year there were for the first time five state comprehensive privacy laws. The year before there had only been one, and last year that number of privacy laws coming into effect more than doubled, so if you're practicing in privacy get ready to just keep learning and learning and learning. It is moving quickly. The good news is that there is a lot of overlap, so with all these new privacy laws—this rapid expansion—these states are largely functioning off of the same kind of concepts that you saw in the five states that were already effective last year. The original state was California with really detailed requirements introducing things like requiring a privacy policy but also certain rights like the right to know the data that this company holds about you, the right to actually get a copy of it, the right to correct inaccuracies, the right to delete information, and there are exceptions to that one especially that I'll asterisk. So, things like that, that were new, also things called opt-out rights. What an opt-out is—let's take where it most comes up—which is when it comes to digital advertising, and if you're going to target ads to someone based not only on your website but activity across other websites, then they want you to have if you're in California, a specific link on your homepage where someone can click, and it says "do not sell or share my personal information," and it opts them out of that type of tracking. That's a little bit of an overview of what you see there. The states that have come onboard after California haven't required so many of the specifics, but they've kept a lot of those key concepts—the privacy policy, the right to opt out of the sale or use of your data for targeted advertising purposes, the right to know the data, to correct the data, to delete data, that kind of thing.

Connor Glendinning: In light of that, could you describe the most common privacy risks corporate entities face in the United States—whether that be private rights of action or administrative enforcement?

Patricia Carreiro, Esq.: So private rights of action I think by far are some of the greatest risks because they just get so expensive so quickly, and you don't really end up getting to go to trial because of how expensive you know that process would be. You then also have some pretty active enforcement agencies, so the [Federal Trade Commission (FTC)] being one of them. They've been especially active. Depending on what industry you're in, there's also some pretty active regulators like [the Department of Health & Human Services (HHS)], so the definition of healthcare data and what's subject to HIPAA has really expanded just within the last two years. If we go back a couple of years, for example, just something on a healthcare provider's website for learning about services, many people would not have considered to be within the scope

of HIPAA—now that's no longer the case. That's been expanded by HHS, so there's been a huge shift of companies just sort of trying to keep up with, "okay this was the law under HIPAA for you know like twenty years and then that shifted, so there's this expansion," but I think we're seeing across other industries as well.

Connor Glendinning: You've advised—I know specifically you have a niche in life insurers—but you've advised companies of varying sizes. How do you think privacy risks vary if at all for companies of different sizes?

Patricia Carreiro, Esq.: Well, I will say under a lot of the state comprehensive laws, you have thresholds, so if you're beneath a certain threshold, often the state comprehensive law just won't apply to you. But once you hit those thresholds for application, there's a lot of similarity because you have all those same requirements. Some of the differences can come up in just what you're doing with the data and how much data you collect because you've got to think about what's reasonable for say that particular type of data. If you're just not collecting a whole lot of data, and you're a small startup, then okay maybe there isn't as much risk to you as opposed to even if you're a small startup but you're doing something that's let's say collecting biometrics. In which case, I am not going to feel very comfortable relying upon like, "we were really small, sorry that your biometrics have been stolen." That company would likely end up folding if there was a data breach. For larger companies, you might say well they've got more resources so maybe that's a higher threshold. I think size certainly impacts it, but I think you have to look at what data they're holding onto, what they're doing with that data, but it's always going to come down to risk. What's the risk to that data and how do you take care of that?

Connor Glendinning: Given the industry related differences then, what industry differences do you see in privacy risks? What industries face the most privacy risks?

Patricia Carreiro, Esq.: The ones with the most data, right? I mean healthcare, certainly that's one. It also tends to be heavily targeted by the bad guys, the threat actors, so that's certainly a huge area of risk. I would say now probably substance abuse because that's been a focus for HHS, so I would point to that within healthcare. Within life insurance, it's always an issue because you have a lot data being collected, and I know just mentioning life insurance makes you want to fall asleep a little bit probably, but from a privacy perspective, it's fascinating how much data there is about you and how that can be used to predict the amount of risk

with insuring your life. They have life insurers using like your watch—they can see how many steps that you fit in, so they know how active you are. Say you're going to order groceries, so they can see what type of food you eat—if you sign these authorizations. Don't worry it's not some secret thing that you can't find out about. It's in the privacy notices. Frequently you actually sign an authorization to permit it. Your car, right? All of the data that's coming off it. Well, we can see what kind of driver you are, and all of this can be factored into the risk of evaluating you and can adjust your premiums, so maybe you might get a better life insurance policy for cheaper because they see that you're pretty safe. It can actually be a positive, but I think that's a huge area of figuring things out because you also have what's called automated underwriting now. I'm going to get too far into the details, but the idea is that you sign an authorization and we go and pull data from like LexisNexis, we go and pull data from like the DMV, and we quickly apply technology to evaluate how much of a risk you are, so that I can give you an instant response as to here's how much life insurance costs for you. As opposed to saying, "okay I need you to go to a doctor and get a physical exam and we've got to draw some blood and work it up to see how much we would charge you for a policy." Instead, there's all this other data that just exists around about you, and they say, "okay we can know a lot about you just from data that we already have, so let's just interact with you, you sign this authorization, we pull this data, and we'll have a good sense of your risk."

Connor Glendinning: I think insurance probably provides a good backdrop for thinking about given the amount of data they have about you, what are companies doing right to keep consumer data private?

Patricia Carreiro, Esq.: Well, I think that one, just in their privacy policies if you read them. I realize that a lot of my life goes into drafting things that people don't always read, which hurts me deeply—start reading them. I'm just kidding, but truthfully, they're trying and building things into their processes. Like sometimes you'll see a checkbox, sometimes they'll require you to scroll through a document to be like, "no really please read what we're telling you," and I think that there's that consideration that's more and more becoming something among companies that this is a part of our brand, and so they're putting that sort of focus on telling you the data that they collect and why, so I think that is a huge something that they're doing right on the front end. I have clients that are going above and beyond. They know that they're not required to get certain authorizations, but they get them anyway because they want that additional transparency. Also, [they're making] huge investments in protecting the data that they have, so you've got two sides of the house. Think of privacy as far as those notices that you get; think of it as far as

authorizations you'd have to sign; what you're doing with the data if you're sharing it or selling, and then on the cyber side, once you have that data, how are you going to protect it, and that's where we get into the like techy encryption and all that fun stuff. So, they're investing huge amounts on both sides. Both in their disclosures and what they're doing with the data as well as, "okay we have the data and how are we going to protect it?"

Connor Glendinning: It seems to me that in structuring something like privacy policies, there's the opportunity for businesses to structure that in a way that might be more beneficial to them than it is to their consumer. Could you talk about whether that's the case or alternatively if consumer and business interests are aligned?

Patricia Carreiro, Esq.: Yeah, so I feel very strongly that the consumer and the business interests are aligned, and I know that's frequently something that people are like, "no way the business is out for the business and the consumer's getting their rights taken advantage of," but I just don't see it that way. If you think about this business—particularly, I'll speak to my clients, which are often very large—a huge focus for them, the reason they go so large, is because they're offering something of service to the consumer. If they weren't useful to the consumer, then they wouldn't have gotten this large. They got that large because they did something right, and so they want to continue doing something right, and if they start getting sketchy with data, they're concerned about their brand. They don't want everything they've worked so hard on, that trust that they have with their customers to crumble, and so they invest huge amounts, and as I said often going above and beyond, just because they're like look this is our relationship with our consumer. So often times, I actually see much smaller businesses doing much sketchier things with data because sometimes what you see is this idea of well if there's a data breach a lot of those small companies just fold, but when you have these large companies, they don't want everything they've worked for to just crumble away. They have a reputation to maintain, and they know they're on the front page if they get compromised, so I think it's a large incentive, but it's one that focuses on a trusting relationship with the consumer, so what's good for the consumer is aligning with what's good for them because they exist to serve their consumer.

Connor Glendinning: I think that leads to more thinking then about how our perception of personal information—of what information is private—has changed. What's your take on that, and then how do you think businesses have adjusted to that changing perception?

Patricia Carreiro, Esq.: Yeah, I think there's been a huge expansion in people's view of data and what they have control or rights over. So, if you go back, we had personally identifiable information, and that's where privacy laws focus, and then that got broadened out to personal information, which was anything just linkable to you as a person, and even if you needed to combine it with some other things maybe. And now I think where we've gone—particularly when you start factoring in artificial intelligence—is even if I had that data out in public, I feel some rights over it. So, you have these litigations that have been coming up in relation to AI saying, "well you didn't have my permission to scrape my data off of that public site." So, what I think that we've seen is this expansion of people expecting more and more control over data even if they made it public, which in the past would have placed you outside the privacy laws, so I think there's an expansion and we'll continue to see that.

