DANIELLE CITRON: There's definitely nothing better in life than being able to share your work with your beloved students. And so this is really meaningful to me. So thank you so much, all of you, for being here. And we agreed. So TOLU and I agreed that-- thank you so much for being my amazing mistress of ceremonies-- that I would do 15 minutes or 20 minutes describing the project. What it's all about. And then we're going to dive into some questions.

So let me just define for you what I mean by the concept of intimate privacy, which is at the heart of the book. It is how we manage the boundaries around our intimate lives. So it's information about and access to our bodies, our health, our innermost thoughts. Which, of course, we know we document every second per second a day, browsing, reading, searching, sharing, texting, emailing. It is our sexual activities, our sexual orientation, our gender. And it's our closest relationships.

So for us, I think-- I always lead often with people's experiences, because I think that's how we can viscerally understand them and how I've had experiences with companies and with lawmakers, how they can come to understand these issues. So I'm going to give you two examples about-- that have implicated and involve violations of intimate privacy.

So Joan, and I'm not using her real name-- recent grad of law school-- had traveled a number of states to help depose an individual witness in a case. She stayed in a hotel. And as one does, she was there for about two days. And when she landed home, she received an email from someone who said that the email sender was not a bad guy, too. And the email had a link.

The whole thing the email said is, watch this. Send me more nudes, or I share this with all of your colleagues in 24 hours. So she clicked on the link, and it was a link to-- from her hotel room, her undressing and her showering. So clearly, someone had planted a mini recording device in the bathroom. So she's urinating and she's taking off her clothing and showering. It was posted on Pornhub. And embedded in the name of the video, was her full name.

So she calls her favorite law professor. He calls me. I call Joan. Joan says, what do I do? And she reads me the email. And I said, you're absolutely not sending nudes. Let's wait this out. Sometimes there is no response. And this is where we are. And then we'll deal with Pornhub separately. But he made good on his threats.

So in 24 hours, he had clearly mined and weaponized against her all over social media, including her LinkedIn account. So that everyone who was a follower or friend on LinkedIn-- to the extent this person could find their email addresses, which is often easy because many people are available. These were her work colleagues. These were her law school classmates. You can find them online. They all received in their inbox the next day, from an email that looked like it was from Joan, so like a spoofed email.

And the message was, see me. I think you'll find this really exciting. This is my real self. Another quite salacious suggestion that she was interested in sex with them. So 24 hours later, not only is it emailed to all of her colleagues and friends, it is then seated on about 300 adult sites. Adult and adult finder sites, so those are sites where people put up ads. So it included her full name, her cell phone number, and the suggestion in many of these ads that she was interested and available for anonymous sex. And some said, rape fantasies.

So within the 48 hours, her whole life changes. Once from being a first year associate, doing-- basically, litigation associate doing her own thing, to having her life from what she understood of herself being sort of destroyed. She went to her boss. And she said, the hardest thing was to say to her boss, I know you got this email. And to think that her boss and her colleagues had seen her naked. She said, I no longer could see myself as myself. I looked in the mirror and I saw how they saw me. Like I was just a vagina. I was just a naked body. I was just someone showering.

She just didn't even almost know how to talk to them about it. She went to site for site. So there are 9,500 websites, whose raison d'étre is intimate image abuse. So these sites, this is their business. She went to many of them and asked them to take it down, but no one responded. The only site that responded of these types of sites was a site operator in Russia who said, if you send me more nudes in a video of you masturbating, I'll take it down. So met with sextortion, was her request.

Pornhub actually, every time she asked Pornhub to take it down, for three times they took it down. But the third time she got bothersome. So every time it would go down, it went up, went up. And then after three times, they just ignored her requests. And again, embedded in the video was her full name. So what Joan experienced was three types of intimate privacy violations; video voyeurism, an attempt at what we call sextortion, and non-consensual pornography-- intimate imagery.

It was there as Joan would explain, a before and after. Before, she loved using social media. Like Facebook, was how she kept in touch with her high school friends. So because she knew that her social media would be weaponized against her, she shut it down. She shut down LinkedIn because that's how this person clearly, figured out who to contact. And she had wanted to apply for a clerkship. She went to our fancy law school. She went to one of our fancy law schools.

And decided, listen, my Google is my CV, which she knew. And she said, look, I'm not applying to clerk on the Seventh Circuit. There's no chance. If you Google my name, what A, will come up initially? And she asked Google to de-index in searches of her name, these videos. But he was persistent. I say, he because more often than not, intimate privacy violators are male. The women do it too. But often, the victims are more often female, sexual and gender minorities, and non-whites. And often, kind of as-- on an intersectional basis.

And so Joan, she put off that plan. She had a fiance, a lovely human being, who didn't abandon her. He stood by her side, which is quite rare. But they put off getting married because as Joan explained to me, how could I have a wedding and invite all my family members, when all this stuff is about me online? I have to talk about it and explain myself. And she said, I knew that strangers, people who would meet me for the first time might very well see these images of me before they ever met me.

So they finally got married three years later. And it did take, I'd say, about four years since first half in 2018, for her to have a sense of safety. So this is a very common theme among intimate privacy violation victims. They radically change how they look. And so either gaining a tremendous amount of weight, so you're unrecognizable, or losing a tremendous amount of weight.

