Risa Goluboff: Are you ready to pay your bills with your face? In this episode, we will be talking to UVA law Professor Elizabeth Rowe to learn more about how facial recognition technology is changing society and how we might regulate it.

Elizabeth Rowe: Your face should be your trade secret, and I do think your fingerprint should be your trade secret, and by calling it that we give it a lot of power.

Risa Goluboff: Welcome back to Common Law, a podcast of the University of Virginia School of Law. I'm Risa Goluboff, the dean. We are wrapping up our fifth season today with a very compelling topic and with help from my co-host, Danielle Citron. Danielle and three other UVA law professors have served as co-counsel this season, helping choose and interview guests connected to their fields, ranging from law and psychology to business law, to one of Danielle's own specialties, privacy and technology. Danielle, thank you for finding such a great – and perhaps unsettling – topic with which to conclude the season.

Danielle Citron: Ahh, there's so much unsettling about privacy now in general, so I guess it wasn't too hard to find.

Risa Goluboff: So, as listeners may remember, Danielle is the director of our LawTech Center here at UVA Law School, which serves as a hub for faculty scholarship and student engagement in this area. Danielle also has a new book out – excellent new book – that focuses on similar issues that we will discuss in this episode. So tell us a little bit about “Fight for Privacy.”

Danielle Citron: My book, “The Fight for Privacy, Protecting Dignity, Identity, and Love in the Digital Age” is about why intimate privacy matters and how we're under-protecting it. And it's been really a great joy talking about it and writing about it since its publication in October.

Risa Goluboff: I would be remiss if I didn't mention that it is on Amazon's list of best books for 2022, among other accolades and attention that it's gotten. But that one is pretty cool.
Danielle Citron: Thank you so much.

Risa Goluboff: Oh, it's absolutely my pleasure. So I'm very excited for our show today. So tell us who will be joining us.

Danielle Citron: We are going to be interviewing Elizabeth Rowe, a trade secrets expert who joined our faculty this year. Her work fits right in with the law school's new LawTech Center because she's an expert at the intersection of intellectual property and corporate espionage. So in addition to being the co-author of the first and leading U.S. case book on trade secrets, Elizabeth recently wrote a paper for the Stanford Technology Law Review about facial recognition technology – how far it's already pervaded our everyday lives, and how far it might go, given the example of how facial recognition is being used in China. It's terrifying, and she looks at the framework for regulating this kind of technology through a trade secret lens, which is really creative.

Risa Goluboff: I am getting the feeling that I might want to put some tape over my computer camera after we have this conversation, but I'm very excited for it and we will be right back with Elizabeth Rowe.

[THEME MUSIC UP FULL, THEN UNDER AND OUT]

Risa Goluboff: Thanks for being here, Elizabeth.

Elizabeth Rowe: It's my pleasure to be here. This is very exciting and I'm honored to be a guest of the show.

Danielle Citron: We're honored.

[LAUGHING]

Danielle Citron: How did you become interested in exploring facial recognition technology?

Elizabeth Rowe: A lot of my work in intellectual property, I feel almost inevitably focuses on the work from the perspective of IP owners. But I also have themes of looking at things from the consumer perspective as well, or from the end user's perspective. And so, naturally, this also felt like it would meet that need. And overall, because a lot of what I look at in my work on trade secrecy involves information and data, I often like to look at areas of data or kinds of data that really sort of push the
boundaries, where there's no regulation or where the law is unclear. And to me, not only is this about data or about information, but it's biometric data. And something about that seemed really special to me and unique and I thought it might be just the kind of thing I should look at, especially since there was no federal regulation.

**Risa Goluboff:** I'm so excited for this conversation and, as I said, a little scared of it.

**Elizabeth Rowe:** Right.

[LAUGHING]

**Risa Goluboff:** In your paper you talk about so many different ways facial recognition is being used in the United States, and the uses are both on the private side by private corporations and things that we might be doing that lead to those uses as well as things that are, you know, on the government side.

**Elizabeth Rowe:** Mm-hmm.

**Risa Goluboff:** Let's start with the corporate side. So what are some common ways this technology is already being incorporated into our lives, given our interactions with private corporations?