Connor Glendinning: Do you think the law is reflecting that change in perceptions now?

Patricia Carreiro, Esq.: I think the laws are going to take some time to catch up where we're already seeing litigations coming up around it but not as much. In many of the laws there are some exceptions, so for example if we're talking deidentified data that varies. Gramm-Leach defines the information it protects not only as identifiable but any information derived from it, so that has a broader view, but for most other privacy laws, you don't run into that. It's still limited to personal information and then it would cut outside of the law for deidentified information. I've heard regulators say, "well if you've deidentified it, I don't care about it," and that can vary by industry significantly.

Connor Glendinning: Thinking back to the alignment of business and consumer interests, what burdens do companies face unnecessarily in cybersecurity and privacy law? And I'm thinking specifically maybe with reference to recent [Securities Exchange Commission (SEC)] rules and then FTC rules that might be imposed on them.

Patricia Carreiro, Esq.: Sure, so I think that part of the issue with those rules particularly is how specific they are, and I know there's this view of like, "well just tell them exactly what they should do; we're going to provide these specific rules." The issue when you have a lot of specific rules is you're taking away a little bit of the resources that could otherwise be based upon risk. So, let's say I'm going to require you to have A, B, and C. Those are required when this company is approaching what it wants in place for cybersecurity. Then it thinks, "okay we must do A, B,

and C; what do we have left?" To address the issue there, is that what if I'm being told I need to have A, B, and C, but I've done the risk analysis, and I know my company, and I know the risks that we're facing and where the threats are, and I know D, E, and F are the much bigger risk for me because the regulators don't know my company like I know my company. They're trying to draft something for all of these companies, so for me there's a lot of unnecessary requirements and jumping through hoops that happens when you get really specific requirements on the cybersecurity side because it takes away from those resources that could otherwise be addressing the larger risks as tailored to that particular company.

Connor Glendinning: I guess then thinking about perhaps not regulators but those that might take advantage of private rights of action. I'm sure you have thoughts on the merits of most data breach class actions you litigate. What are those thoughts?

Patricia Carreiro, Esq.: Here's my invitation to rant I feel like. So, let's think about how it plays out temporally. There is a data breach, it hits the papers, and like the next day there's a plaintiffs firm in court suing about it. My issue with that is that I know these companies and how much they've invested in trying to protect this data. To me, they're a victim of a criminal who's come in and stolen data, but what's pegged on them is these quick lawsuits, and my issue with these lawsuits is that they don't know any facts besides that a breach occurred, and yet there's this expensive class action litigation, and I have never seen a plaintiffs firm come back and say, "you know what, after discovery, we realized that it actually was pretty reasonable the cybersecurity measures that you had in place." Never ever have I seen that. Never have I heard of it, and I would bet money that it has never actually happened because I think essentially what happens is you have, "oh data breach—sue—how much money can I get out of you?" And that to me is this huge victimization of a victim already. I would feel differently if the lawsuit was based upon, "okay here's information you should have done, X, Y, and Z," but that's not what I see. What I see is: there was a breach, and there's a lawsuit filed the very next day with to me has no basis because everybody can be compromised. Just because your company was compromised, doesn't mean you did something wrong. And then what happens in these class action litigations is that these people get what, maybe like a dollar and twenty-five cents or something, and then the plaintiffs' attorneys are walking out with a million dollars, and so I have a lot of trouble stomaching that.

Connor Glendinning: Could you talk about the role of statutory damages in that as well, and how that plays into award amounts?

Patricia Carreiro, Esq.: Yeah, so with statutory damages—these are the laws that basically say if there's a violation typically you owe the greater of actual damages or like $2,500 per violation. So, if you think about it alleging a violation of something on your website that is $2,500 times any person whose visited your website in that period, so it quickly multiplies, multiples, multiplies. What that means is when the plaintiffs firm comes forward and says, 'here's your exposure,' it's a massive number right because it's for any person who's visited the website and then multiply, and maybe they visited it multiple times, so then we're going to multiply it some more, and so that creates huge exposure for a company just based upon those numbers. I have much more faith in regulators because regulators can then exercise discretion in enforcement and say, 'okay, I understand, do I really want to pursue this?' Versus what I see in class action litigation is, 'let's drive up the numbers and make this class as large as we can and then get a ton of attorney's fees out of you when we settle this case,' and not actually have to establish it because these things aren't going to trial because it would be too expensive because as a company you're not only paying your lawyers, but you know you're going to have all those fees that you're going to have to pay the plaintiffs law firm as well, so typically what you say is like, "this isn't worth it; just make it go away." So, for me it often feels like just a shakedown because it's like, "how much will you pay me to be quiet, and I'll never have to prove my case at all."

Connor Glendinning: Shifting to thinking about all of this on a global scale. For a company—a large transnational corporation—how do they manage so many different privacy laws across the globe?

Patricia Carreiro, Esq.: It varies. So, to cover sort of two views on it, you'll have some companies who will have a lot of different processes in place, so maybe they'll be like "if you're in that state, here is what we owe you in rights, so we'll just do that." That's not typically what I see. What I typically see is, "okay, we're going to treat everybody the same. Let's bring everybody up. Even if your state wouldn't give you that right, we've already set it up so we're going to treat everybody the same irrespective of what state you're in. We're going to extend these rights to you. We've already got the privacy policy. We'll give you the privacy policy we've already drafted it." So, they just sort of say, "okay, everybody comes to this level up here based on whatever the highest is across all these jurisdictions." That is what I most often see. I do see some companies do the more narrow analysis, but that analysis takes a lot of

resources, so it's often just not worth it, and I think it becomes less and less worth it the more privacy laws we have on the books.

For background there's a ruling in the E.U., the *Schrems II* ruling, that struck down the previous agreement on data privacy. However, they implemented a new adequacy decision framework.

Connor Glendinning: How are your clients approaching the adequacy decisions?

Patricia Carreiro, Esq.: Yeah, so none of my clients are relying upon it. So, for anyone who doesn't have the background on what this is, basically the [General Data Protection Regulation (GDPR)] says if you're going to be shifting like an E.U. resident's data outside of the E.U., they want to make sure there's certain protections in place but they accept that data flows to certain countries are adequate, so that's what we're talking about when we say an adequacy decision. If you don't have adequacy, then what you would need to have is other stuff. So, for example, like standard contractual clauses that are providing that two parties are agreeing that certain protections are going to be in place for this data to keep it safe. So, one issue that's come up with my clients anyway is that they don't want to rely upon adequacy because if they rely upon adequacy, and it's expected to be challenged again, then they just put all this work into it, and then they've got to redo it over and over. They'd much rather have something steady that they can rely upon, so my clients are typically just sticking to having standard contractual clauses in place rather than relying upon adequacy for fear that that it is going to go away, and then they've got to redo all this all over again.

Connor Glendinning: To start thinking about a conclusion to wrap things up, how do companies move on from litigation?

Patricia Carreiro, Esq.: Plenty of small businesses, when they're compromised, don't come back. It's a very hefty proportion of them because it gets very expensive.

Connor Glendinning: Do you think that reputational harm can be managed in this and how do you weigh that against the economic harm in making decisions in litigation?

Patricia Carreiro, Esq.: It all goes together actually as part of responding to a data breach. They have [public relations] coaches that you can retain that help you with your messaging, so I think that can certainly be managed. I mean it's always going to come up, but certainly something that you factor into the decisions and how you're portraying it

when you're responding to a data breach—there's a couple things you really do want to do and don't want to do. One: you want to provide the notices you're supposed to provide. You want to be truthful in them. If you make a mistake, you own up to it. That's part of the basics of what you do when responding to these incidents, and that's typically where people get into trouble.

Connor Glendinning: Do you think it's inevitable that businesses that face this sort of litigation may face it again and is there anything they can do to really protect against that moving forward?

Patricia Carreiro, Esq.: Not a hundred percent. I mean what they're going to do is try to avoid being compromised, which they are doing, but no matter how much you invest in that, you will probably be compromised again. That's just the reality, and that's why I get so upset by all the class actions because that's not fair. Just because they were compromised, doesn't mean they didn't try, doesn't mean they weren't doing reasonable things. Stuff happens. It stinks that it happens, but that's life. We don't need to then throw them under the bus and run them over again. The thieves that came in and took their data are already dragging their name through the mud. We don't also have to be like, "and now you owe us millions of dollars that'll all go to the plaintiff's attorneys instead of the people whose information was actually compromised."