And for Joan, it was like crossfit. As soon as she got out of work, she was so thin as to be almost unrecognizable to me. And I had met her before in the initial stages, and then a year later. So incredibly thin that I couldn't recognize her. She also interestingly-- and this is another common theme. I interviewed 60 people from the United States, Iceland, Australia, the UK, and India. And a common theme of victims of intimate privacy violations is they get tattoos.

And the explanation is, I get to reclaim my body. It's mine. It's not this other person's. So that's Joan's story. And we can talk about how we ought to think about it, and why we have a lot of work to do for law and for industry norms. But I'm going to tie it to what I often call, what, spying ink in the book. Which is, there's a monsignor Jeffrey Burrell. And he was an administrator for the national organization of Catholic churches. It's a high up administrative role that he had.

And he had relationships with men, went to gay bars, and used the Grindr app. Now, Grindr was and remains sharing people's intimate information, including their profiles and their location data with advertisers and marketers, who are sharing it with location data brokers. And there are over 4,000 data brokers, who mine rank rates for us, and have about 10,000 data points on each and every one of us.

Now, an enterprising-- I don't if we'll call it enterprising. A reporter bought information about the monsignor from a location data broker. And because it's really easy, once you have location data about visits to gay bars, to then re-identify the mobile advertising ID number on your phone, that each and every one of us has. It's really easy to then connect it with you.

Now, this reporter told-- well, esteemed Catholic press. The press wrote about it. He lost his job. But Monsignor Burrell could be any one of us. That is all of the information that we share. And that includes just taking our phones with us everywhere we go, tells a really intimate story; who we're sleeping with, what doctor we're going to, what bars we're going to, who we love, and what we share. Our phones, our apps, our searches, tell so much about everything we care about. What we read, what we think about, who we love, and what intimate privacy violations do.

So this is companies, this is individual privacy violators, and governments. They're undermining our capacity. And you think, what's your first relationship with? It's with your body. It's through our bodies we figure out who we are. Not only who we are now, but who we want to be. And it is with our bodies that we develop authentic selves. And that takes a lot of time and a lot of work. And you've got to trust who you're with.

Privacy is not being alone. It's being with other people. And it's using devices that help us-- connect us with those other people. And it's intimate privacy that enables us to see ourselves with some sort of self respect. So that you think of yourself, not as an object as Joan did, but as a subject. Like you're the boss of your life, having self respect.

And it's also social esteem. That is how you're viewed-- is the respect. The dignity that you enjoy is how everyone else sees you. They don't give you the look like, I've seen you online. They look at you like a full person, a fully developed, whole human being. And without intimate privacy, we can't love each other. We develop relationships-- and I'm not just talking about people who are sleeping with. I'm talking about the kinds of people in this room are close friends.

How we develop close friendships is-- social psychologists teach us, it's like an onion. We reveal ourselves to one another. And it's called reciprocal vulnerability. And the only way we're going to do that is if we trust each other. If we trust each other and if we trust the companies that are storing our information, sharing our texts, and sharing all of our communications with each other. All those dating apps, all the ways that we interact with the world.

So the difficult news is that our intimate privacy is woefully under protected. We view data privacy, including intimate privacy as a consumer protection matter. And so what that means is if companies notify us on some privacy policy, which I'm going to take a poll, who reads them. Who reads their privacy policies? I see my five friends who do. But who reads their privacy policies or ever read a privacy policy that they've ever interacted with? Andrew, I see you. You and I, we read them. but who reads those privacy-- I love you. Sorry, Ajanae's one of my fellows and my research assistant, so I--

But who reads them? Nobody reads them, right? As long as companies don't lie to us, they are free to collect, share, exploit, and sell our data, including to data brokers whose biggest clients are law enforcement. In a post-Dobb world, our reproductive health data is going to be weaponized against women and girls exercising reproductive freedom. So my pitch in the book is that we ought to understand intimate privacy as a moral right, as a human right, and as a civil right.

And what I mean by the term civil rights isn't just in as we think of modern civil rights laws, as a commitment to anti-discrimination. It is that, but it is a legal right that each and every one of us enjoys, so that we can all flourish. So that we can feel like we belong, that we're citizens. And once we understand intimate privacy as a civil right, it changes the game entirely. It flips the default from being, sure, collect it all, sell it all. It's a business model proposition. It's profits. You need a really good reason to violate a civil right.

And when you are the holder of intimate information, just as schools, just as public transportation are the guardians of our-- for the disabled, the ability to use transportation. For schools, the guardians of our educations to be free from hostile environments. If you handle our intimate data, it means you're the steward. You're the caretaker of that data. And that might mean you can't collect it if you don't need it for the product or service. And it definitely means, you can never, ever, ever sell it.

And you know those 9,500 sites, that traffic and intimate image abuse? They're immune from responsibility right now, thanks to Section 230 of the Decency Act. People are like, what's this Section 230 thing? It's a nightmare. We have to fix it. And if we understood intimate privacy as a civil right, we would then shift the onus. And A, if you're a bad Samaritan trafficking, and soliciting, and encouraging, and keeping up intimate images, you are not enjoying that immunity from responsibility.

In the just ordinary business-- and I advise companies. If you keep up intimate privacy violations-- and you can make mistakes at scale. You've got a duty of care, that to deal with intimate image abuse responsibly. So we have to have a whole approach. And each and every one of us now-- I got to stop because I promised 20 minutes. But we all have a role in this.