**Elizabeth Rowe:** Well, to start, probably one way everybody today has already used it is when they picked up their iPhone. If you have an iPhone and you're using your face or your fingerprint to unlock the phone and to get in, it's already right there in your hand.

**Risa Goluboff:** That was my first thought. Absolutely.

**Elizabeth Rowe:** The technology is also being used in homes. So a lot of new luxury apartment buildings and condos are adding in facial recognition so that residents, when they walk in are immediately recognized, they're given access to various areas, you don't need to carry around your keys. And it doesn't even need to be, you know, a brand-new luxury condo. I mean, almost anyone can retrofit their homes already to use this kind of technology.

**Danielle Citron:** And not just homes, but stores and other public places.
Elizabeth Rowe: Yeah. Shopping centers and malls are using facial recognition technology, for instance, to, you know, see what we're looking at, and what stores we're going to. And apart from the shopping, a large number of uses are also by employers. So employers are using this technology internally for all kinds of business purposes, timekeeping for employees and that sort of thing.

Risa Goluboff: So it's already everywhere is what you're saying.

Elizabeth Rowe: Already everywhere. Yes. But it's not completely everywhere. It's not as everywhere as in China.

[LAUGHING]

Risa Goluboff: All right, we'll get to that.

Elizabeth Rowe: But everywhere. Yes.

[LAUGHING]

Risa Goluboff: But everywhere. Okay.

Danielle Citron: So, so we've got this kind of surveillance creep from one device to another to different spaces and spheres, right, in the corporate sector. But I'd like you to explore and, and talk to us a bit about that invisible handshake between the private sector and the public sector, right, and increasing ways in which government is getting its hands on these technologies and using them.

Elizabeth Rowe: The government uses these kinds of technologies in all kinds of settings. So, for instance, if you go to an airport, especially an international airport, and you're at the gate, you're leaving the country, or you're coming back into the country through customs, et cetera, right, facial recognition technologies are being used to check who's coming in, who's getting on the plane, et cetera.

Danielle Citron: Not to mention law enforcement.

Elizabeth Rowe: Yeah. Making arrests, getting evidence, surveillance during protests. Just as in the private sector, the government uses are quite extensive — even in public housing facilities, for instance, we're seeing use of this technology.
Risa Goluboff: You talk in the paper – and Danielle mentions this invisible handshake, right – so how does the government get this information and what is the relationship between the private corporations and the government?

Elizabeth Rowe: There are several ways that it gets to the government, depending on what setting and what uses we're talking about, which agency. So for instance, there are instances when the government will actually purchase technologies from a developer who has, you know, created the technology. So, Clearview, for instance, is a well-known company that supplies to many different government agencies.

Danielle Citron: They're the heavyweights in this arena right now, aren't they?

Elizabeth Rowe: Yes, Clearview technology has been used worldwide, and they supply not only law enforcement, but also private companies. There's been a bit of controversy and litigation about how Clearview obtained some of the information that it has obtained in order to build its massive database. So, for instance, they were said to be scraping information from all kinds of social media sites, like Facebook, and images from other sites.

Danielle Citron: Sure.

Elizabeth Rowe: So one appeal of using a company like Clearview's program is that it's an infinitely larger database of photographs to compare. So for instance, if the government would normally rely on mugshots for pictures, that requires that people have already been arrested. But now with Clearview, they have basically everybody, practically anybody who's ever posted a picture on Facebook, or anywhere else of their children, of themselves, of, you know, all kinds of settings. And the technology is also advanced in the sense that it doesn't necessarily require a face-on, full view of the individual. So it's very powerful. And there has certainly been praise by law enforcement because, you know, from law enforcement's perspective, they say, “Wow, this is fantastic, right? It allows us wonderful access to this database of information that we normally would not have had access to.”

Risa Goluboff: It seems clear to me, but maybe not to everyone, that there's room here for regulation. And maybe one would say a really big need here for regulation. But one of the things that you do so well in your
paper is point out that consumers appreciate a lot of these technologies, right? And they make life easier even at the same time as they might make privacy harder to come by, right? And so, on the one hand, consumers appreciate these technologies, so maybe that clouds the regulation picture a little. And on the other hand, a lot of businesses are asking for regulation in the space. So you might think, “Oh, consumers want regulation and businesses don't want regulation,” but that's not what you see. So can you talk about both sides of that a little bit?

