UVA LAW | Citron Foundation talk

RISA GOLUBOFF: Good afternoon, everyone. I am Risa Goluboff, The Dean of the University of Virginia Law School. I want to thank Ellen Walker and everyone at the Law School Foundation who has organized this event. There have been very few silver linings of the pandemic that we are still unfortunately in.

But one small silver lining has been that we are no longer as constrained by geography. And it's allowed us to think more expansively about how, and where, and when we engage with you, our wonderful alumni. And that thinking has in turn led to today's event.

I am so delighted that you have made the time to join us this afternoon to hear Professor Danielle Citron talk about the fight for privacy. It is my absolute pleasure to introduce Danielle Citron, who is the inaugural Jefferson Scholars Foundation Schenck Distinguished Professor of Law here at UVA Law School.

She writes and teaches about privacy, free expression, and civil rights, particularly about the nexus of those three areas. Danielle is the author of more than 50 articles, essays, and book chapters. Her 2014 book *Hate Crimes in Cyberspace,* published by Harvard University Press was called a breakthrough book that would change the law, change the conversation, and change attitudes. And it did, and it has.

Danielle's scholarship and her advocacy have been recognized nationally and internationally, including with the MacArthur Fellowship, more commonly known as the "Genius Grant" in 2019, for her work on cyber stalking and intimate privacy rights.

Over the past decade, Danielle has worked with lawmakers, law enforcement, and tech companies to combat abuse online, including testifying before the United States Congress, as well as the British House of Commons. She serves as an advisor to Facebook, Twitter, Bumble, and Spotify on privacy related issues. She is the vice president of the cyber civil rights initiative, a nonprofit devoted to fighting for civil rights and liberties online.

And she is a board member for the Electronic Privacy Information Center, EPIC, and the Future of Privacy. She's also an advisory board member of the Anti-Defamation League Center on Technology and Society as well as the Center on Investigative Journalism.

She regularly speaks and writes on cutting edge technology issues, including online harassment, the use of deepfakes, and how to build a better internet. Danielle is also, I must say, a beloved teacher, and mentor, and an absolutely stellar law school citizen.

And she has already made a huge mark on the law school in her single year thus far on our faculty. May there be many more. Among Danielle's responsibilities at the law school, she serves as the inaugural director of our recently launched Law Tech Center, which does three different things. It explores the law, policy, and ethics of technology and its applications.

It uses technology to research the law, using cutting edge big data and text analysis. And it trains our students for technology that they will encounter as practitioners. You can read all about both Danielle and the new Law Tech Center in the current issue of the *UVA Lawyer.*

Today, Danielle will talk with us about the fight for privacy, drawn from her forthcoming book,*The Fight for Privacy-- Protecting dignity, identity, and love in the digital age,* which will be coming out from Norton in 2022. I could not be more excited to introduce Professor Danielle Citron.

DANIELLE CITRON: Thank you so much, Dean Goluboff. It's such a treat to be on your faculty. And a gift of the pandemic for me, was getting to join you all at the University of Virginia Law School. So I'm thrilled to talk about my book project with all of you. So it's coming out this summer. And let me start by defining what I mean by the concept of intimate privacy.

So intimate privacy covers the boundaries that we manage or have around-- that we set and fortify around our intimate lives. So it's information about, and access to, our bodies, our minds, our thoughts, our innermost thoughts, our communications, our searches, our health, sex, gender, and sexual orientation, and our closest relationships.

It's both a descriptive but also a normative concept. So it concerns the privacy that we want and expect, and the kind of intimate privacy that we deserve, because it's a precondition to human flourishing and citizenship. And so intimate privacy, as I've conceived it, is instrumental to how we develop ourselves in a way that it's a foundational privacy interest.

It's not that it's the only privacy interest that matters, but it's a crucial privacy interest that we can contrast with financial privacy. So the privacy over our bank account information. Yes, protecting it is important, because we're going to protect ourselves from theft and some dignity concerns with other people knowing our financial status.

But it's limited in our impact over our lives, in a way that intimate privacy has its tentacles. It's rooted in. It's a precondition to our self-development, our human dignity, our close relationships, in a way that a bank ledger never could. So let me just describe why it's so important-- the concerns about self-development, about human dignity, and about intimacy, that intimate privacy is a precondition to.