We have young people in our lives. We have older people in our lives. We like, click, share. We don't think about it. And we're particularly drawn to gossip and salaciousness. And we have to teach. And we need to bring our humanity, friends, to the fore. Like kindness first, like lean into the fact that we're all human beings. We're all flawed. We all have sexuality, we all search adult sites. Hello, 42 billion people visited Pornhub last year. That means every single person in this room has visited Pornhub. I don't want to hear anything about it.

We need to give each other room to be ourselves. And we need to teach other people we care about to respect intimate privacy. So now I'm very, very, very excited to have my very dear student friends talk to me and ask me questions. Thank you.

[APPLAUSE]

Who's going first?

INTERVIEWER 1: Hmm, a quick question, we can start this way and work around. Oops, let's see if I can turn on the mic. Testing, testing. No, no, no. All right. Round two, there we go. Excellent. So digital spaces are obviously, an incredible place for connection. But also an incredible place of risk, as you've already discussed.

And especially, for queer folks and in particular, queer youth. But again, also very important for connection as they're exploring their identities and reaching beyond their physical spaces. So do you have any advice for how we can advise youth, and in particular, queer youths for navigating these spaces at least a little more safely?

DANIELLE CITRON: Yes. Some of the difficulty I always have is people who want tips, like how we protect ourselves. And I have this moment of sheer terror because there's often nothing I can tell you that's going to solve our problem. Like yes, put a little sticky note on your camera, on your computer. And yes, if you're going to-- first of all, if you're under 18, no one should be sharing nude images because it's considered under state and federal law, child sex abuse material. And prosecutors, many are dingbats, and they go after the children, not the predators.

So we've seen prosecutions of young people, of teenagers sharing nude photos with one another as one does. There's nothing wrong with it, but it implicates child pornography laws. So I would say to young people, don't do it. It's a structural problem. We need to moral suasion and bug the heck out of industry. We need to go to our lawmakers. And also to tell young people-- queer young people, that I want them to use all of these tools. These tools are such important tools of connection of community, of being seen. It gets better project.

There's so many amazing pieces of these tools that I want us to use. And I just would say, I guess my best advice is to think about the people we bring into our lives. And you can't-- there's no fail-safe. Every person I interviewed said, I really did trust that person. The problem with young people is they're often pressured into sharing nude images. And they often think, I'll just send it. They'll get off my back if I send it.

That's the moment you don't send it, is to trust them. And they often have-- their inner voice will tell them like, I don't trust this person. So I think, I don't want them to lead with distrust. I want us to be open to love and all relationships. But I think, for young people-- I'm especially worried, especially young queer kids because sextortion-- the rates of sextortion with girls and boys, and often queer kids is the highest category of cases.

Perpetrators will have over 300 victims before they're ever stopped in their tracks. And so I do have special concerns about children, especially because the rates of suicide are also really high when it comes to intimate privacy violations. So I think, trust and think about it. And don't share nude images until you're-- the law recognizes that there's nothing wrong with sexual expression at all, but wait till you're 18.

INTERVIEWER 2: Thank you. So last month, California passed laws prohibiting health care providers from releasing the medical information of individuals seeking abortion care in the state and prohibiting California corporations from releasing customer communications related to legal abortions in the state. Do you think that legislation like this will be effective in preventing law enforcement from hostile states, from weaponizing abortion seekers, private data, and digital communications? And just more broadly, how do you predict that regulation and enforcement of data privacy protections will continue to evolve in this post ops world?

DANIELLE CITRON: I always applaud California. I feel like as AG Harris once said, as we were working on a cyber exploitation together, as California goes, so goes the nation. And it's optimistic. But can be true, as the Brussels affect many, states follow. It's cheaper and easier to comply with one law, than many. It's a good start. But of course, law enforcement with a warrant, gets that data.

And it is true that Silicon Valley, many of these technologies are based in California. So that law does provide-- it's got knock on effects in really important ways. I've been working with Senator Warren and Representative Jacobs on federal bills that would prevent the sale-- A, limit the collection, but also ban the sale of intimate data to data brokers, which is part of this problem. And because law enforcement, we also need-- the Fourth Amendment is not for sale, an Act by Senator Warren to pass.

The problem is, well, law enforcement just buys it. And so we're in a sticky wicket because the data that I-- this is the deal, if we don't collect it, you can't get it. And it's circumstantial evidence of reproductive freedom. It's not the only evidence. But my fear is as we use period tracking apps and our location, that's then sold to data brokers. No matter what app is on your phone, it's tracking your location. My worry is that as law enforcement buys that data, that's not the basis-- that's not what's going to get you thrown in jail.

It's the basis of a warrant. It's the circumstantial evidence that says, it looks like this person had their period, then missed their period. Their location suggested they went to a clinic. And that then leads to the probable cause that leads the warrant, that then gets to their texts and communications, like in the Nebraska case, and their medical records. So I worry about the preconditions to permission to get a warrant. Good start. I always love California, but the beginning of a longer fight.

INTERVIEWER 3: OK. Thank you. In chapter A of the book, you propose reforms that Congress can make to Section 230, specifically Section 230(c)(1). Recently, the Supreme Court granted the cert to a case coming out of the Ninth, Gonzalez v Google, which examines whether section 230(c)(1)'s protection liability extends beyond traditional editorial functions to target recommendations. I'm wondering if you could talk a little bit about how you think the court's decision in Gonzalez, could impact intimate privacy for better or for worse. And if you would speculate a little bit on what you think the court's decision will ultimately be.