**Elizabeth Rowe:** Yes. One of the interesting things about this area and the way that I particularly do my analysis in this paper is by identifying the fact that here, there are various stakeholders, there are the consumers, there are the producers, for instance, and they all actually have common interests. When we think about regulating in this space, I think that's an important observation, because it's a good place to start. And just as consumers would want regulation – or at least they say they want regulation – companies want regulation too. You know, Amazon, which is a producer of a program called Recognition, which is also widely used, has proposed and encourages regulation in some of its proposals to Congress — has set out certain guidelines that it suggests might be used. So there are a lot of other companies as well, that say, “Yes, we want regulation.” And there are various reasons for that, but one, I think, important reason just from a business perspective comes down to efficiency. It's difficult when you are doing nationwide business, right, as every business does today, to not know what you can or cannot do or what you can or can't develop.

**Risa Goluboff:** When there's a patchwork of laws across different states.

**Elizabeth Rowe:** Across different states, exactly, when, when there's a patchwork and just piecemeal legislation here and there. So from their perspective, they say, ‘We want to know. What is it that you need us to do? What is it that we can do? What is it that we can't do?’ And that's the million-dollar question.

**Danielle Citron:** Businesses aren't really demanding that there be uniform rules, right? They say they are, but they're not banging down Congress' door to pass comprehensive privacy legislation. But in this particular space, we're talking about the body, right? We're talking about identity and the appropriation of your identity in ways that I think are both
terrifying and, of course, for companies and governments exciting cause of the power it gives them.

Elizabeth Rowe: Mm-hmm.

Danielle Citron: Companies recognize that people have a more visceral response to the sort of appropriations of their bodies and truly the image of the face as the soul, right? What have states done and has that been effective? Tell us a little bit about the Illinois Biometric Protection Act and, you know, some of the lawsuits perhaps that we've seen emerge in the wake of that law. And is that, by your lights, the way to do it?

Elizabeth Rowe: Well, Illinois, as you know, Danielle was the first state to enact what's called BIPA. It's B-I-P-A, it's Biometric Information Privacy Act. And most of the litigation that we've seen so far comes out of Illinois as a result.

Danielle Citron: It's a potent law.

Elizabeth Rowe: Yes.

Danielle Citron: Why is it that terrifies companies the most of all the privacy laws?

Elizabeth Rowe: So it's among the most comprehensive so far. One of the things that's relatively unique about the Illinois statute, and the reason that we have a lot of litigation from Illinois, for instance, is it has to do with the remedies, right? Illinois has a civil cause of action.

Danielle Citron: Yeah.

Elizabeth Rowe: So we're going to see lawsuits.

Danielle Citron: Yeah.

Risa Goluboff: Lawsuits by consumers against companies.

Elizabeth Rowe: Lawsuits by consumers. Exactly.

Danielle Citron: Yup. Class actions.
Elizabeth Rowe: Class actions. Lots of class actions.

[LAUGHING]

Elizabeth Rowe: Yes. In general, I don't think class actions are the best way to settle these more global issues that we're having. Other states that have regulated in this space only allow, for instance, for an attorney general action. Right? So consumers can't bring an action. Others mention biometric information, but they don't go so far. They may say, for instance, as part of the data security disclosures, “Oh, and by the way, if there's a breach of biometric information, you need to disclose those as well.” So what we're seeing among the states is that even though there have been attempts – and there certainly are laudable attempts to recognize that there is this very special data, this biometric information that we ought to do something about and protect, there really is so much variation. And the protection in many ways is – if you're looking at it from a consumer's perspective – the protection is thin.

Danielle Citron: If you get written consent, like in Illinois, then you can use it.

Elizabeth Rowe: Yeah.

Danielle Citron: The devil's in the downstream uses, right?

Elizabeth Rowe: Yes.

Danielle Citron: And that I think brings us to China, which is definitely the Wild West, right, of facial recognition, pervasive uses. Can you describe how extensive it is being used? You know, the, the notion that it's not effective – well, golly, maybe there is a part of the story where you have societies training their data sets in such extensive ways that there's higher accuracy. Tell us how it's being used and why we should be pretty scared. I don't mean to cede the ground, but I've read your paper, so I feel like I can say that!