That without intimate privacy, it's incredibly difficult to develop and figure out who we are, and who we love, and the kind of people we want to be. So intimate privacy provides that invisible space that we all have and want to enjoy with our bodies. Our bodies are our first form of reference to figuring out who we are, both who we are now and who we want to be.

We might think of our clothing as sort of providing a guard for it. It gives us a physical space, but there are also other ways in which we can sort of set ourselves apart from other people. And having that invisible space with our bodies, with our minds allows us to develop our identities and figure out who we are, both in the self that we want to present to other people, and as we develop and think about ourselves.

Now human dignity is intricately connected with the intimate privacy that's afforded our bodies. Think about human dignity. And as I'm using the term, we can think of it has two pieces-- both our ability to have self-esteem and social esteem.

So the ability to figure out and to decide who has access to our most intimate selves-- our bodies, our thoughts, our innermost thoughts-- gives us a sense that we're in charge of our lives, that we have a sense of self-esteem. But it's also true that having the ability to present ourselves as a fully integrated person, as we want to present to other people, allows us to enjoy social esteem.

So Jean-Paul Sartre in talking about why is it that we wear clothing, it allows us-- and this has to do with social esteem-- it allows us to be seen as fully integrated people, as whole selves, rather than as just as objects, or as fragments of ourselves. And so intimate privacy is essential to having that sense of dignity, both in ourselves and then for others.

It's also so crucially important for the ability to develop close relationships. So if you think about it, our closest friends, our family members, and our partners and loved ones, we develop those relationships through a process of mutual self revelation and mutual vulnerability.

And as we peel the onions and the layers back to one another, we depend upon intimate privacy, or the kind of trust and discretion that we're willing to share our innermost selves, and develop those relationships with friends and close loved ones. Only if we think that they'll be discreet, but we trust them to be discreet with those innermost aspects of ourselves.

And so intimate privacy is-- Charles Reed would say, it's the oxygen for love. And that's true, not just of your lovers, but also our closest of friendships. So now unfortunately, and sort of at the basis of my book, is the ways in which individuals, companies, and governments deprive us of intimate privacy.

So I'm going to start with privacy invaders, and just give us an example. So I'm going to call her Joan. But Joan was a recent graduate of law school on her first job, and went traveling and was at a hotel the night before a big deposition she was to give.

And when she got back home from that trip, she received an email from someone calling themselves "notabadguy2." And the email included a link to Pornhub that says, you see this video of you, I'm going to share this video with your friends and loved ones, your colleagues, unless you send me more nude photos and a video of you masturbating.

So instead of responding and sending what notabadguy had requested, she talked to me. Joan decided, obviously, she wasn't going to send him more nude photos. It's something called sextortion. And of course, in response when she refused to send the video, he then sent it, the video of her.

So it was a video of her that was taken in her hotel room, while she was showering. So it was a hidden camera. A camera was hidden in the bathroom of her hotel shower, presumably by a hotel employee. So the video captured her showering and also going to the restroom.

The person then sent the video to all of her contacts on LinkedIn, which included her law school classmates, her colleagues at her firm. And then he posted the video, not only at Pornhub, but at other sites, sites devoted to non-consensual intimate images, video hidden cameras, like hidden cam sites, and sites devoted to deepfake sex videos, which is manufactured videos, where a woman's-- usually typically woman's-- face is morphed into porn without her permission.

And so what Joan faced was at the hands of a hotel employee presumably, was both video voyeurism, which is a way that we invade intimate privacy, sextortion, the demand for additional nude videos on the threat of releasing more of those videos that the person already had. The person then posted that online, which we can refer to as non-consensual intimate images.

And then shared them with her friends and classmates to her great shame, embarrassment, and sort of constant fear that where this video was going to be posted next. And had huge implications both for her sense of physical safety, her emotional stability, and her feeling like she could never really move jobs, because the video was posted on countless sites along with her full name, so her first and last name, her cell phone number, and her email address.

OK, so now the sites that this video is posted on, there are approximately 9,500 sites that are devoted to hidden video, like hidden cameras, non-consensual intimate images often called revenge porn sites, and deepfake videos. And how they operate and run is they're an ad based model.