DANIELLE CITRON: You want to make me feel like Russian roulette with that one on the latter part of your question. So Section 230(c)(1), just to give everyone a sense of, there are two parts of Section 230 that by the way, the relevant title of the part of the statute we're talking about is called good Samaritan blocking or filtering of offensive material. So let's just be clear, we're talking about good Samaritans, supposedly.

OK. So (c)(1) is the leave up provision. So it says that we're not going to treat interactive computer services as the publishers or speakers of somebody else's content. It doesn't have any conditions. The language is quite plain. And so courts have interpreted it in a wildly, overbroad fashion. So that sites that solicit, that aid, and abet illegality, they enjoy the immunity as well.

Now, the Gonzales case versus Google, that the court just took up as a twin case with another case against Twitter. It involves the terrorism-- a federal law involving anti-terrorism protections, that has a civil liability provision for aiding and abetting, including spreading information about terrorist organizations.

And so normally, the case is civil liability. There is no exemption for civil liability. It would and should fall-- as most courts would say, would fall into the legal shield, no liability. The question that has-- there's been a small split in the circuits. And this is the least exciting case for me to be taken by the Supreme Court. So of course, they take it.

But there's a small split-- I think there's disagreement in the Second Circuit and two other circuits about whether the algorithmic amplification and profit making, that is recommendation systems, whether that transforms the provider into, in effect, a speaker of themselves. That is, they're creators of the content, because they're monetizing it, because they're trumpeting it, deamplifying, amplifying. That is, a recommendation engine is different from just publishing somebody else's speech, even if you're encouraging that speech. This is my worry.

So I can't say, what-- so I'm the vise president of the Cyber Civil Rights Initiative, an advocacy group. And we are now considering whether we file an amicus brief. So we are pondering, and puzzling what we might say, and considering whether we'll file an amicus. But what I can say is this case worries me. It worries me because the plaintiff who brought the case is someone who is Supreme Court litigator but knows nothing about Section 230. And my worry is that everything-- I'm just going to [? TS ?] my phone. It's not on, I promise. I'm not looking.

Everything we do with this thing involves algorithmic mediation and recommendation. My spell check is algorithmic recommendations. My searches-- like literally, everything that makes the online life manageable is algorithmic amplification or deamplification. I worry about the long tail of remove the shield. I'm enthusiastic about removing the shield generally, when you don't deserve it. I think should earn it. You should be a good Samaritan.

My worry is that it's like so overbroad. It's as if to vitiate 230. I think ultimately, I don't want to lose 230. I think it's given us a lot of great things. It's given us a whole lot of content that we would say, people can really express themselves, domestic violence victims can engage, political dissenters. There's so many people I want online, engaging, that is not destructive.

And my worry is that if we effectively take away Section 230, we're going to have an internet which is, its moderation first, like all prescreening. And like what's my spell check looking like? And it's not that all of this is presumed liability. None of this is strict liability. So if you take away the shield, all that means is people can sue. But in the shadow of potential lawsuits, I don't know what the long tail looks like.

So our worry at CCRI is every organization now wants to know what we're doing, in this case. And we're not going to join, I don't think, with other people. We need to speak to our own issues about what we care about and intimate privacy. I think any time you file an amicus-- like this isn't the right case. We're not going to join the plaintiff. I'm pretty sure we're going to do something.

Your then question was, well, what do I think is going to happen? Oi, that anything good is going to come from a very weird set of bedfellows on this issue. Because you've got Justice Thomas, who I found myself agreeing with him in his dissent to a certain case, where he says 230's interpretation of (c)(1) has gone way too far. And I'm like, yes, I'm totally with you.

So it has been interpreted in an overbroad way, but this is not the example of the overbroad way. And my worry is that there's a narrative about 230-- the part we didn't mention, which is section 230(c)(2), which allows you to take down illegality and other kinds of offensive content. It makes the internet what the internet is, man. I do not want--

I'm soon to be off Twitter, if there are no rules. I don't want to hang out with neo-Nazis, spam, and lunatics. I'm out. I love Twitter. I'm so sad that my only social media meaningful footprint will be taken away if Elon Musk decides there's no moderation. I hate that idea. I worry though, that the court might seize on this case, in dicta. In dicta, of course, it's not about a (c)(2) case.

And say something like (c)(2) is very, very narrow. And then therefore, will be gamed by all sorts of people and lead to litigation with really troubling results so that we see no moderation. That's not the universe I want us in, either. So I don't know. I hate-- sorry. I'm like, I can't predict. This is truly, really above my pay grade in many ways. Like God bless the clerks, good luck with that. So sorry, I can't guess. I feel a little out of my skis on that one. I'm going to be wrong.

INTERVIEWER 4: Well, professor, thanks for having us tonight. One of the themes that we recognize in privacy laws, the balance of power between individual privacy interests, and governmental interests, and security, or whatever a governmental interest might be. And I think this book attempts to bridge the gap between the government and the individual. There's also a commercialization aspect in spot the spies chapter, and also the government chapter and the government's responsibility, and how our data is commercialized.