Connor Glendinning: Thank you so much. Are there any questions from the audience right now?

Patricia Carreiro, Esq.: I should have started with a disclaimer: I only do defense side, in case that wasn't clear.

From the Audience: Thank you for being here. It's been very interesting. I don't have a background in privacy, so I apologize if there are any unfounded assumptions. You had mentioned that ideally there would be a shift from class action litigation to a regulatory agency pursuing these claims to avoid that unfair pursuit of companies. What would that look like in practice? Has that been proposed? Would an existing agency be divided or a new agency be created? How close is that to happening?

Patricia Carreiro, Esq.: Every state already has a data breach notification law and then there's a regulator involved there and can enforce. So, there's some states that are more active, like there are some states where you send out a data breach notification letter to them, and you know they're going to follow up and ask you questions. Like Indiana

being one of them. If you provide them a notice, and you'll be like, "there was the information of one person from India impacted in this breach," and they will send you a letter asking for further information. So, what often happens is regulators then get together from like multiple jurisdictions. For example, if a credit agency was compromised, and you had all fifty states' attorneys general getting together and entering a settlement with them over the practices that they had in place. So, these things do already happen. The bigger risk that monetarily companies face is typically from those class actions, and that is what concerns me more than are regulators coming in and actually trying to gather facts about what happened and then deciding what they're going to, so whether they're going to require additional cybersecurity because maybe they think something should have been done and wasn't, and what sort of fines they're going to bring down because at least them I trust their discretion a bit more. And particularly in regulated industries like insurance, right, often times you get into issues that result if you were supposed to have––like a plaintiffs firm doesn't actually care about the law, in my view, and what happened—versus a regulator who knows the industry and how people generally do things, like in the insurance industry they'll send out questionnaires and gather information from people like, "hey what are you doing with data, how are you protecting this data," that kind of thing. And they know the industry and what should be in place, and they can actually decide how hard they want to come down versus having this, to me, an incentive of driving up cost to grab those attorney's fees. That's why I trust regulators more than I trust private litigation. I think it's just a different incentive.

Connor Glendinning: I'm going to ask you one quick follow-up. We talked about the privacy risks of the insurance industry, but what are the insurance options for companies to insure against these cyber risks?

Patricia Carreiro, Esq.: So, there is cyber insurance—the premiums like doubled last year—but it is out there, and you also have something called silent cyber coverage. Basically, there's an incident and then you may get coverage under other policies that you have that maybe wasn't initially planned, but it's happened in a number of cases. As well, the issue with cyber insurance is that with lots of other insurance, you have like forms, and so it's like here's the language that we've agreed upon, and then you have more precedent interpreting that language to tell you what's actually going to be covered. With cyber insurance, you don't have that standard form, so what you get into is that there's this uncertainty about what exactly is covered, and I've seen insurance companies be very good about paying these claims, but you have that risk, and there's a lot more variation in the policies, so it's harder to set

precedent that's more in point for your particular policy. So, what you have in cyber insurance is it's typically like a Chinese food menu: you can choose, "I want this coverage from column A and that coverage from column B, and I'm going to wrap that altogether to form my cyber policy." So, all those variations create more difficulty in interpreting what's actually going to be covered.

Connor Glendinning: Thank you so much for speaking to us!

[Applause]

Connor Glendinning: Alright. We're next going to hear from Professor Mason Clark who is the Bruce R. Jacobson Visiting Assistant Professor of Law at the Stetson College of Law. He is a three-time graduate of Indiana University, having received his bachelor's degree there, a master's in cybersecurity, and also his J.D. He has an extensive background in privacy and cybersecurity. He has served as global deputy privacy officer for an international life sciences company. He has worked on hundreds of data breaches through the incident response cycle, and he currently serves as a professor at the Stetson College of Law. His forthcoming article focuses on where privacy rights are best placed to keep information about reproductive health from law enforcement, and he's going to speak to us today about the E.U., the GDPR, and about the human rights roots of the E.U. privacy law.

[Applause]

Professor Mason Clark: Well good afternoon everybody. Thanks so much for being here. As someone who is relatively new to privacy academia, it's so awesome to see so many people at least tangentially interested in it. I really encourage you if you haven't yet—I don't know how many 3Ls we have literally hanging on in the last two minutes before you graduate—but for any 2Ls in here, I strongly advise you not only to have an interest in this area, but to take any class possible and consider it for a career because it's incredibly fun. I could not imagine myself doing something like trusts and estates for the rest of my life, and I've had an incredible first six to seven years of my career working in privacy and cybersecurity, so it's great to see everybody. I'm going to talk about the origins of privacy in the E.U. and how that compares to the U.S., and I teach an entire semester's course on that, on comparative privacy in the E.U. and the U.S., so I'm going to boil it down to about twenty minutes, which is virtually impossible. I don't want to flip the script on you because you're not in class, but does anybody here have any idea why the E.U. and more generally Europe might have seen or viewed privacy as a

human right from the beginning? Think about a conflict in Europe that may have suggested that we should look at privacy as a human right.

From the Audience: World War II

Professor Mason Clark: World War II, very good. On a more serious note, there's a reason why German data protection authorities in particular were the most aggressive in helping the GDPR come across the finish line when the E.U. finally passed it in 2018. There's a reason why the European Union views privacy as a human right, and it's because privacy started as a human right in 1948, right? So, the U.N. post-World War II, and the Universal Declaration of Human Rights, and in Article 12, we have the first codification of the right to privacy in your family, in your private life, and in your reputation. So, this is 1948, and the very next year the European Convention on Human Rights essentially copies that human right into their own convention on human rights in Article 8, and from that point on, privacy was viewed as not necessarily a market value, which is what's so fundamentally different from what we see in the U.S.

And I was a practitioner too, just like Trish. I also disagree with privacy plaintiffs that are just looking for a cash cow, but there is a reason why U.S. privacy laws focus so much on the consumer to the business relationship and the idea that we have to balance power between how much that company's making off of your data, and how willingly or unwillingly, they're violating your privacy rights to do it. There's this kind of economic underpinning of U.S. privacy laws. In the E.U., not so much. Even moving past the conventions on human rights, in 1993, the European Union is formed, and almost two years later—less than two years later—we had what was kind of the precursor to the GDPR. It was called the Data Protection Directive. Now, I don't expect anybody to know the difference between a directive and a regulation, but a directive simply just lists the rights that all member states in the E.U. must protect, but it doesn't tell the member states how they can protect them. One of the reasons the directive is effective is that it allows different member states in the European Union, for example, Germany, France, Italy Ireland, to pass different laws that take into account the cultural values of each member state.

Now, you could make the argument that we could adopt that system here in the United States. Every different state or at least regions of different states have different cultural values around privacy, but in the E.U., they universally as member states agreed that at least for now, that's the best thing to do, and it wasn't until 2018, when the GDPR passed that we had a regulation. A regulation is similar to a directive, but it actually imposes the standards and the obligations, and the regulations on

companies operating in the E.U. And the GDPR—I don't even know how old most of us were in 2015, but one of the big scandals that preceded the GDPR was the Ashley Madison scandal, and it was revealing who you were sleeping with, who you were having an affair with. And that included everybody, Joe Schmo in Ireland, all the way up to members of parliament in the U.K. And there's an idea of the GDPR that privacy isn't just an economic imbalance between the companies operating in the E.U. and the consumers in the E.U., it's that we have to protect privacy as dignity. We have to protect privacy as reputation. We have to protect privacy as the right to engage in trade union membership. We have the right to engage in religious observances. We have the right to love who we want, when we want, and however we want. It's a fundamental difference that still to some extent plagues privacy advancements in the United States, and the GDPR gave us eight fundamental rights.

One of them, the right to be forgotten, is more colloquially called here the right to delete—the right to delete your information. And many of those eight rights that came from a human rights base were actually adopted in the United States in the consumer context. The right to know; the right to access; the right to delete; the right to rectify, which is the right to change and correct information; but the right to be forgotten is probably one of the clearest examples of privacy as a human right in the E.U., and it was one of the first rights that was conceived of while the GDPR was being made. It's the idea that once my relationship ends with a company, or once my relationship ends with a government agency, or once my relationship ends with my employer, you shouldn't be allowed to retain not just the data, but you don't retain the leverage over me that that data provides. And again, here we think of it as, "I want Target to delete my information because I'm so sick of getting Baby Shark advertisements for my two-year-old son because we're trying to break his addiction to Baby Shark." But in the E.U., the right to delete is more commonly exercised, you know outside of Meta and Google, outside of those big players in the space. It's exercised against employers; it's exercised against organized places of worship; it's exercised at trade union memberships, right? It's the idea that what you knew about me then and the leverage that it gave you should no longer apply now that we don't have any reason to be involved with each other.