And they can post people's nude images taken without their consent, whether video or photographs, without any worry about being sued, thanks to a federal law that I'm going to talk a little bit about called the Communications Decency Act. But the logic behind those 9,500 sites, is the same logic of the companies that are busy amassing our intimate information, that I call in my book *Spying Inc,* that is the countless businesses that are collecting information about our bodies, our health, our sex, sexuality, and gender.

So dating apps, one half of all young people in the United States use dating apps. And dating apps collect an extraordinary amount of intimate information about us, including sometimes the nude photos that we share on the apps. But information about the kinds of individuals were interested in, our chats, our sexual activities that are facilitated by the apps.

So dating apps-- femtech, so that's period tracking apps. One third of all women and girls use apps to help them track their periods and their fertility. And now these apps, you might think, OK, well they're just collecting information about people's periods, and they would willingly share that with their doctors.

Why not these health or fertility apps? They're collecting far more than people's periods. They require people who use these apps to tell them who they're sleeping with, when they have sex, have they orgasmed, who they were sleeping with. And it's often when you use these apps, because they're free-- free in theory-- they often require an extraordinary amount of information in order to use the app, so that the app is functional.

And so they ask questions about the medicine you're taking and your health conditions-- so extraordinary amount of information about your bodies, your healths, and your sex lives. Porn sites, so Pornhub, one of the most popular adult sites online, had $42 billion visits last year. So that's across the globe.

Pretty much means everyone that we know probably has visited Pornhub. And they're tracking the videos that you watch, the searches that you run. And they have an extraordinary amount of information. You might think, well, what are they really doing with it? They're selling it to advertisers, and marketers, and data brokers.

There are over 400 companies in the United States who collect and amass over 11,000 data points on each and every one of us, and then sell that information. They categorize, rank, and rate, and score us as sex toy users, as rape victims. They collect all this information about us and then rank and categorize us in ways that we often might even not see ourselves-- HIV sufferers, prostitute interested.

And that information is then sold and monetized. So you might think, OK, well that is extraordinary amount of intimate information about us. Isn't it protected? Don't we have things like health privacy laws and laws that would protect sensitive information?

And the truth of the matter is, spying largely precedes and runs amok with very little regulation. And so we often treat-- I'm just going to take individuals who invade our intimate privacy, governments that are amassing and collecting, sharing, selling, using, categorizing, ranking, rating, and scoring our intimate information.

Even governments get in on the act of buying that information from data brokers, or obtaining it from individuals. It's large. We have a very soft hand of regulation in the United States. So what's interesting is the kinds of the lack of privacy protections that we have in the United States, it means that we externalize it across the globe.

So that the nude photos that you can view in the United States for sites that are hosted in the United States, can post nude photos of people from South Korea, from Australia, the United Kingdom. And there's nothing that their governments can do. They don't have jurisdiction over these sites hosted in the United States.

And the same is true for these dating apps that are based in the United States. So Grindr is popular in Russia. It's popular in Egypt. It's used around the globe. And yes, they may have privacy laws. They often comply with them in the breach, in the sense of like, whoops, you've discovered us. We've screwed up. Norway, we will now do better.

But their practices are molded and shaped by having been created and sort of with a hacker's ethos in the United States. Now for individuals the problem is, we have far too little laws. We often deal with-- think about-- so the privacy invaders I talked about, the individual who, presumably, hotel employee, who invaded Joan's privacy.

We deal with intimate privacy violations on a catch can manner. It's very piecemeal. And so up-skirt photos, sextortion, deepfake sex videos, we don't regulate them. We don't have laws that often, and to the extent that we have laws, they're sort of ill suited to address them.

And laws that we do have on the books-- so for example, and I've been involved in the work and ensuring that we criminalize some intimate, the non-consensual publication of intimate images. They're often misdemeanors. And so what happens is, victims go to law enforcement. Law enforcement says, like, eh, turn your computer off. It's no big deal. It's a misdemeanor.

They have no interest in pursuing it. And they probably don't understand the technology involved. They're just not good at online crimes. And so often, victims will walk out of police precincts feeling worse than when they walked in, unfortunately. And individuals have no deep pocket to sue, thanks to that federal law, the Communications Decency Act passed in 1996.