So I'm wondering, because if I ask you to talk about the evils of capitalism, I'm sure you could do that. Are there any positive aspects of capitalism? Because we've seen politicians-- Yang in 2020 talk about how we could benefit off of a universal basic income. Or particularly, marginalized communities that have their data harvested and/or are powerless. Do you see those mechanisms, those being things that we can use to reclaim dignity, maybe through capitalism? I know that's a wild concept.

DANIELLE CITRON: I love that question. You could ask me any wild question, any day. So can our intimate privacy-- can our intimate data be leveraged in ways that are dignity enhancing, autonomy securing, intimacy securing ways for marginalized communities? And there is great potential. I always worry when people say there's an app for that. My first response is, oi. And then the next response is Bitcoin. And then I want to cry. So the journals about Bitcoin need to go away.

But can industry norms adapt, and enable, and protect, and secure opportunities for marginalized communities? Absolutely. And so I've been working with companies to do just that. How can we use this data for good? And so I'm going to hearken back to a dear friend, Mutale Nkonde who runs AI for the People. And she's been taking the case to companies, that the designers of these tools need to look like everyone. We need way more black software engineers and product designers.

Because not only can people imagine themselves as doing that in the future, but they're going to see the harm, that as you build the tools-- and you build tools with harm in mind, only if you understand the harm, and can imagine it for yourself. So there are strategies I think, that industries must adopt right now before we do too much damage. Because the ethos of building it-- the beta test ethos has gotten us in a sticky wicket. We're in a world of harm.

Because poor you, you're taking-- lovely you, you're taking my class. What you entail are my privacy law in theory class, which is the story of surveillance, is a story of Black surveillance. The story of surveillance of marginalized communities. It's a long story. It's a story from the 1700s. Our governmental structures of surveillance were aimed at enslaved individuals in the late 1700s onward.

So I worry that what we have seen, whether that's reading Safiya Noble's *Algorithms of Oppression,* or Khiara Bridges' *The Poverty of Privacy Rights,* or Dr. Simone Browne's brilliant *Dark Matters.* The way that we have seen these tools of capitalism and also government mandates, have been used as Dr. Anita Allen would say, the Black panopticon. So I worry that unregulated-- that we know the lesson of unregulated markets. It's markets' failure and discrimination. I have a healthy skepticism.

INTERVIEWER 4: So the answer is no?

DANIELLE CITRON: Yes. Sorry. So yeah, you know me well. I'm going to have a big wind up for my-- it's not that I don't believe in the potential for industry norms. I wouldn't work with Twitter, and Bumble, and TikTok, and Facebook, Spotify, if I didn't believe in it. And I believe that career staff really think they're doing good. And it is often the c-suite because monetization is welcomed. And it's in shareholders' interests that any time there's a safety issue or privacy protective measures that would cost companies money, the answer is too bad, so sad. Build it, we'll throw content moderators at it later.

So I remain skeptical because it's 12 years of working with these companies, that makes sense? It's not that I don't want it to work, I'm so ready for industry or for the market to work. I am-- bring it. We're in a world in which we need federal legislation that's comprehensive. We have some impending possibilities, but we're not there yet. So what do they say? It's a hard possible, rather than no, never.

INTERVIEWER 5: I don't if this is on. It is on. So in your book, you describe how intimate privacy violations are really a failure, both on the legal side and for social norms in Silicon Valley and such. And you also really illustrate through all of these stories of victims in other countries, in Ireland, South Korea, and elsewhere. Just that this is not an issue confined to the US. And it's really one of international scope.

And so to address some of these issues in the US, on the legal side, you propose your Section 230 reform, comprehensive federal privacy framework rules. And on the social norms side, you propose training programs and educating your peers and youth. And so I was just wondering if maybe you could explain the extent to which these changes in the US might be different from how an approach might be taken internationally. And whether it might be similar.

DANIELLE CITRON: I get excited to talk about South Korea, because they have come a long way. And there's parts of the South Korean response that we can't bear because of the First Amendment, but there is so much that we can. So in 2000, South Korea-- 2018, going to the public bathroom as a woman was often a nonstarter because the number of hidden video cams in public bathrooms that were then streamed to the internet, was basically every bathroom.

So that women would-- and they called it Molka, which is a jokey name. It's like hidden camera. Or I forgot the TV show from the '70s. But there was one in South Korea. And Molka is the name of the TV show. And so the phenomenon was named after a vicious intimate privacy violation. It's named after a jokey TV show. So you can see how society is responding to it.

So women, for like $20-- I can't tell you exactly in one, but it's $20. You got-- this is pre-pandemic-- a mask so that your face wouldn't be seen when you went to the restroom. And silicones, you can fill in gaps in the bathroom stalls. And most women just didn't go to the restroom. It's not great on your bladder, to decide you can't go to a public restroom.

And in 2018, this is like social movement from the ground up. In the beginning of 2018, 30,000 women and allies took to the streets of Seoul. And the signs were, "My life is not your porn." Everybody had the sign. Three months later, 60,000 people, streets of Seoul. Four months later, 75,000 people. For the 5th match, same year in December's frigid-- really cold out 2018. 120,000 people took to the streets.

And that's when the president and the government decided, we've got to get our acts together. This is untenable. So I've been advising the Digital Sex Crime Information Commissioner, now, instead of calling it Molka-- the newly created Information Commissioner. As we urge them, listen to advocates, and call it the digital sex crime content. No more Molka. No more, haha, joking.