Elizabeth Rowe: Right.

[LAUGHING]

Elizabeth Rowe: So if you think about how as consumers we go through kind of our day-to-day lives interacting with businesses, in
almost every single one of those instances, China is already using facial recognition technology. If you're applying for a job, if you're applying for health insurance. They can even allegedly detect, for instance, do you look like a smoker? Do you look like you're being honest when you're answering questions in, in various kinds of interviews? Of course, on the street, sort of from a surveillance perspective, right? The technology has evolved that not only are individuals able to be detected as they walk down the street, but groups of people, right? So groups in a stadium or groups anywhere can be detected and can be matched.

**Risa Goluboff:** And the technology is being used for financial purposes as well, right?

**Elizabeth Rowe:** Right.

**Risa Goluboff:** Tell us about that.

**Elizabeth Rowe:** So for instance, in China with banking, if you apply for a loan, they can use the technology and decide, do you look like you are trustworthy. You know, here we're so advanced because now we don't need to carry a credit card and we can use our cell phones to make payments right at the grocery store and everywhere else. Well, guess what? In China, you don't need your cell phone either. You just show up with your face, and that's all you need to make payments.

**Risa Goluboff:** Paying with your face.

**Elizabeth Rowe:** Yes, paying with your face.

**Danielle Citron:** Tell us about the downsides too, though, right? Because that seems pretty nifty.

**Risa Goluboff:** But also scary, also scary! Yeah.

**Danielle Citron:** No, of course. The power piece, put that aside, right? But let's assume that there's accuracy, that they're getting it right. How are they using it to prevent people from doing things? I think that's the most devastating part.

**Elizabeth Rowe:** Well, you can be denied jobs. You can be denied health insurance. You can be denied loans. You can be denied entry into various places.
Danielle Citron: Yes. Mm-hmm.

Elizabeth Rowe: During the pandemic it was very useful because, you know, you can tell who's out. Are they wearing a mask?

Danielle Citron: Yup.

Elizabeth Rowe: And the technology has evolved so much too that they were able to detect faces even with a mask on.

Risa Goluboff: Wow.

Elizabeth Rowe: To us, it's kind of like science fiction, but it's not. That's where we are headed. Because without a regulation, the technology has been limitless and boundless, right, in terms of its various applications. And a lot of these technologies and applications developed in China are being exported.

Danielle Citron: Yeah.

Elizabeth Rowe: It's business like everything else, and it's being sold. Somebody needs to be looking out for how it's spreading and how we're using it. And I think that, that somebody is the federal government. Hence the reason for raising the awareness in the paper.

Risa Goluboff: That all makes sense to me. As a historian, I'm not a technological determinist. I'm not an economic determinist. So, where I see hope, I think is where you see hope, which is even if the technology is similar or the same, literally being exported from China to the U.S., the rest of our governmental framework is not the same. So, we are a democracy, and so one important difference and tool that we have, obviously as you've been saying and as you show in your paper, is governance, right, is using our democracy to create regulations so that the future looks different in the United States. So, how much different do you think the future is going to look, once we get to the place where you think we should be – or where you think it's realistic to think we might be.

Elizabeth Rowe: That's hard to tell, Risa. I don't know. I guess it depends ultimately on whether, you know, how much of a pessimist one is. But again, thinking about it in terms of what has happened historically in other areas, privacy generally, I suspect it might be one of these things where we say, “Okay, let's just put people on notice, right?” Let's
just have some kind of notice regime. You put up a sign, you click to consent, or you buy the ticket to consent, right? Because for instance, if you go to an amusement park, right, and you purchase the ticket, right?

**Risa Goluboff:** Yup.

**Elizabeth Rowe:** Right?

**Danielle Citron:** Yeah.

**Risa Goluboff:** And of course, arbitration and no rights to litigation.

**Elizabeth Rowe:** Yes. But then, there will come a time we start to see really bad cases, right? The kinds of cases that might end up in the tort system, the kinds of cases that might call for constitutional challenges. Then we'll have litigation, which might address a sliver at that time down the road. But I think that kind of history of the way we do things is unsatisfactory because it's all sort of after the fact, right? We let it be market-driven, and then harms occur. We deal with these harms on a case-by-case basis or through the class-action system, somebody gets paid and we keep going. I think that's not ideal. I don't have a magic bullet as to how to fix it all.