The idea was to provide an incentive for "good Samaritans" to block and filter offensive content. But the way in which it was drafted, it was drafted in such a way that it's been so broadly understood. So that even sites whose business model is abuse, their business model is the invasion of intimate privacy, they enjoy immunity from liability.

And so they can say to victims, sue me, go for it. They have no worries about being held responsible, because they enjoy immunity from responsibility under Section 230(c)(1). And their business model is predicated on the idea of making money from advertising.

And in the United States, we understand the massive collection and sale use of intimate information as a consumer protection matter. And so in the United States, we basically have a very sort of weak sauce of notice and consent, as the way in which we approach privacy protections, which is to give some notice about your privacy practices.

Then we're going to presume that individuals have consented to the collection, use, and sharing of that information, even if no one has meaningfully consented. Really, the idea that your dating app is sharing the gay subculture community that you've identified in the app that you belong to.

The idea that we're sharing that with marketers and advertisers came to the great dismay of people using Grindr, when the Wall Street Journal did an expose of the sharing of that information. So notice and choice doesn't do much for individuals. We have some sort of movement around State AGs and the Federal Trade Commission, but it's certainly not robust protection.

And so we are largely in a deregulatory landscape. And I often view America-- where I call us, we're the scofflaws. We externalize a whole lot of harm, because we're building these technologies on the notion that, we'll just build it, and figure out harms, and deal with harms later. And we've got this Section 230 immunity, which means that sites can create a lot of mischief.

Their entire business model can be illegality, and they don't have to pay for it. They don't have to internalize those harms. And so we need a new way to think about intimate privacy. We need to revise, rather than a consumer protection matter, rather than a question of, there's a legal shield, so that we want the internet to be boundless in its development.

And we're going to trust companies to be good Samaritans, to block and filter offensive content, which they're not doing, and especially not those 9,500 sites that are in the business of it. And instead of looking at privacy invasions as it's a personal conflict, we don't get involved.

At the heart of my book is an argument for viewing intimate privacy as a civil right. And I use that term, both as a term that refers to substantive obligations that each and every one of us should enjoy, sort of drawing on the work of Robin West and our own Dean Risa Goluboff. And how she wrote about how in the 1940s, the civil rights attorneys at the Department of Justice fought hard for recognition of a right to labor.

It was understood as a right everyone should enjoy. And we were going to protect the possibility of free labor. And that civil rights should be understood as having two components. One component is that it's a right everyone enjoys. But the other component is that we need to protect intimate privacy understood as a civil right from its denial on the basis of someone's membership in a protected class.

So an anti-discrimination mandate, both as a right everyone should enjoy, and a special protection against discrimination. Because all the processes that I've talked about before, who is more often targeted for intimate privacy violations are women, non-whites, sexual and gender minorities, and the disabled. And that's true across the globe.

So 98% of the photos on those 9,500 sites that are devoted to hidden cams and non-consensual intimate images, they're women. So deep fake sex video sites, sites devoted to inserting people's faces into porn-- you're not seeing men's faces being inserted into porn. 96% of those videos are women's faces being inserted into porn.

And combine that with pernicious stereotypes. So that the bodies of LGBTQ individuals, of women, of people of color, are viewed as-- due to those troubling, controlling stereotypes and images-- disgusting. And it's costly. If your nude photo is in a Google search of your name and you're a woman, it's going to be more costly to you than a white male.

Because we're going to view that woman as, she's a slut. What was she doing sharing her nude photo? And I can't tell you how many times women, just anecdotally, have shared with me and victims of intimate privacy invasions, have been denied job opportunities or fired on the basis of their intimate images being posted online.

And those controlling images are also true in employment practices. When intimate information is shared from a data broker to a life insurance company, we're going to see the cost lie pretty heavily on women and marginalized people. And so a civil right is understood has important expressive value. It would change the social meaning of intimate privacy.

So instead of a consumer protection problem, instead of it's a personal issue that people can address, instead of something that the internet-- it's important that information be free, and that we should have no liability online. It would reverse the stakes. And it would say, when we call something a civil right, we say that it's so important that you need a darn-- you need a really good reason to deny people of their right to intimate privacy.

We would flip the script from one where we can presume the collection, use, and sharing of intimate information, to requiring a good reason to do it. And it would say to victims, that you should see yourselves as being harmed. And that you should be able to bring civil suits, and go to law enforcement, and to be taken seriously. That you have been grievously harmed, and wronged, and the legal system sees you.