And what the South Korean Government did, and the Information Commissioner, who they're extraordinary, created a whole of society approach. So the first things first was to tackle platforms that are hosted in South Korea. As my colleagues in South Korea have told me, there's nothing they can do about Twitter in the US. So often when a platform would take something down in South Korea, you just go to the next best thing, and go post it in a site hosted in the United States.

But what South Korea did was strong penalties against platforms hosted in South Korea, and a 24-hour or a 48-hour period in which they could take down posts. So that no liability, if you take down this content that's ruining people's lives. So changed their approach to platform liability, strengthened criminal penalties. They have a comprehensive intimate privacy law, which covers deepfake sex videos. Like all different types and stripes, with a focus on intimate privacy.

Rather than our laws which are sort of siloed, like misdemeanor video voyeurism, misdemeanor non-consensual pornography. In the United States, they're as if they're unconnected problems. But in South Korea, there's a comprehensive law that they now enforce. Rather than, literally, the only person who got punished was the woman complaining. Now, people can get caught. It's everyday, people-- and get punished.

And most importantly, and this is what I value so much, is a whole victim approach. Where people who have faced non-consensual intimate imagery and other forms of Digital Sex Crime Information, get support from the government. Support if they've lost their jobs, economic support, financial support, psychological support.

And the numbers that were just shared with me-- so there were like 6,000 victims, who reported to the DSCI commissioner about having experienced video voyeurism. And almost 95% of them took up the welcoming opportunity for psychological support. So that victims need the psychological support and are getting supported.

So some of that I think, is untenable in the United States in the sense of, I think we could have a 48-hour takedown. We do it for copyright. Why do we care so much about copyrighted material, but not my vagina? I'm sorry, but that is just not an OK-- sorry, excuse me. So that happens when you take my class. These students me very well.

Why treat copyrights so differently from-- content ID means that content that violates copyright is never posted. It's filtered immediately through software management. We can have that kind of change in platform responsibility. That, we absolutely can do. Can we have a whole approach to victim services? Absolutely. Can we have a very comprehensive strong law?

The ACLU is going to kick and scream, we've passed laws. So since Mary Anne Franks and I have been working on the issue of nonconsensual intimate imagery, there were two laws that criminalized the practice in the last-- so 2014, now, we're 2022. There are 48 state laws, DC and two territories. We've come a long way, but they're all misdemeanors. I have a feeling that the ACLU would scream, if we proposed felonies, because they would say it's speech.

And my response is, it's coerced sexual expression. And in the five states where our laws have been challenged, all the way up to the State's Supreme Court, we went through the crucible of strict scrutiny, and our laws all have been upheld. So bring it, I'm ready. We have laws that we have at the ready, right?

I worry, though, that the civil liberties community is ready to fight for the privacy of our faces and facial recognition software. God bless, I agree 100%. But not for my nude body? I'm so confused. So I think the civil liberties community makes a lot of stuff difficult. I see a hand.

CREW: Oh. I was just going to say really quick--

DANIELLE CITRON: Oh, go ahead. Sorry.

CREW: --that was a really great conversation. I wanted us to give our panelists a quick round of applause because they did a great job.

[APPLAUSE]

And we do have time for questions. I'm going to try to get this mic over to you if you have a question, because we're recording this. So if you just raise your hand, I'll try to get over to you. OK, Bertie. Taylor, if you would pass Bertie your mic, that would be great.

DANIELLE CITRON: No, no, no. Well, we're recording it. So we want --

CREW: We want to hear.

BERTIE: Oh, OK. Got it.

DANIELLE CITRON: Yeah. We want to hear everyone.

BERTIE: Thank you. So with the issue of criminalization or at least criminalizing these private sex crimes essentially, which is what they are, is there a fear there that it would be unjustly enforced, specifically against communities of color?

DANIELLE CITRON: It's a great, great question. And in my book, the Black Jim Crow, as Michelle Alexander has described it is, my commitment to intimate privacy should not come at the cost of equality. It's like first things first. But what I can tell you about gendered harms is that they're woefully under enforced. But you're right, to the extent we see enforcement of intimate privacy violations, who are we arresting? Women and people of color.

Like they're nary in arrest. But the five arrests in the one state is the one ex-girlfriend who is angry. Do you what I'm saying? We have a big education problem. So my book is so focused on the civil story, that is enabling pro bono services, changing Section 230. And I say explicitly.

And it's a little at odds with my organization, CCRI, because we're allowed to write different things on our advocacy group. That I don't lean as hard into criminal law because I worry for that precise reason, that we're going to see a disproportionate impact on marginalized communities without question, as we've seen-- as to drug crimes. But gender crimes have less of a risk because we just don't enforce them at all. But you're right, that when we do it often, it is on the backs of marginalized communities.

And so a huge part of my agenda is education of law enforcement. I did that with AG Harris, when we worked together for two years. And we have so much work to do with educating law enforcement. Because when most victims walk in the precinct-- and it's at the state and local level. Their response is, why did you take that photo of yourself? And even when it's a deepfake sex video, it's like what did you expect? You were on Instagram. Or boys will be boys. Like ignore it, turn off your computer.

But you're right that if we're going to go forward with a comprehensive reform to criminal law, that we need education that's paired with it, and incredibly mindful of the way in which the criminal justice system has disenfranchised and incarcerated way too many Black men over nonsense.

BERTIE: Sure. And so do you feel like in your approach to solution, that criminalization is one part of the solution?