So, from 1948 until 2018—70 years—you saw consistent use of human rights as the bedrock. That's not to say the GDPR isn't economic, it absolutely is, and we'll get to that in a second in kind of the data trade war that has gone on between the E.U. and the U.S., but it is to say that the bedrock was always in the concept of privacy as dignity. You know, in the United States, we talk a lot about the difference between decisional privacy and informational privacy. Decisional privacy being the right to bodily autonomy; the right to keep the government from interfering with

your private life, something that was protected up until the *Dobbs* decision. But in the E.U., that truly was the beginning of privacy. It was the right to operate your family and control your reputation at your discretion. And now, in the trade war that has begun between the E.U. and the U.S. ever since I was an attorney and probably will continue for the rest of time, we are seeing a switch back to informational privacy—the idea of just controlling your data because it has economic value.

So, really quickly, I know Trish and Connor discussed you know the transatlantic data trade issues that we've had, and the reason that it's become so burdensome is because there is one individual in particular named Maximillian Schrems who is an Austrian privacy advocate—activist—who started a nonprofit called None of Your Business, and in the wake of the Snowdon revelations, all of a sudden, he said we should never ever send data to the United States again because of NSA surveillance because of CIA surveillance because of the relationship between government agencies and large corporations. So, he invalidated twice in a row two different frameworks that we had between the E.U. and the U.S., and it's important to remember that the E.U. isn't just a political union. It started as one. It started as a bulwark against genocide and communism and post-World War II concerns, but not only is it just political, it's an economic union too. There was money to be had by European regulators forcing American companies to undertake mechanisms both contractually, procedurally, even in adjudications. There is an incentive for American companies to do that, and Schrems knew that, and that's why we have the *Schrems I* decision, which killed the safe harbor that was one of the first iterations of data transfers between the E.U. and the U.S., and then he killed the second version of that which was the privacy shield. And, honestly, I do have to give him a little bit of credit. Even as a practitioner, I remember signing my clients up for privacy shield, and basically all it asks you is, "are you compliant with the privacy shield," and you say, "I think," and now you're certified. So, there were inherent problems, but the biggest concern was government surveillance, and the way the U.S. allows our law enforcement agencies to surveil private citizens and more importantly, under the GDPR, European citizens.

So, the most recent iteration of this is the new data privacy framework. President Biden and a couple of data protection authorities from over in the E.U. agreed to terms, and it is in effect. We do have an adequacy decision, but like Trish, I absolutely agree, it's probably not going to last very long because the one change that they made to try and account for Max Schrems' concerns and the E.U. data protection authorities concerns, which was this NSA surveillance and this big government surveillance and law enforcement surveillance, and the only thing we changed in the data privacy framework is that now law enforcement must

show that there is a necessary and proportionate need in order to obtain mass surveillance and mass data collection to protect national security. That doesn't sound very strong at all. In fact, it kind of just sounds like they literally just went to Google and found synonyms for important security interest. So, now we have companies who are either—you know if they have a good counsel like Trish who's advising you, "I wouldn't bet the farm on this adequacy decision," but you have so many companies that are not like that, that are scrambling, paying fees, meeting with data protection authorities, trying to read guidance, trying to hire new attorneys to try and comply with this data privacy framework, and we have no idea how long it will last. But one thing that I would bet at least half of my son's college savings on, it's not going to last very long, at least in its current form.

And there's another kind of consequence of the E.U. taking the lead on privacy is it's so influential in the way that the United States does privacy, not only in the types of rights that we've started to protect but also in the way we adjudicate privacy here. How do we vindicate these rights? Even though it's influenced how the U.S. does it, the E.U. still has fundamentally different ways of not only forcing privacy to the front of American companies' minds but also enforcing privacy and forcing these companies to keep their business in the E.U. So, for example, under the GDPR, there are data localization requirements in some circumstances. So, if you are Meta, a former client of mine, and you've been operating in the United States and you've been operating in Ireland for the past fifteen years, new data localization requirements is becoming an increasingly serious problem for companies like that who have large swaths of data, but they're being told by data protection authorities that you have to keep it local in the E.U. where we have one of the strictest if not the strictest privacy regime in the world. So, here's your choice, play ball with us, or get out of Ireland. Seems like a relatively harsh choice even though we all might have different opinions on Meta and what they're doing, but at the end of the day, it's a forced choice because the E.U. has so staunchly supported privacy and so smartly used it political and economic capital to keep data in the E.U. and to force American companies to play ball. And I'm not totally sure what we're going to see if the data privacy framework is finally, or for a third time, stricken down by Max Schrems, Schrems III. I don't know what's next. One thing we do know though is that we are consistently behind the European Union when it comes to privacy regulations, cybersecurity regulations, and artificial intelligence regulations.

The E.U. again as a matter of dignity, as a matter of human rights, as a matter of social protection, not market protection has passed or is about to pass in maybe the next month, the first comprehensive artificial intelligence act. And it is not business friendly, at all. It essentially creates

different categories of artificial intelligence and it sets—first of all, if it creates an unacceptable risk, the use of an artificial intelligence creates an unacceptable risk, it's not allowed. So, we already have this strong prohibition against at least one class of artificial intelligence, and I'll you tell you what that is. There's cognitive, behavioral manipulation of people or specific vulnerable groups; social scoring; biometric identification or real time and remote biometric identification systems such as facial recognition. That's a lot of industry that is heavily involved in artificial intelligence not just stateside, but also in the E.U. too. Beneath the unacceptable risk, they've created high risk companies, so companies that use artificial intelligence to target children, to provide medical information or devices, to provide a whole host of what we kind of consider analogous here in the United States to critical or high risk individuals or products and services. They have to undergo significant risk assessments, testing, validation, third party assessments, etc. and again, the reason the E.U. wants to be out in front of that and is always ahead of the United States.

There's kind of like an inside joke with privacy attorneys that we're always like two to three years behind even though we were writing the same laws at the same time. I don't know if it's just because folks in the European Union work faster. I have a feeling that can't possibly be true, but there is something about the E.U. that is always ahead of us. But again, laws like that, they want to be in front of it because one, they have to honor the human rights of their citizens, and two, it's economically advantageous to be the first player in the game and set the rules for artificial intelligence. And so are we going to see something like that in the United States? We've both been hoping, or maybe not both of us, but we've both been in conversations with other privacy professionals who are waiting for a federal privacy law. I don't think my two-year-old son's going to graduate college before we have a federal privacy law. We can't even agree at the congressional level if the sky is blue let alone whether we should continue to allow private rights of action that are clearly hampering business or if we should allow for preemption. All of these states laws that have wreaked havoc—is one way to look at it—on companies operating in data transfers. These states have already passed pretty significant state laws. It's going to be a real bummer if they worked for it for three years only to have a federal privacy law that's watered down and meant to apply across industry, if that shows up and preempts the state law. And so there's so many issues with trying to keep pace between the E.U. and also honor that kind of U.S. system of privacy and data protection, and we will always be second because we respond to not only what's happening in the E.U., but we respond generally to economic concerns around data protection and not so much around the human rights aspect of data privacy.

How am I doing on time?

Connor Glendinning: Why don't we take questions?

Professor Mason Clark: Yeah, let's take some questions.

From the Audience: Hi, thank you for being here. I know you were touching on the trade war between the E.U. privacy laws and U.S. privacy laws. Forgive me if this is out of the purview of this conversation, but I was curious about China's privacy laws and if that plays into any trade war between these three big global entities?

Professor Mason Clark: It certainly does, and so first with the Chinese cybersecurity law that first came out. That was the first kind of iteration, at least in my practice so far in the past five years say, that really scared some companies because not necessarily just the cybersecurity requirements, it was the registration of your business, and the certification that you comply with government sanctioned cybersecurity regulations. Also, they introduced, again a concept from the GDPR—the GDPR has its feelers in every single international privacy regime post 2018—but in addition to that they also added data localization and database localization. It's one thing to have your business physically present, it's another to say I'm willing to host a database where I'm not a hundred percent sure that my company controls. So, that was kind of a first iteration of it. Now they've passed additional privacy laws, and they've passed what we'd call a GDPR like comprehensive, omnibus privacy law with the data subject access request rights and things like that. I don't think that companies are necessarily worried about complying with transparency. Transparency's not that hard. The issue is a little more technical, and it's do we want to relinquish control of the data that isn't even ours, right? It's the consumers, but the data that we own that is essential to running our business and the only way that we make a profit and pay our employees, we're not so sure that we are the ones controlling it. That's what's dangerous. Now in other areas—Brazil, for example, passed a very copycat, almost identical version of the GDPR— the concerns maybe aren't as heightened there. And I'm glad you brought up China because I don't know if anybody saw, but President Biden recently signed an executive order that's going to govern what kinds of sensitive data are allowed to be sent and transferred to China, to Russia, and to the countries on the OFAC's sanctions list. We tend to not be as scared of anybody outside the E.U., except in areas where we don't always maintain private control of data, and so those laws have different technical requirements and different privacy requirements, but it's really

more of threshold issue of are we willing to keep our data over there? It's a great question.