There's also practical payoff. So the expressive value as seeing something that intimate privacy that we all should enjoy. We should all be guaranteed. And that it ought to be respected, also as practical payoff. Because when we call something a civil right, think about civil rights era laws with regard to education, the workplace, reasonable accommodations for the disabled individuals.

We view the institutions in charge of those rights, whether it's universities for educations, whether it's the work that employers for workplaces, whether it's the owners of transportation to reasonably accommodate the disabled. We treat them as the guardians of those important opportunities to work, to go to school, to ride the bus.

And as guardians, they have special responsibilities. They are the caretakers and have to protect those rights. That was true in physical space. But to the extent that companies are collecting, using, and sharing, displaying intimate information, they too should be understood as data guardians.

And so when we make that shift from a consumer protection matter to a civil rights model that companies amassing, and collecting, and displaying our intimate images, intimate information, they should have the obligation to act as the guardians of that intimate information.

And those obligations include not collecting and not selling certain information at all where there's not a really good reason for them to be collecting, and holding, and sharing that information. Something that wonderful UVA Law alum Neil Richards has developed in his book. And he has a new book called *Why Privacy Matters.*

And in his scholarship, the notion that companies have duties of loyalty and of care. And we should imbue a civil rights approach. It would imbue those substantive duties of robust protection of loyalty and care for individuals, and to ensure that they act as the data guardians of our information.

So law can do some important work. As a law professor and as lawyers, we know law has to play an important role. And it's also our teacher. So law, not only has practical value, but it has expressive value. But it can only do so much. And so I've also been working with companies on using moral suasion of engaging in and using technology to address some of these issues.

And so some of the book, I talk about both developments we have seen, both as a measure of hope, but pushing companies to do better, to thinking about ways that they can protect our intimate information and protect our intimate privacy far more than they are.

And we've got to educate us. In some ways, we have this captive audience in children at schools. But we don't talk to them about intimate privacy. We don't talk to them about the taking and the sharing of nude photos. We usually never talk to them about digital citizenship and what it means to engage with others online.

To the extent that we do it at all in public and private schools, we talk a bit about disinformation. But we hardly ever talk about the responsibility that students have for each other, to protect one another. And so that has to be an important part of it. Now, grown-ups are difficult to reach. You might think, well, how are we going to train grown-ups in thinking about intimate privacy.

And one thing, Facebook unfortunately-- there was a proposal to Facebook that they train their users to handle information responsibly. And unfortunately, and this is frankly no surprise, but the response was, we can't impact how our users behave. It's not worth the time and money. And essentially, the bottom line was, we want to collect their data, use it, and share it, and monetize it.

And we'll deal with harm later. We'll apologize later. And we're not going to engage in that kind of education. And we should. Companies should lead the way in thinking about and educating individuals. So I paint somewhat of a bleak picture in my book about the ways in which law has-- we have under-regulated intimate privacy and under protected it in the United States.

And how companies have done some, but not enough. And as educators and as parents, we need to do more. But I also end with a story of hope. In my work, I've worked closely with developments in the United States around the criminalization of non-consensual intimate imagery, which when we worked on those laws, was a smart approach.

But we need to have a far more comprehensive tact for intimate privacy. But it's worth kind of noting that we've seen developments in the UK. I've worked closely with the governments of South Korea, the Digital Crime Sex Information Minister. We've seen developments.

The problem with the United States is the same problem of Singapore, is the same problem of South Korea, is the same problem of the United Kingdom, is the same problem in Australia. So the literal term for subway in Japan, the sort of slang term for it, is dick pics.

So it's such a prevalent problem, the sharing of intimate images as you're forced as you stand and look at your iPhone, using AirDrop is to force into, it's called cyber flashing, to force people to look at nude photos. It's a prevalent problem, whether it's the UK on the subway system, or in the New York City subway system.

So the kinds of problems that I've described, we are not exceptional in many respects in the United States. We are first rate offenders in the US. We have the same problems across the globe. But what I can say, is that we have seen really important developments in South Korea, which in part, came from a sort of ground up approach calling for change.

In 2018, the problem with hidden cameras in public bathrooms in South Korea was extraordinarily widespread. It was trivialized often by law enforcement, calling it "molka," which is the name of a TV show, like a hidden camera TV show. Ha ha, not funny. But women took to the streets.