[LAUGHING]

**Danielle Citron:** But you kind of do, right? Tell us how you're going to get us out of this cycle of nonsense, procedural hogwash, right? Notice and presumed consent or written consent. Right?

**Elizabeth Rowe:** Right.

**Danielle Citron:** These kind of, like, procedural thin commitments, because we usually just sign away a lot of our rights without realizing it.

**Elizabeth Rowe:** Yes. So, I identify the concerns here into four main categories. How do we store this information? How do we use them? How do we collect it? And how do we share it? Each of these areas has concerns both for businesses and for consumers. And one of the areas of common interest on both sides is the security, right? Consumers want the security.

**Danielle Citron:** Yeah.
Elizabeth Rowe: We're concerned about misuse of this information, for instance. Companies also want security. Because all of this data, this is their intellectual property, right, these algorithms, these databases, and they want protection. So even assuming, in the most pessimistic way possible, their main interest – or their only interest – is about protecting themselves, they want security. So a trade secret framework is built for just that.

Risa Goluboff: How so?

Elizabeth Rowe: Well, for one thing, we have all this confidential information; we need to know how to protect it. And so having the appropriate security in place from the perspective of the producers and the holders of this information, as companies store and collect and gather all of this information or use all of this information, I think is important. Trade secrecy offers what we call the reasonable effort standard because then we need a standard of care, because companies will say, and some have said to me, “Okay, we, we're collecting, here we are finding ourselves collecting all of this information. Now what do we do with it, right? From a legal perspective, what do we do with all of this?” We need a standard of care, and I think the reasonable efforts, um, standard in trade secrecy is one way to think about what steps have you taken – what reasonable steps have you taken – to protect the information from disclosure and to keep it secure.

Danielle Citron: Mm-hmm.

Elizabeth Rowe: I also think that from a litigation perspective, that, in trade secrecy, we have trade secret misappropriation, a misappropriation standard, right? So in terms of liability, how do we decide when one who has taken this information or caused it to be shared, is liable? And I think we might look to trade secrecy to see how we handle a misappropriation in various contexts as well. So I think that overall, the fact that trade secrecy is built to protect confidential business information, is a very useful place to start when we start thinking about how to protect a lot of this information, which is business information, but it's also more than business information, because it's also private information.

Danielle Citron: But it's my face. How come it's not my trade secret?

[LAUGHING]
Danielle Citron: And we should tell Risa that we are planning on writing a privacy-intimate data-trade secrets article together.

Risa Goluboff: Fabulous. Oh, how exciting!

Danielle Citron: Yes! So we’re going to have some synergies here!

Elizabeth Rowe: Yes, yes.

Risa Goluboff: That's great.

Elizabeth Rowe: Because I do think your face should be your trade secret.

Danielle Citron: Right.

Elizabeth Rowe: And I do think your fingerprint should be your trade secret.

Danielle Citron: Right.

Elizabeth Rowe: And by calling it that we give it, you know...

Danielle Citron: That's a lot of power.

Elizabeth Rowe: Lot of power.

Risa Goluboff: Mm-hmm.

Elizabeth Rowe: Gives us control, it gives us ownership.

Danielle Citron: Yeah.

Elizabeth Rowe: Right? Those two things, the ownership and control over it, is what ultimately I think will make a difference …

Danielle Citron: Yeah.

Elizabeth Rowe:… for a lot of these technologies and for a lot of our privacy concerns.
Risa Goluboff: Well, Elizabeth, this has been an absolutely fascinating conversation. I have to say, I'm so glad that you are thinking hard about this, and that alone makes me feel better about all of the things that you've identified. So thank you so much for being here.

Elizabeth Rowe: Thank you, Risa and Danielle. It has been such a pleasure talking to you about this today.

Danielle Citron: Thanks, Elizabeth

Risa Goluboff: I think the place we have to start, Danielle, is in your future project together. So tell me more about that.

Danielle Citron: We have like tentatively titled it, "Intimate Secrets."