From the Audience: I would just love to hear a little bit about the paper that you're working on right now.

Professor Mason Clark: I didn't pay her to say that. So yeah, my paper's called "Consumer Privacy and the *Dobbs* Disruption" because even though I've talked a lot about the E.U., really the only reason I talk about the E.U., and write about the E.U., and speak about the E.U. is just by happenstance. I started on May 22, 2018, and three days later the GDPR went into effect, and I was the only associate in the group other than my wife, she was also an associate in the group. I got the GDPR and she got HIPAA. So it's really just kind of by luck, but after I spent the first eighteen months working eighty hours a week to figure out what the hell is going on in the E.U., I am a consumer privacy practitioner. And one thing that immediately struck me about the consumer privacy laws that had been passed since the CCPA, the California Consumer Privacy Act, one that we consider to be one of the more strict if not the most consumer privacy law in the United States, one thing that has always confused me is either these consumer state privacy laws wholly exclude your compliance or exempt your compliance with that law if you're responding to a government inquiry or a legal obligation. Or they only very trivially limit what you can give, maybe they say you can still give it to the law enforcement agency, but you need to comply with some of the other requirements of the law, like you need to transmit it to the law enforcement agency securely. I think that's become increasingly problematic in light of *Dobbs*. In my article, I give the hypothetical where someone travels from Idaho using an Uber and using their cellphone to go receive reproductive healthcare at a cash pay clinic. A cash pay clinic is not going to be subject to HIPAA, so HIPAA is not going to save her. The only privacy you might have, that you might be able to rely on, is a state privacy law that you might be able to rely on that prevents Uber and prevents Apple or whoever your phone manufacturer is from giving that data fully to a law enforcement agency. There are other laws that will protect against a law enforcement subpoena.

So, in Washington, I write a lot about in my paper about the Washington My Health My Data Act, which was meant to be kind of the ideal privacy law to address this issue, and I think it failed miserably, but Washington has what's called a shield law, so if a law enforcement agency, or if the Idaho attorney general sends a subpoena for all of that woman's reproductive health information to find out whether or not she broke the law by travelling to Washington, the clerk in Washington is supposed to summarily reject that subpoena. But what about if there's no

subpoena? The Washington Post just came out with an article a couple of months ago that something like two-thirds of the major pharmacies in the United States will hand over your medication information and other information that can be implied from your medication such as your diagnosis, what you're being treated for. They will hand it to a law enforcement on a silver platter without a warrant, without a subpoena. Basically, someone comes in and says we're the cops, give us the information, or we're the investigators give us the information we want. Now you can imagine a pharm tech going "okay," right? And I'll finish with this, the reason I advocate that the state privacy law should do this because brilliant scholars like Danielle Citron, Daniel Solove, Anya Prince, they'll all say well we need privacy as a human right, or we need privacy as a civil right, or we need a federal privacy law. I think those are all great ideas, but I have zero faith that if we can't even pass a politically neutral privacy law, we're sure as hell not going to pass one related to reproductive privacy. So if you want reproductive privacy to be a state's issue, then the state privacy law needs to address it. Thanks for the question. Shameless plug, it's forthcoming in the University of Michigan Journal of Law Reform.[2]

[Applause]

Connor Glendinning: Glad you found a home for it. Thank you so much for speaking to us. Okay, we're going to move into a panel style format moderated by Professor Lidsky rethinking privacy expectations and thinking about what we've heard about so far, what we can expect down the road, and thinking about some of the recent legislative changes. Professor Lidksy is the Raymond & Miriam Ehrlich Chair in U.S. Constitutional Law having taught at UF Law since 1994 with a five year stint at the University of Missouri School of Law as Dean. She returned to the University of Florida in 2022 and relevantly to this topic, she is one of two recorders currently working on the Restatement of Torts (Third): Defamation and Privacy. So without further ado, welcome Professor Lidsky.

[Applause]

Professor Lyrissa Lidsky: So first off, I have to say that thank you all for coming, and I am particularly glad to see so many of the students who are taking my Advanced Torts class in here because we have just been studying the privacy torts, and the privacy torts relate to this broader

2. Mason Clark, *Consumer Privacy and the Dobbs Disruption*, 58 U. MICH. J.L. REFORM (forthcoming 2024).

picture of privacy that happens to be very complex in the United States. We talked a little bit about how it's a hodgepodge rather than a more unified whole as it is in the E.U., and so I guess I have questions for both of you. I was thinking first when you were describing the inadequacy of class actions to police data breaches and get the balance right between protecting the consumer and protecting the companies that are really trying to do the right thing and act in good faith, do you think that the tort system taking that on is partly a product of broader regulatory failures with things like Professor Clark was talking about with your failure to have a comprehensive federal privacy law or our faith in regulators maybe not being so high given our comprehensive failures of that kind?

Patricia Carreiro, Esq.: I feel like that could be addressed by then addressing that problem. Like if you think that's the problem then okay maybe provide more funding to regulators to do more. Although I feel like they can sort of fund themselves because they get some pretty hefty fines out of noncompliance, so I feel like they're an efficient government actor because you bring the fine, you funded yourself and many others particularly at government regulator salaries for quite a while. I spent some fun internships in different government organizations, and I've seen the regulators be like, "I just paid my salary for the rest of my life." So, I feel like that is an issue the regulators can address, and they can self-fund themselves versus the incentives that I have on the privacy side of it. Maybe it's just that we restrict the amount of money that goes to these plaintiffs' firms and require more to go to the consumers themselves. That would also make me happier. It's that sort of big cash out by a plaintiffs' firms and a dollar something to all these people whose information was involved that I find shocking.

Professor Lyrissa Lidsky: I sometimes teach torts; I often teach torts; I have often taught torts, and I guess I've always seen torts in a way as the conservative solution to otherwise having comprehensive government agents involved in your life. Like torts is the backstop, it's the more conservative option to utterly comprehensive regulation. Do you think that in the United States we worry about regulation not being enough because of regulatory capture problems?

Patricia Carreiro, Esq.: I think it's possible.

Professor Lyrissa Lidsky: Was it enough at the beginning? Because I've been around a while now as you can see from my visage. I remember some of the initial data breaches and there was evidence that the companies were just lackadaisical, and then someone would warn them that they had a security breach, and instead of fixing it, they would cover

it up, and go after the person that warned them of the data breach. At least in the early days, there wasn't sufficient regulation to counteract some of this.

Patricia Carreiro, Esq.: I think that's very different now, at least with the clients I have. So, I think at least if they're going to pull that, they're not coming to me, which would make sense because why would they pay me to ignore my advice?

Professor Lyrissa Lidsky: And by the way, Professor Clark mentioned Ashley Madison. Just so you know, it was a site where you went to find a partner for an affair, and it was really tawdry; it was really disgusting. You know there was speculation that a lot of the women that you could find to have an affair with were bots. Go back and do a little research. There's some really interesting stuff there.

Patricia Carreiro, Esq.: And the added fun was that these people were people that had deleted their account supposedly. Turns out the info wasn't deleted, so when they got breached, it was like oops you weren't supposed to have my data on my affair anymore. Oopsies.

Professor Lyrissa Lidsky: And then it opened it up to extortionate uses. Good stuff.

Patricia Carreiro, Esq.: So much drama in privacy. It's fun.

Professor Lyrissa Lidsky: So Professor Clark, I have a question for you about the European conception of privacy and how we ever get to something like that. We used to have a program in France—best thing ever—and I teach privacy torts, but I'd do a comparative privacy with the E.U. because it had French students and American students. And it was really educational because you got into the sense that it's this utterly different mindset as you said, and I used to say that we fear the government and they fear Google because their view of corporations is so different, but how do you transplant an idea of constitutional rights that seems to me to be very different because we think of constitutional rights as rights against the government, and they have that too, but they also think of the constitution of providing affirmative rights that might be binding against people other than the government. And so if we want to really protect privacy and move from this economic conception that you've talked about how do we get there with our limited constitutional conceptions of rights? Even if we had a privacy right overtly in the Constitution.