And over a course of five protests in 2018 in Seoul, there were 500,000 women and their allies who took to the streets to protest what they're called molka or hidden cameras in public bathrooms. And we've seen extraordinary change in the last four years.

And in talking to the South Korean Digital Sex Crime Information Minister, they first began, as we did in the United States, at the Cyber Civil Rights Initiative to change the way they talked about the non-consensual taking of nude images in public bathrooms, calling it digital sex crime information versus the sort of joking molka.

And then they took on more comprehensive reform, criminal reform and platform regulation. And then, also providing resources to victims. And so we've seen a real change in South Korea in the last five years. We've also seen some change in the United Kingdom. Thanks to the work of victim/advocates who took on the campaign to change the laws around up-skirting in the United Kingdom.

And I've been advising the UK. They have a UK Reform Commission around the abuse of intimate images. And they're considering much more comprehensive reform. And I've been on the ground in the United States, working with states across the country and the state legislatures in criminalizing non-essential intimate imagery.

And I served alongside, now our VP, but when she was AG, Kamala Harris served on her Cyber Exploitation Task Force, where we, not only worked to change the law in California around jurisdiction, but also educate law enforcement. That was a key part of our task.

And in 2015, after our task force had began, there were 50 companies that joined us on the task force. And as a result of that work or grew out of that work, Google and Bing announced that they would de-index non-consensual intimate images in searches of people's names, which was a huge victory.

And so we have-- it's not as you might think, it's all doom and gloom. But we have seen some change in the US and other countries. And so I'm not bullish that we can't do it. I don't think we're going to do it on our own without a change in law.

We need law to help us get there, to change how we view and understand intimate privacy as a civil right, as something that we all deserve, each and every one of us, but that especially has to be protected against discrimination for women, sexual, gender, and minorities, non-whites, and disabled individuals, who more often are victimized by invasions of intimate privacy.

But I'm convinced that we're on the cusp of some change. And so perhaps during Q&A, we can talk about some of the changes that I have proposed to Section 230 of the Decency Act, that is, that we should understand them in the tradition of civil rights. The role of civil rights as the guardians of people's intimate privacy. That they be required in order to enjoy the legal shield.

That they be required to act, to behave in ways that are reasonable to address illegality that causes serious harm on their sites. And so I'd love to take questions and talk about ways in which both the nitty gritty of a civil rights agenda, but then also ways in which we can see change by tech companies and what we all can do to help.

So I'm excited to answer some of your questions. I hope you have some, and excited to talk more about intimate privacy.

ELLEN WALKER: Yes, we do have some questions. The first question is from Gabe Walters. He says, how would you reform the Communications Decency Act, Section 230 to impose liability on publishing platforms for the harms caused by their third party users? Why would that be desirable?

DANIELLE CITRON: Perfect. OK, so I don't think we should get rid of Section 230. And thank you for talking about my favorite but also my deep dissatisfaction with Section 230. Thank you for nudging me to be more specific about how we might amend it.

And so the proposal-- so I've written and drafted with Ben Wittes, the editor in chief of *Lawfare,* a statutory fix to Section 230, which right now reads that no provider or user of an interactive service provider will be treated as the speaker or publisher of somebody else's content.

And what I would add is to say that, no user or provider of an interactive service that has engaged in reasonable content moderation practices in the face of clear illegality causing harm, shall be treated as a publisher or speaker. So what I would do is condition the legal shield. Keep the legal shield.

But condition it on reasonable practices in the face of clear illegality-- so what's illegal-- speech and conduct that's illegal on the books in the face of serious harm. So my hope is that, that standard would nudge online platforms to actually act as the good Samaritans.

That when the folks in 1996 passed the Decency Act. Then Congressman Ron Wyden and Chris Cox, they wanted to encourage sites and internet service providers to act as good Samaritans, because they knew that the federal government certainly couldn't keep up with all of the illegality online themselves.

So they created a carve out, a legal shield for what they call the good Samaritans, for blocking and filtering. And so I want to bring us back to that original purpose. And how we would figure out if someone is a good Samaritan, is if they engaged in reasonable content moderation practices in the face of clear illegality.