Risa Goluboff: A good combination of your key interests and her key interests. That's perfect.

Danielle Citron: Yes, and I think the agency-securing and dignity-entitling, and all the way that we think about why intimate privacy matters and giving that kind of important ownership interest in one's own intimate secrets, right? And we might be quite narrow, whether it's the intimate image, the body, ways in which we concede ground to individuals rather than companies. You know, the narrative has always been about, it's the company's trade secret. And Elizabeth knows, I want to say, “Hold on a second, let's foreground the individual.” It's their faces, their irises, their fingerprints, their bodies in nude imagery, their health information, their innermost fantasies, should be understood as their own and not necessarily as a property right, cause that always worries me that we're just going to sell it and give it away. But one that would entitle us to far more significant protection. So we're, we're puzzling through, we haven't written anything yet. But we figured if you center the individual in the question of one's intimate secrets, then you give them a whole lot more power than they currently have. You can't assume away that they've consented and agreed, and in some respects, it's more profound protection for the individual. So we're getting companies out of the picture and thinking about how individuals might have some trade secret interest in their own bodies.
Risa Goluboff: Well, it's very interesting and it's very important and it makes me very happy because it highlights exactly the kind of synergies that we hope the LawTech Center will create among our faculty.

Danielle Citron: Absolutely.

Risa Goluboff: That's just wonderful. One of the things that's exciting about that project is using Elizabeth's expertise of trade secrets and thinking about this in this different context and taking your context of intimate privacy and thinking about it in the context of trade secrets. But we have intimate torts, right?

Danielle Citron: That's right.

Risa Goluboff: We already have a way of dealing with this. To what extent can those torts be used, both in what Elizabeth is talking about …

Danielle Citron: Yup.

Risa Goluboff: … as a first instance, right? Do those torts have any role to play in the regulation that she's thinking about? And then, how will it figure in, if at all, to your joint project?

Danielle Citron: So one of the four privacy torts is appropriation of someone's image or personality.

Risa Goluboff: Why is that not the end of the story? We've already got a tort.

Danielle Citron: I wish it was the case, because it's been really narrowed to only cover commercial uses. And you might say, “Well, isn't facial recognition software and the use of people's intimate images, their, their identities, for someone else's commercial purpose, isn't that precisely the kind of …”

Risa Goluboff: Yeah! If Clearview is selling these images ..

Danielle Citron: Right.

Risa Goluboff: … to the government, that's a commercial use, is it not?
Danielle Citron: Courts have been really narrow about how they understand commercial uses as to really only relate to advertising. So if you use my face in an insurance advertisement and suggest that I’m endorsing Northwest Mutual Insurance and you make money off of that project and you don't pay me – sort of like I have an interest of publicity and I've got to be worth it, my face has to actually generate money. And courts just have refused to find that the tort is capacious enough to apply to the kind of uses of one's image that isn't immediately money. Right? It is money, of course. You might say this is a perfect application of the tort.

Risa Goluboff: Yes!

Danielle Citron: As I have argued, let's get away from this commercial story. The right to privacy as it was originally conceived by Warren and Brandeis, I argue, it was about the inviolate personality and all the ways that's dignity-conferring and autonomy-enabling. That is, your image is who you are so that you can be a subject rather than an object. You decide, right?

[THEME MUSIC CREEPS IN]

Risa Goluboff: Well, I learned so much from Elizabeth, and I'm glad she's thinking deeply about this, I'm glad you're thinking deeply about this. Knowing the two of you are on the case is definitely cause for optimism.

Danielle Citron: We're excited. So thank you for bringing us all together.

[THEME MUSIC UP FULL, THEN UNDER]

Danielle Citron: That wraps up this episode and this season of Common Law. If you want to find out more about the work of Elizabeth Rowe, visit our website, Common Law Podcast.com.

Risa Goluboff: Danielle, I cannot believe the season is already over, but I want to thank you so much for being one of my partners in making it happen again. It has been so much fun. I also want to thank my UVA Law colleagues and other co-hosts, John Harrison, Cathy Hwang and Greg Mitchell, who joined us earlier this season and who were just terrific. And a big thanks as always, to our audience for listening. I'm Risa Goluboff.