Professor Mason Clark: It's an excellent question, and I think the way I would answer it is, one of the things that makes the E.U. regime—the GDPR and the E.U. privacy directive—what makes them so successful is from the beginning, they had the structure for this. We, of course, have state attorneys general in addition to federal regulators like the FTC, but we don't have truly independent authorities that dedicate staff, money, and expertise for these kinds of things. So, I think that even if we wanted to adopt a comprehensive privacy law, that looks like the GDPR, has extraterritorial scope—we can finally start picking on the E.U. like they pick on us—how are we going to do that even if we can finally wrap our heads around it and maybe this generation of students philosophically supports that as a human right? Who's going to help us? Because the FTC is so busy enforcing unfair and deceptive acts for economic issues related to privacy. We have the OCR enforcing HIPAA. We have these different agencies that all do other work than privacy, and they all typically have some kind of economic consumer privacy imperative, but what we need are data protection authorities. We need an independent resource mechanism and arbitrators, and we don't have any of that. And I think it's telling that one of the new things in the data privacy framework that we changed here in the states to try and allow more transatlantic data trade is the requirement that we have an independent recourse mechanism that is actually independent and not what we had under safe harbor and privacy shield, so we're outsourcing all of that to the E.U. Wouldn't it be nice if we had that here? Maybe that will foster kind of an attitude change and a truly regulatory or legal regime change too.

Patricia Carreiro, Esq.: So is that a new? I don't even know what to call it.

Professor Mason Clark: Yeah, the American Data Protection Board––the ADPB. We've got the EDPB over there, and maybe we'll just say that's a great idea; we're just going to change one letter.

Professor Lyrissa Lidsky: Well part of your argument is we don't even need to adopt it because the tech companies have to adopt it because they have to go to the lowest common denominator, and so we can just rely on them to make the regulations, and then they'll comply with theirs, so it'll benefit us.

Professor Mason Clark: Perfect, less work for us.

Professor Lyrissa Lidsky: So, I was going to ask you, both of you kind of alluded to this. Is Federalism the problem in the United States or the solution? You seem to think states are wonderful. In your practice, how's California for you?

Patricia Carreiro, Esq.: It keeps me very busy.

Professor Lyrissa Lidsky: Can you talk a little bit about how you serve clients when you have you know fifty states and then these federal regulators? Who do you have to satisfy?

Patricia Carreiro, Esq.: Everyone, everyone, right. So, you often start with California if you're just not in a particularly regulated industry because it's the most specific, and then you sort of tack on the appeal right from all these other states, and then you're like, well that was fun. If you're in a really regulated industry, then you'll often start with whatever that specific regulator has.

Professor Lyrissa Lidsky: HIPAA, FERPA, you know.

Patricia Carreiro, Esq.: Right Gramm-Leach, and then you know which particular interpreter of Gramm-Leach and then go from there because you have that divided up, and then you can layer on concepts that you see are missing. Then that also goes to this point of with these really large organizations, you're overlaying a lot of different exceptions and oftentimes trying to be like, "okay, so in California I'm seeing okay well that's health data, so maybe we can exempt that, no well that other entity we have, like that affiliate has the Gramm-Leach exemption, but wait in sone states you get both the financial institution and its affiliates to be exempted," and so you just start piecing together all these exemptions. Sometimes what you get is you just say, "forget it, just comply with everything, and I don't want to worry about it because we don't really know how it's going to be interpreted yet," right, because these are new laws. So, you also get into this question of okay even that Gramm-Leach exemption, how do you interpret that and are you going to interpret the same way that the state regulator like that department of insurance is interpreting that or are you going to view that exception more narrowly because that would be the exception you know pulling stuff away from your power, and regulators do tend to interpret as broadly as possible, right, so what happens when you have different regulators with different incentives over interpreting that exception?

Professor Lyrissa Lidsky: Wow, so I'm going to follow up with [Professor Clark] on one federalism question, but I want to do one follow up with you first. Given what you've described and the complexity of your practice, what would you advise somebody who's a 1L or a 2L out there about how do they get ready to do what you do?

Patricia Carreiro, Esq.: Learn to learn. Really, the law is changing so quickly. There was no privacy course when I was in law school. Never took it. I probably would've been like, "that's interesting, I don't know what that is," and moved on. I'm going to do something practical; now it's my entire career. Just learn to learn, and if you are doing something, like when you get into practice, and you realize, you know what, I'm not enjoying this, do something else. Like, make that choice. Work hard and find something that inspires you to want to work hard. Don't go through the drudgery. Life's too short, and there's too much interesting stuff happening.

Professor Lyrissa Lidsky: I could not agree more. I'm a cancer survivor, and that was the rule. Please don't have to get cancer to learn that life's too short to be unhappy. I could not agree more with what you just said.

Patricia Carreiro, Esq.: And you can change. You can change. When you're looking for firms to go into. Look for a firm that allows you that opportunity as well, and identify a firm with a culture where you can learn from your colleagues that do stuff that's totally different. Make sure that it's a firm where you can pick up a phone and call someone or walk into an office if they're in office, but identify the culture and the capability and then make that choice and be conscientious about it. It's your career. Do not have it formed by other people. Define your success and then make your choices.

Professor Lyrissa Lidsky: Mason, how 'bout that federalism for you?

Professor Mason Clark: It's so funny because I'm not in any way shape or form really a federalist. I wrote a paper advocating for more reproductive privacy rights, and in some ways came out with a federalist solution, and really to be quite honest, it was out of exasperation, desperation. It's the last thing we have, and what I thought was, again I kind of mentioned this, every conception of privacy as a civil right or as a federal initiative, or as a human right, I one-hundred percent think is amazing—fully support—but it's not happening. What's happening is state legislators are getting this done. Texas just passed one of the most

restrictive abortion bans in the country. It also just passed one of the most comprehensive privacy laws that looks a lot like the California Consumer Privacy Act. So, if we're going to see a wave of consumer privacy at the state level, why don't we just hop on the wave and ride a little bit because we have to act now. And sorry, it sounds kind of pitchy, but if we want to counteract *Dobbs* now, well the thing that's working really well is state privacy laws. Let's add one little provision that would keep a company from sharing that information with a government agency or law enforcement. Make a quick change. In fact, it's already changing. We've already seen Connecticut, Vermont, Colorado, and now Washington, either pass new laws or amend existing ones to try and account for this issue. Let's keep the momentum going, and if it's a federalist solution, I had no idea that I'd be submitting papers to the Harvard Journal of Law and Public Policy or anything like that, but maybe that's where the policy is going.

Professor Lyrissa Lidsky: Well, I also teach conlaw now. I spent most of my career teaching mostly torts, but I ride at the intersection of torts, and conlaw, and defamation. Anyway, the right to travel may have something to do with all of these laws I hope going forward, but we shall see, we shall definitely see. What about the—and this does have to do with conlaw—I'm going to ask about the balance between privacy and first amendment freedoms eventually, but what about the mentality in E.U. law that constitutional rights are never absolute? That you can have proportional restrictions on speech rights; that you can have proportional restrictions on privacy rights; and that everything is proportional and needs to be in balance? This mentality of balance? I see the current U.S. Supreme Court trying to move away from any kind of balancing of rights against each other. How do you do privacy law if you can't really overtly do balancing as against other rights like free speech? Like how do you ever have privacy if it can't ever tip the scales?

Professor Mason Clark: So I also teach—I have a Comparative Privacy and then I teach Privacy Law I, and it's the intro to the privacy torts, and my exam this year was a content moderation law, and what privacy torts could you envision; is it the right regime; should we switch to something else? So, to answer your question as directly as I can, I have no idea how to answer that question because if you can't balance, I don't know what you're supposed to do. But one thing that we've seen in the informational privacy space is the idea of consumer choice, and there's concepts like the privacy paradox, like do we actually trust people to act? You might value privacy, but your actions are completely antithetical to your values for convenience, safety, security, cost effectiveness, whatever it may be. Maybe our only option is to increase ability for

choice and increase informed choice, and I don't know how you—I mean my exam put out a few ideas, but I think they were all half-baked exam answers. I don't know how we practically solve that, but people are moving away from notice and choice, right, because we're trying to look more like the E.U. So, we're trying to fight competing trends I think, so if we take away choice and we can't balance, then I don't know what's left.