And so that would encourage platforms to have coherent, and clear, and accountable speech rules and policies around illegality. And that they, instead of sitting on their laurels and just waiting for content to be reported as abusive, they would have to also act proactively. That a reasonableness standard is flexible enough that they would do that, and so that's how.

And we've been working with folks on both the House and the Senate side to take seriously this possibility. So far we've really only had some carve outs to Section 230, which both are too narrow and aren't going to incentivize the good Samaritan. So I'm going to keep working on it. So thank you.

ELLEN WALKER: The next question is from Gavin Corn. Most of these changes you are recommending would have no impact on the worst of the worst actors who use technology like Tor hidden services. How would you address that? Do you see the Tor Project as being within the scope of these regulations?

DANIELLE CITRON: OK, so one part of my proposal, with regard to content platforms, is to ensure that right now-- and this will borrow from civil rights law-- but right now, because content platforms are immune from responsibility, they don't have to respond to lawsuits to take down material. And so part of my proposal is to require that we recognize injunctive relief, vis-á-vis platforms to take down intimate information.

So even if, as you suggest, somebody is using Tor, the worst of the worst actors. There are a lot of dumb defendants in my experience. But you're right, some are smart. They're veiling themselves and their identities. It would be very difficult, if not impossible, to sue them or to have law enforcement to pursue them.

But what victims so often want, is to have intimate images removed, or to not appear in searches of their names. And so to the extent that we would recognize, what I call, privacy injunctions, then platforms would have to take down that content or block it in ways that it wouldn't prevent the harm. It would mitigate harm and stop it from endlessly continuing.

So yes, you're right. There are people who do a great job covering their tracks. And that's true of every defendant. No matter the crime, there are some defendants that make it very difficult to find them. And you never find them. And with online tools, we can mask ourselves. But as it turns out, we're a lot less masked than we think we are.

If you take away anything from us talk, it's that we have digital fingerprints that we leave everywhere online. And that so much is known about every single thing we do. That really would take someone who's really smart and can use these tools to hide themselves. And even with Tor, sometimes we can figure out who people are. So the criminal and civil law may be available against them. Thank you for the question.

ELLEN WALKER: OK, the next question is from Chad Marlow. Do you see an intimate privacy right being implemented statutorily or constitutionally? How would the effort to implement such rights differ on the federal level from largely stalled consumer privacy rights?

DANIELLE CITRON: So as I'm arguing and imagining, we need both federal and state statutory mandates. We need to-- the first thing is, of course, for Section 230, that would require an act of Congress to change and amend Section 230, which is how we would deal with, at the content layer, the posting of intimate imagery. Right, that's first things first.

We also need, on a parallel track, federal and state legislation that mandates a commitment to intimate privacy and such strong substantive protections, duties of loyalty, care, and limits on the collection of intimate information. You're right, we have stalled in Congress.

So much of the proposed protections, the privacy legislation that's been proposed in Congress, are frankly weak sauce-- procedural protections of notice, just better notice, more consent, procedural protections, so that you can figure out what kind of information is held about us, if you went to all thousands of sites that had your information.

But we need to do far better. We need comprehensive, federal privacy legislation that is viewed as a civil rights statute that provides strong protection. If it's going to preempt state laws, it better provide strong obligations. And I'd like to see, sort of, states being able to add to and strengthen protections that we have. So federal law acting as a baseline, and states able to step in and provide more robust protection.

So it would be very much a statutory scheme, rather than an interpretation of the right to information privacy embedded in the 14th Amendment's Due Process clause. Which have to say, given the way, as a practical matter, the court is moving, would not be something, I think, this court. But that aside, my ideal nonetheless is a statutory approach.

ELLEN WALKER: The next question is from David Saunders. Without a standard, isn't your proposed Amendment just tantamount to second guessing as to what is reasonable?

DANIELLE CITRON: OK, so when talking about Section 230, because that's what you're referring to there, my reasonableness approach, what's interesting is actually much like, as tort law operates depending on the field, that what's reasonable there are professional practices. And this is particularly true. So I've been working on the issue of reasonable content moderation practices for the last 12 years.

And there is a entire professional organization called Trust And Safety for professionals. They have their own organization. And within the last 12 years, we have a baseline of what is reasonable. And I've included those sort of baseline requirements-- having clear policies, having modes of accountability, being able to easily report abuse.