DANIELLE CITRON: It is. And I think an important piece to, why at all? My hope is just deterrence. We always talk in law school about, what are the theories behind criminal law?

A study that we did at the Cyber Civil Rights Initiative in 2017 was, we were able to find and interview people who had been perpetrators. And 60% of the people who were the perpetrators responded to our question of, why did you do it? And would it change your mind if you knew it was-- you would face criminal penalties? And 67% or so people said it was for fun. They were doing it to show off. It wasn't revenge. That's nonsense, right?

And most of the individuals said if they knew there are criminal penalties, there's no chance, no how they would have done it. And that has been replicated in studies from Australia, from the eSafety Commission. So I feel like I can't take that off the table, in some sense, but it's only-- and I say this really explicitly in the chapter. The sort of comprehensive response intimate privacy violations, which leads with the civil story.

And all the ways that we can and should reform, getting lawyers. Everyone, hello, pro bono. I'm talking to Davis Polk next week, getting them hopefully, to take on pro bono cases. It should be all your firms. But until we get there, I do think we need to have a deterrence strategy.

BERTIE: Thank you.

DANIELLE CITRON: Thank you.

CREW: More questions? OK. I'm coming, give me a second.

INTERVIEWER 6: Hello. Thank you so much for doing this talk. So my question is-- and I've been practicing it. So let's see if I can articulate it in the way that I've been mulling it over in my mind. But I guess, basically, sometimes topics like these are just the landscape of privacy, or the lack thereof-- or the lack of, I guess, autonomy that we have over our own internet privacy, can sometimes sound like bleak. And to me, at least apocalyptic.

I was wondering, how do you-- and I guess, in the age that we're in, technology is basically integrated in every part of our lives. And so it would be very difficult for us to completely come off of all the things-- or just stop using technology. Do you have any advice or things that you could say for us to-- how we should engage with technology within the little-- see, and this is where it breaks down-- but with the little, I guess, privacy that we have now.

DANIELLE CITRON: Oh, God. I'm so sorry to be bleak, but it's true. I say, hello, and I'm bleak. So I can't help myself. And I share that frustration. And I say this every time people-- when Dobbs first came down, the question was, do we get rid of our period tracking apps? And my answer was sadly, yes. Why provide opportunities for tracking that can be used as circumstantial evidence for a warrant? I always say, get rid of Amazon Echo, bye. It should never be in your house. No, no. OK, we'll talk about why.

But how can we-- what are the little things we can do? It's really difficult to-- if you are a California resident. And how many California residents are there? We have some. Your California law allows you to opt out if you go to a company and say, do not sell or share my data. You can do that, but it's really hard. There's no one like, do not sell. That's like the do not call list, which is what we need.

It's really hard to do as a person, individual. Can you go to the 10,000 data brokers? No. You don't who they are and I don't either. It's almost so enormous as to take a whole year of your life. But I do think that we can communicate to companies in small ways. Small ways though, that are measurable. So like I bug the heck out of Reddit. They have subreddits devoted to intimate privacy violations. And I report the same damn subreddits with 1.1 million users.

It's so clearly, NCII. I report it literally every week. And I'm to the point where I testify with Steve Huffman, the CEO. I'm ready to just get right to him. Like say, Steve, buddy, take this down. This is so clearly, NCII. And every time I report it, I get the message 48 hours later, this doesn't violate our policies. They bear nonconsensual pornography. So I would say, the small things that we can do is to when you see intimate privacy violations report it. A lot of sites prohibit it. It's tough at scale.

Even let's say, Twitter, has a tough time catching everything though they've banned nonconsensual pornography since 2016 or '15. Help your friends who are experiencing it. You can go to Google and ask them to deindex in searches of your name, non-consensual intimate imagery. Help if your friend has experienced this and has a tough time. It's really hard when you're facing it yourself. It's like a tsunami. You almost don't where to begin. We can help people we care about.

And I think the hardest part is realizing that it's structural. And that bringing the case that is-- it's very hard. The idea of noticing consent is premised on the notion as that anything we say is meaningful. And it's not. That is, companies can collect, share, sell, exploit, use our data without our explicit permission as a presumption. So we need to change the law. And we can use moral suasion against companies.

So I think it's going to take collective action. That's really tough to do. It's hard to get people to vote. Please, everybody, vote. It's really tough to get all of us to do things together, but we have to speak in one voice together. We're much stronger when we have support for one another. And I have some tips. I just feel like I hate telling them because; strong passwords, double-factor authentication. You know, look, I have four pages. They made me write it, tips in my book. I couldn't resist my editor's insistence, people love tips. OK?

But I mean, one thing too is I always think, talk to your partners and your friends about your expectations. People often leave that unsaid. One thing you can do is let people in your life know your expectations about sharing your email and texts, forget the nude images. But whatever it is, have conversations with people you care about and you communicate with about the kinds of privacy you expect of each other.

And for all of you, lean into your humanity, friends. We care about each other. We protect each other. That ought to be how we live every day of our lives. So it's small solace. So I couldn't-- what do they say? A Band-Aid for a bomb, you know what I mean? Like I know it's small, but it is what we can do. Thank you.

CREW: Any more questions? Yeah.

INTERVIEWER 7: Thanks for taking the time to talk to us. Outside of the practicality of getting something like this passed, what are your thoughts on just the wholesale banning of business models that rely on this type of just invading people's privacy, and spying on them, and then selling their data.