Patricia Carreiro, Esq.: So, with the E.U., one thing they're doing is basically like, do you want the internet to be free, right, or are you going to agree to the tracking and pay for the internet? So, I think that's one thing they're tossing around that I'm interested to see where it goes because there is that sort of reality of like, do you want the internet to be free? Well then somebody's going to pay for it, and if the people providing the ads are willing to pay for it, are you okay with that? And what some regulators also come for, and we hear about it a lot in the insurance space, is like, do we trust the consumer to make the choice to protect the information and how protectionist do we want to be, which is something that regulators are always arguing about when they're forming these laws because you have one side being very paternalistic like, "no, absolutely not, they won't understand the privacy policy," and then you have the other side being like, "okay but if we can make it plain language enough for them to understand it, don't we want to give them that choice," because you're right is being traded all the time, but I want targeted ads. It's not going to reduce the number of ads; it's just going to make them actually apply to me, and there's a big generational divide that comes up as well.

Professor Mason Clark: Well it's funny you mention the pay for internet freedom too. There's also new models coming out in some places in the E.U. that you can pay for privacy. Like if you want to use Apple CarPlay or a similar app on a smart car, you can pay a subscription model starting at 150 bucks a month or something like that in order to have your data immediately anonymized. Now, it's going to suck because each time you get in the car you're going to have to re-setup your Apple CarPlay, which if anyone has to do that because your car doesn't work the way it's supposed to, like me, it's annoying as hell, but is that even really a free choice if you put money behind it, and of course everybody probably shakes their head no.

Professor Lyrissa Lidsky: How is generative AI going to affect your practice and then, you know, all of these privacy concerns?

Patricia Carreiro, Esq.: Yeah well you know for me the big thing is how the definition of data that I have an interest in applies. So, that shift from the personally identifiable, to the personal information, now to any information about me even if its public, which has never been within scope before, and how can you manipulate that data, and what rights do I have, and if I submit that request that I want to correct it, but you know it's already fed into this algorithm spitting out twenty other things. How do you actually delete my information? How do I actually correct that and see it roll forward, and what rights do I have to do that if it's out in the public? I'm sure this goes into your defamation side of things.

Professor Lyrissa Lidsky: Well there's a professor named Jennifer Rothman who's like one of the top people in right of publicity. You may know her work, but she recently testified before Congress, and she argued that you shouldn't be allowed to consent—this is about consent regimes for privacy—when you're like eighteen, or really ever, to all foreseeable future uses of your name, image, and likeness on into eternity because we're at a technological inflection point where we can't foresee the uses that our data or our name, image, and likeness will be put to. And so is that you know, for consent regimes, how do we inform people what they're really consenting to?

Patricia Carreiro, Esq.: Yeah and the FTC has specifically come out about this and been like, "you can't just get permission for like any future use of AI," they're like, "no, unfair trade practice on its face," but you're also in a position with companies where it's like, "well, Trish, we don't know exactly what we want to do. We want to provide this notice, so what do we do?" So part of me is like, "well let's disclose really broadly and then anything you want to do with that data, let's talk about it, so you don't start getting sketchy."

Professor Mason Clark: And maybe an optimistic view of this is maybe artificial intelligence, particularly generative artificial intelligence, right now we already have some great software that's available that helps companies using generative AI classify certain data based on risk. Not necessarily within legal classifications based on what does California think is personal information but based on risk, so that you're not spending those hours doing that. I'm optimistic that maybe generative AI can also help us solve the problem of if this is like the technical, logistical problem of trying to offer fifteen different notices and two different consents on one website. You know, the My Health My Data Act for example requires a separate consent to collect, a separate consent to sell, and then a valid authorization if you're going to use it for a different purpose. That's three different consents within the first fifteen

seconds you go to a website. Maybe we could not think of artificial intelligence as always being this threat to privacy. Maybe the tools this will create can help us proactively manage consent, provide consent, and remove consent when it's been removed by the consumer. Maybe that's a little optimistic.

Professor Lyrissa Lidsky: Well, I had not thought about this until you said it. I had a guest speaker yesterday who works for a company called LawVu, his name's David Lancelot. He's a grad of the University of Florida. Anyways, he's done privacy work and general counsel work generally, but he was talking about the use of AI to harmonize contract review or risk review, and I wonder, you know, I've often thought, you know, in the E.U. they have projects called law harmonization projects, and they'll go and look at member state laws and try to come up with the best harmonized version of them. And we don't have—even though we have the Restatement—we don't have anything truly comparable in the United States that can later be binding, but maybe generative AI will finally harmonize all of these conflicting privacy policies so that you can just go for one. It may solve all your problems.

Patricia Carreiro, Esq.: And we are kind of doing it. I have insurance companies where I'm like, "here's your one privacy policy." It covers Gramm-Leach; it covers state comprehensives for people who are just on your website but haven't gotten your financial product or service yet, so we're a little like, where's that going to fall. So, we've been doing it, but it would be helpful for all these changes that will come to be like okay, AI analyze it. The problem is someone's going to have to program that.

Professor Lyrissa Lidsky: The human has to be behind it at the end of the day, and then you have to judge the output quality, which means you need your expertise to judge output quality.

Patricia Carreiro, Esq.: I'm hoping.

Professor Mason Clark: Yeah, there's a saying that I've heard several times when I was in private practice just starting with generative AI assessment, and this guy used to always say it, and I love it. It was, "AI's not going to replace you, but somebody who knows how to use it will," and rest assured that you'll always need your expertise, but the more you can learn about it, and the more you can use it, the better off you may be. And I also think, you know, going back to your point about creating the one privacy policy, so many of these state laws here require it be in clear and concise language and that you can't force your consumer to scroll all the way to the bottom before they see their rights. Maybe

generative AI can help us create video privacy policies. Maybe we need somebody to convince legislators to allow us to do that, to allow us to use the new technology to provide those in a more readable format.

Patricia Carreiro, Esq.: VPPA claims out.

Professor Mason Clark: Yeah, right, until the VPPA claims come.

Patricia Carreiro, Esq.: So, VPPA is the Video Privacy Protection Act. It's triggered a slew of class actions from people being like, "you disclosed the fact that I saw that ad or watched that video about that product and you needed a separate consent to do that," so it's been a fan favorite among the plaintiffs' bar recently.

Professor Mason Clark: So first we need to repeal that.

[Laughter]

Professor Lyrissa Lidsky: Why do you think that perhaps European lawmakers are motivated differently than at least U.S. lawmakers at the federal level and maybe in some of the states as well?

Patricia Carreiro, Esq.: I mean I think the World War II background was great context for the different culture.

Professor Mason Clark: Yeah, and I mean I think it's a little harder to make that argument the more attenuated we get from World War II, and that's why I say, you know, I don't like when people only categorize the E.U. as it's human rights based and they actually care about their citizens and the U.S. doesn't. It's an unhelpful of a way of looking about it, but you'll see privacy scholarship kind of argue that. The more we move away from that, it really has become a more of a it's made the E.U. politically and economically stronger, and it's kept their leverage even when they're falling apart, even in the midst of Brexit. The GDPR was so powerful that the U.K. was like, we don't want to be a part of you, but we want to take GDPR because that was awesome, and so there is the kind of motivation. And I think what also helped and what European lawmakers definitely still have in their minds because it was relatively recent, the Data Protection Directive before the GDPR, allowed members states to account for cultural values and to account for the things in privacy, even informational economic privacy, that they cared about. France really cared about data minimization. Germany cared about dignity.

Professor Lyrissa Lidsky: Britain cared more about not being erased in the free speech concerns they were very upset about that before Brexit.

Professor Mason Clark: Yeah, of course, and I think that in the states because we view it almost exclusively as informational privacy is a consumer issue and all consumers across the states are having the same issue with the same companies about the same data.

Professor Lyrissa Lidsky: You have here a wonderful audience of people who may be contemplating this kind of thing. Is there something you want to leave them with, or just something you think we missed before they walk out of here about this area of law?

Patricia Carreiro, Esq.: Carlton Fields is great firm to practice in. Always hiring.

Professor Mason Clark: To a point that they made earlier, I went into privacy while I was in law school, and I worked data breaches, and I did GDPR compliance, and CCPA compliance, and state consumer privacy issues my entire time at a firm, in house, academia, and I can tell you that the most helpful thing that you can have right now as a student is practitioner networks through the IAPP, a certification through the IAPP, and then with that you have to pick what kind of privacy do I care about. If you want to be a practitioner, you'll have a lot of fun. You'll work great data breaches. You'll have way more fun than some of your other colleagues, but it is hard work, and you are busy all the time, and if you don't like the firm, then try in-house, and if you don't like in-house, try academia. Do it while you can because no matter where you land in this field, you're doing meaningful work, and you truly kind of are shaping how this generation, including you guys, view data privacy in the states and elsewhere, so thanks so much for being here.