So that I have suggestions about what would constitute reasonableness. And because this isn't new, in the sense that courts would have to assess this issue anew, and say, we don't know what reasonableness means.

There are actually practices on the ground for what's reasonable, vis-á-vis threats versus intimate images, and distinct practices that have been developing on the ground and within companies Trust and Safety Teams over the last 12 years.

ELLEN WALKER: The next question is from Mark Williams. I lobbied to help get SESTA passed to amend Section 230 to allow sex trafficking survivors to sue intermediaries for their role in facilitating sex trafficking. I agree with your legislative solution. And my employer IBM has called for your solution to become law.

Today Democrats and Republicans see content moderation very differently. Democrats want more moderation to curb misinformation and harms. And Republicans see moderation as squelching speech. What do you see as a path forward?

DANIELLE CITRON: And we appreciate it so bad. And I so appreciated IBM's endorsement of our approach. And I think it has an impact when companies come out and say, we need regulation, and this is a wise approach. I think, it resonates with staff. And you're right that there's disagreement about what the problem is. That so often, at least the sort of more liberal leaning side, the problem is too little filtering.

And for conservatives, the problem is too aggressive filtering. That is, your censoring my speech, and therefore we need to stop you. So one approach would say, you can essentially do no monitoring. And the other would say, we do too little and need to do more. And I'm in the camp of, we need to do more.

We have very little empirical proof that we're seeing over censorship of people's political views. Where we're seeing it, is with regard to hate speech and health disinformation, which I think some of the biggest platforms rightfully remove. So your question is, how do we get people, who don't have shared realities of what the problem is, how do you get them to work together.

That is a difficult, just real politic problem. And so to the extent FOSTA and SESTA had-- which you worked on and supported-- sort of bipartisan support. I've been skeptical about it, because I think we've seen the actual wording of the statute has led to an over monitoring, like almost the moderator's dilemma. We're seeing the takedown of too much sexual expression online.

But nonetheless, how are we going to get these folks to come together? And I think part of that is bridging conversations about what the problem is. You've got to get them to agree on what the problem is. And so often, at least where I've been seeing some movement, is around issues of the exploitation of children. And so much in the way that FOSTA and SESTA addressed online sex trafficking.

Also, the exploitation of children is what brings people together. But I think there's ways and opportunities to get staff to kind of come together and see the problem for what it is, which is that the legal shield is not in return. It's not earned, and it ought to be. We need to get back to the good Samaritan proposition.

So I guess, I'm working hard on educating staff on the Democratic and Republican side about what the problems really are, rather than the rhetoric of what we say that they are to get people to agree with them.

ELLEN WALKER: OK, and we have time for about one more question. This one is from Karen Rothenberg. If we care about this issue, how can we get involved? Are any civil rights organizations working in this area?

DANIELLE CITRON: Be still my beating heart. My first Dean, the Dean who told me that I should write and that I should join academia, the brilliant Karen Rothenberg. So she's just asked that question. She was my Dean at the University of Maryland. Gave me my first job and a chance to see myself as an academic. So I love you Karen Rothenberg.

And to answer the question, we have groups in the United States that you can join. So the Cyber Civil Rights Initiative, where I'm the vice president-- Dr. Mary Anne Franks is our president. We work on advocacy and also supporting victims through a hot line. And so the CCRI is a wonderful organization, both to look to learn about what we're doing, to help victims, and provide support to victims who are struggling.

In the UK, there is the End Revenge Porn hot line. So that we do have some. We're a mighty little band. We're small at CCRI. But there are some groups in the UK and in the United States that you can support. So thank you. So I can't tell if this screen, Ellen, means that I'm to wrap up.

I just wanted to say thank you, all of you, so much, UVA Law. One of the parts about being here that's been so special, is getting to know alumni, who are incredibly supportive of our mission. And so I am so happy to be here. I feel so nurtured in this community with faculty, staff, our students.

In fact, I'm so supportive of our school. One of my kids is a first year. And my other is joining us next year-- will be a first year. So the whole Citron family, including my spouse, loves UVA Law. So thank you so much. Thank you so much to the foundation for inviting me. It's such a pleasure. And thank you for your fantastic questions, of course, keen and brilliant questions. So thank you.