DANIELLE CITRON: Love it, let's ban it. Ad surveillance, the dumbest theory ever. Do we really always buy all this stuff? Do we really need ads tailored to us? We absolutely don't. I'm still going to buy the damn shoes. Do you what I'm saying? I just think the premise-- that the advertising model-- the premise of free is absurd. Pay for your newspapers. Pay for books. Pay for music. I love Spotify. And I work with them, but I am obsessed. Pay for stuff. Yet, we are paying. We're just paying with our futures. We're paying with our intimate data.

And what we don't realize is that downstream, this ad-based model, which is absurd, is exploitative of the most vulnerable. The jobs you never get and never get called to get interviewed for is because third party hiring services know that at some point, you get migraines, and they're not going to hire you. Your life insurance premiums go up and you never why. It's because some intimate data says something about your potential health conditions. You've been ranked, and rated, and scored, that you're going to someday get type 2 diabetes or develop colon cancer.

The whole thing is premised on lies. It's an absurd model. So sorry. I am willing, so Andre ready. Buh bye. I guess I am being assertive now. You knew we'd get me there, right? It's the dumbest model, bye. If I-- it was-- if I'm queen for a day.

BERTIE: I think we have time for one more question. Oh, all the way in the back. Oh, sorry, he was first.

AUDIENCE: Hi. Sorry, I'm in the back. But at least you guys have a mic, so that's good.

DANIELLE CITRON: Thank you for staying and standing.

AUDIENCE: Yeah, no. So you just talked about a pretty aggressive standpoint, I would say, in the negative towards ads, right? But from an engineering standpoint, let's look at *The Social Network.* It's a very interesting film, but like let's focus on Facebook.

DANIELLE CITRON: [INAUDIBLE]

AUDIENCE: Yeah, I mean, I think it's a very interesting movie, right? It touches on some very, lets call it interesting aspects of life. But yeah, so when we're thinking about Facebook or I mean, maybe even just Facemash, the way that it first got adopted was when people don't need to go over that initial energy activation barrier of actually having to pay for something, right?

When you have something that's free online, it makes it much faster for it to grow. And you talk about things like AI and data personalization, right? You're absolutely right that in a lot of cases ads might not necessarily be useful for the user. But personalizing things to them, personalized job alerts, things like that, they do make use of your data.

Or personalizing weather information if that's what you want, that can also significantly increase utility in life. There are certain types of data-based applications, for example, that might maybe even use data, for example, machine learning, a lot of pre-label data that one might consider to be insecure in order to create abilities for people with-- people who are disabled. So there is a lot of kind of-- there's a lot of benefit out of having that type of labeled data.

So in a world where ML is going to continuously become more and more important, where our society is continuously getting more and more important insights out of that data, and then that data is also enabling various different parts of the economy, what is your standpoint on siphoning off the entire operation? And if it's not to just siphon off all of the potential benefits we can get out of data in the first place, how would you recommend that we maintain that privacy?

Are you thinking of just straight up anonymizing all of the data so that way, there's no label data ascribed to a given individual? Or are you thinking of just shutting off all types of data collection that could potentially yield benefits?

DANIELLE CITRON: OK, great. So you've a couple of questions there I want to respond to, which is faster isn't better, right? Faster is also faster to discrimination. Faster is easier, quicker, no friction to abuse. And it's so often about transaction costs when it comes to illegality, suffering, right?

So faster isn't better. Technological determinism is on us. That is we imbibe the notion that because we can do it faster and at scale, it's on us, right? We are making decisions about the tools we want to build. We've got to be much more thoughtful about the tools that we build.

And one thing I have to say is that, yes, data can be used for good. Absolutely. I think my highest priority is public health, right? We can and often do ask with explicit affirmative consent with protections around HIPAA to do research. Honestly, I would never give up big data when it comes to public health breakthroughs.

But I can tell you I'm really happy to give up ads for my Ferragamos. 100% ready to get rid of those, right? My tracking of my CVS purchases, my searches, my visits to WebMD, my visits if I'm young, a dating app, et cetera, whatever, right?

So in my book, I'm not as aggressive in my recent queen for a day imagining. I set strong limits around how to be a data steward and guardian. And I say if you're going to collect intimate information, then it needs to be strictly necessary for the product and service and that you can't sell it and that you have to have commitments of loyalty, non-exploitation, care, and crucially anti-discrimination commitments.

So I'm not as bold as in the book as I think we don't-- I'm pretty pragmatic operator. So I sort of working in the world in which I'm living. And some of my recommendations are embedded in the Americans of Data Protection Privacy Act that has bipartisan support in the House. So I'm not giving up at all about this.

But the idea that we can throw generative adversarial networks or cool, whip bang machine learning algorithms at it, I'm not impressed. It leads to a lot of oppression. Asks Safiya Noble. So I think we've got to be careful about what we build because we make-- we are building dystopia.

BERTIE: Great. Well, that's a wrap. Thank you everyone so much for coming.

[APPLAUSE]

And can we give a round of applause to Professor Citron?

[APPLAUSE]

DANIELLE CITRON: Yeah, thank you so much, my student leaders. I love you, love. Thank you. Thank you, everyone.

BERTIE: This was really fun. If you have any more questions, send her an email, take her class. She's teaching lots of them. But yeah, everyone have a good night.