Patricia Carreiro, Esq.: And do some internships, publish things. When I'm looking, that's what I'm looking for. Have you demonstrated an interest with things like certificates? I can tell you that the most recent associate that I hired was on leadership at an IAPP board with me because I was just like, "you seem to know what you're doing, join the party." So, internships, publishing, showing that you're doing something in the area. I did an internship every semester in law school because it was like, do I actually like this in practice? And savor it because in your career, you won't be able to jump around like that. Plus, they bring the books to life.

Connor Glendinning: Do you hear how relevant your note publication could be?

[Laughter]

Professor Lyrissa Lidsky: Wait—one shameless plug, not for my course, which you should take, we're going to take that as a given, but Professor Haley who had a family emergency and couldn't be here today is teaching a privacy course. Also, we have one of the nation's foremost privacy experts, Jane Bambauer, all of the internet law, Rachel Jones, Derek Bambauer. I teach internet related AI things as well, so you have a lot of resources here at this law school that you can take advantage of, and we didn't even get into choice of law, which Professor Lear would welcome you in her choice of law class.

Connor Glendinning: I'm going to open it to questions now, and I can start because I am interested in if all the state legislation in the privacy sphere combined with the changes in privacy law frameworks between the E.U. and the U.S. is going to create much more complicated conflicts of law issues, and how much more complicated you think that might make some of these class actions?

Patricia Carreiro, Esq.: Conflict of laws is pretty academic.

Professor Mason Clark: Yeah, so immediately in an E.U. context, the independent recourse mechanism being allowed to be hosted here in the states if you can find one is going to be weird because it did not work under the privacy shield. And generally, the GDPR enforcement, it's a big scary omnibus law and we just spent an entire hour, and I spend an entire semester talking about how great it is, but really the only big enforcement actions have been against serious perpetrators like Meta, and Google, and WhatsApp, and some of these big players. The rest, I think it's because they don't want to test a truly domestic company that makes twenty-one and a half billion dollars, like a grocery retailer that's experiencing a data breach. I don't know if they really want to test the conflict of laws issue here because I'm not one hundred percent sure they can even do it. The only time they've done it is against other E.U. companies. Now, they're Meta and Google, but its Meta Ireland, Google Germany. It's not the stateside entity. So, maybe the independent recourse mechanism is their long arm into the states, but I have no idea how that's going to work.

Patricia Carreiro, Esq.: Yeah, I think it's interesting because to your point from earlier as well about how the enforcement works because if you have a regulator, they're trying to set precedent—find the best case they can and set an example for other companies, right, so they tend to get some of the most egregious violations versus on the class action side where it's almost like apart from any of the facts that might be at issue. They're going after everything like, "someone was breached, sue them," so I think it's interesting that you have this sort of coming both from different edges and approaches with you know the pros and the cons of each.

Professor Lyrissa Lidsky: Well, and let me add one thing too, so I'm always worried about the weaponization of various areas of law, including privacy law, by rich people to manipulate the stock of public information, and you know under the right of erasure there was some evidence that that was exactly what happened. So, if you're rich enough to afford a lawyer and there's something on the internet that you don't like—not in the U.S. so easily—but you can find a way to go to the regulators and get it taken down. In the U.S., we have that happen with copyright, so sometimes we think, "oh wow, those Europeans are so weird about privacy they care about it so much." You know what we care about so much that they don't care about? Copyright law. So—every tool—it may sound good, but you have to worry that it's going to be used, and I'm very aware of this because I write about weaponization of defamation lawsuits to shut down free speech.

Professor Mason Clark: There's an excellent book, by the way. It's the book that made me want to be an academic a long time ago called The Poverty of Privacy Rights by Professor Khiara Bridges. She's at Berkley, just because you mentioned, and it's something I say in my paper, and it's an idea that really I got from her, and it's that privacy is a right for the privileged in some situations, particularly if you rely on government assistance. But Poverty of Privacy Rights is a great book to read if you have the time.

From the Audience: I know that in a lot of the state laws that have been coming out, data of young children is treated different from other kinds of data, so as far as enforcement, how do you know whether or not something comes from a young child or from an adult, and how are companies sorting these pieces of data?

Patricia Carreiro, Esq.: So, they don't always. It's confusing. The law requires you to try to figure it out, so sometimes I think there's a lot of different approaches you see. The most basic is where you put in the

terms and conditions that you have to be eighteen to use our website because that way if they're not eighteen, you're like, "violation of our terms and conditions," but another piece you see is different tests—people actually having to submit an ID or something that proves their age. There was a joke that we're going to put up like a rotary phone and be like, how would you use this or what is this, so that you can actually see how old are you really based on those kinds of things, but we're still working on figuring it out.

Professor Lyrissa Lidsky: Sorry, I just want to add to that California's really pushing hard on this right now. There was a concern back in *Reno v. ACLU* back in 1996 that we're going to reduce the internet to what's fit for children, and there really is some concern with these privacy laws that it's going to have a dramatic effect, but one of the things it's going to potentially effect is something I write about, which is the First Amendment right to speak anonymously because to the extent that you have to put in credentials and then that enables massive surveillance both by the government and private companies. So, I would just say as general matter always be suspicious of something that sounds like your heart is in the right place. The devil is always in the details, just to mix metaphors will nilly, but nonetheless just because it sounds like its well-meaning doesn't mean that it's not going to have some pernicious unintended consequences.

Patricia Carreiro, Esq.: I feel like everything is well meaning. I feel like republicans are well meaning and I feel like democrats are well meaning. I think it's just like people define things differently. It's like you said, it's in the details.

Professor Lyrissa Lidsky: I'm always most nervous when republicans and democrats unite around something well-meaning because then that's going to be a law that's really messed up.

Professor Mason Clark: They're both going to make lots of money. So, to answer your question with kind of things that are changing now. There's been a lot of talk, it's mostly theoretical at this point, but maybe something if you're really interested in this, you can follow for the next few years—zero proof IDs, so the idea that instead of having to put in your driver's license on the website so that your child can use it, so you've proved that you're eighteen, or that you can use it so that you prove that you're an adult, you would use basically a system that's like tokenization. You'd have a unique token that would confirm across websites because we have things like the global privacy control that will track you through different websites and say that you have preferences for opting out of

information, why can't we use that same technology to create an ID? Now, again, super well intended, and it might be better than having to upload your actual driver's license, but it's still a piece of data that someone somewhere has your full identity. Everyone else has the token, but you have to give it to somebody to create the token, so does that create the same risk as it does if you upload your driver's license, right? So that's a conversation that people are having right now. It's trying to move to like a tokenization system.

Patricia Carreiro, Esq.: One thing I find very interesting within privacy that doesn't get talked about a lot is typically there's a first party data exception to a lot of things, which is like, well you know you're giving me that data and so you don't have to disclose certain things about that, or yes you can do certain things because I know I gave you the data as opposed to if I disclosed it to someone else, but I think that gets very interesting. It really favors the, okay, so you have Google who has first party data on everybody as opposed to if it were like that website and that website, so I think this gets into like antitrust territory and the powers that like data has, and it's one of those things where I'm like, "I think that'd be cool to think about," but no one has paid me to think about that yet.

Connor Glendinning: Final question.

From the Audience: Do you think that consumer protection will ever catch up with human rights, or is it just inherently going to be behind, do you think the only way we catch up is abandoning consumer protection and moving to human rights as our focus?

Professor Mason Clark: Not to plug the paper again, but I think you can read between the lines and my attitude on that, and I think the ship has sailed, particularly when even legal definitions of things that we would consider human rights, you know, the right to make decisions about our family and about our sexuality and about our health—I even argue in the paper that the collection isn't even what worries me anymore or what we should focus on anymore because that business model's never going to change. There's too many lobbies; there's too many companies using it for good purposes too—good collection purposes and uses—but that ship has sailed and we're never going to change the business model. It's super cynical, but to answer your question, no, I don't think we're ever going to abandon that, so now we need people like y'all to start inserting it when you can into legislation and try to bring out what little human rights theory, decisional privacy versus informational privacy, that we have left into consumer privacy.

Patricia Carreiro, Esq.: And there are state constitutions that have the right to privacy inserted—including in Florida.

Connor Glendinning: That is all the time we have today. Thank you all for coming today. Thank you to the Levin College of Law again for making this possible, and please join me in thanking our speakers.

[Applause]