

UVA Law – Privacy and Democracy in Technology

MAX LARSON: Perfect. All right. Thanks so much, everyone, for joining us. We're very excited to have this panel today. We're sponsored by ACS, Lyst, and the new LawTech Center. And we have three stunning panelists. We'll start.

Megan Gray, here on the right, is a principal at GrayMatters Law and Policy. She's an advocate for entrepreneurial companies at the intersection of free speech, privacy, online content, and competition. She was formerly general counsel and vice president of Public Policy at DuckDuckGo-- she brought some shirts for those who are interested-- and an attorney at the Federal Trade Commission's Bureau of Consumer Protection Division of Enforcement, where she was lead counsel in the first consumer privacy civil penalty case.

To her left is Professor Danielle Citron, who's the Jefferson Scholars Foundation Schenck Distinguished Professor in Law, the Caddell and Chapman Professor of Law, and the Director of the LawTech Center here at UVA. She's the author of *Hate Crimes in Cyberspace*, and in 2019, Citron was named a MacArthur Fellow based on her work in cyber stalking and intimate privacy. Her upcoming book, *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age* will be published next fall.

And joining us on Zoom, we're very excited to have Rachel Levinson-Waldman, who's Deputy Director of the Liberty National Security Program at the Brennan Center for Justice. She leads the Brennan Center's work on social media surveillance by law enforcement bodies and is active on broader issues related to policing and technology, including body cameras, protective policing, facial recognition, and information collection in the immigration context.

Her most recent work includes the groundbreaking release of documents exposing LAPD's broad social media monitoring practices. Prior to joining the Brennan Center, Levinson-Waldman served as counsel to the American Association of University Professors and as a trial attorney in the Civil Rights Division of the Department of Justice.

Can we all give them a warm round of applause for joining us?

[APPLAUSE]

DANIELLE CITRON: Rachel, we are, in fact, really pretending that you are with us, so we have scooched our chair as if you are sitting next to us.

RACHEL LEVINSON-WALDMAN: That is very kind. I wish I were there in person. So this is a second best.

MAX LARSON: Great. Now I think to start, if we can maybe start with the order I introduced you all, and you all can elaborate a little bit on your relevant positions and priorities as advocates before we move to a discussion of some contemporary privacy frameworks and changes.

MEGAN GRAY: Sure. So first off, the DuckDuckGo merch that's on the table. There's books, stickers, shirts, mis-sized shirts because it's the remnants of what I had. But we have sent boxes to Max. So you will have your assorted sizes, and just check in with her later.

My background. I went to University of Texas Law School, simultaneously got a master's degree in public policy. And then after that, I moved to Los Angeles, where I worked for big law and was at the first

internet age. And I did content moderation. I did privacy, anonymous speech. I did just about everything there. So that perspective has been incredibly valuable as I've moved forward in my career into civil rights advocacy, privacy advocacy, government, and then in house, and then my own firm. So it is interesting, and I'm very fortunate that I've got to see so many different angles.

The part that interests me right now with privacy and how to deal with the toxic environment and problematic speech that we're all aware of is I'm concerned that we're focusing on the wrong thing. It's kind of like being concerned about privacy and then having cookie banners. That has done nothing. It has slowed down the cause of trying to fix the online privacy dilemma by spending so much time negotiating and enacting and implementing these dumb cookie banners, which have done nothing to solve anything. And so my concern is that the problems that we're trying to solve for now, in my mind, seem to be going in a similar misdirection that's going to slow down what we're actually trying to accomplish.

DANIELLE CITRON: Thank you. May I ask a follow-up?

MEGAN GRAY: Sure.

DANIELLE CITRON: So what's the misdirection? I mean, we have some myths and misunderstandings around 230. I'm happy to give everyone a little primer on what it is, Section 230, and what it was meant to accomplish. But it'd be interesting to kind of at the start where we're being misdirected in your view.

MEGAN GRAY: Sure. I think the misdirection is that we're trying to get rid of speech that we don't like-- amplification, highlights, toxic Facebook groups. All of those, I understand why we don't like them. I don't like them. But I don't think, if you're going to be practical about it, we're not going to be changing the First Amendment. So given that, there's only so much we can do because that is what a democracy is. It's going to have some really ugly people who talk.

So that's not going to change. And I'd rather see more focus on, OK, what we're really, I think, trying to grapple with is that we are inundated with this. There is no other place to go. We cannot escape from it. It drowns out more healthy conversations. And how do we get to a world where we're not completely submerged in a sea of hate?

DANIELLE CITRON: So I think that's really helpful to start us off and to frame our conversation because you might imagine, I'm going to disagree with you a little bit and what we mean by the concept of speech. But just to start us off, Section 230 is a federal law that Congress passed in 1996 as part of what was called the Communications Decency Act. Just let's pause for a second, decency. It was like an anti-porn statute which, believe it or not, we once thought we could get rid of porn on the internet, a useless proposition. But most of the statute is struck down as unconstitutional, and rightly so.

But what remains is part of the statute called-- this is the title of it-- Good Samaritan Blocking and Filtering of Offensive Speech. And the idea was-- so Ron Wyden and Chris Cox, then two Congress folks, got together. And there was trial court decision that really upset them. It disturbed them because it found that defamatory speech, what it jeopardized, early internet service provider are facing was strict liability, essentially, as a publisher.

And so Cox and Wyden, they wanted to encourage responsible content moderation. They wanted people to act-- that is, the providers of the internet platforms that they couldn't imagine then but were in the future-- that they would have a legal shield for engaging as good Samaritans blocking and filtering of offensive speech. They also recognized that if you took down too much, you had to act in good faith. So this is the provision that we're talking about, at least so many of us are. And Congress woke up to this issue. After 12 years of doing nothing, all of a sudden it's the thing everyone wants to talk about. And it is.

There are a lot of myths and misperceptions about what Section 230 does, what the problems are, what the pathologies are.

And so you have folks say the problem with Section 230 is that it enables the filtering of speech, my speech, and that really pisses me off. It's censorship, even though we're talking about private companies. So it's not censorship in the classic First Amendment sense.

So that's, on the one hand, one complaint about Section 230 is that it enables the censorship or the removal and blocking of too much speech, too much speech that I like.

And on the other hand, there are those who criticize Section 230 for enabling the under filtering of troubling speech activity. So on the one hand, Section 230 is a gift because it has, for the past 25 plus years, given us the Arab Spring. Section 230 is why platforms like Twitter didn't crack down when we had bravery on the streets, whether it was Cairo-- throughout the Middle East.

At the same time, Section 230 is why we have revenge porn sites whose raison d'etre, whose business model is the tormenting of individuals, the publication of their nude photos without consent, often with their names attached to them. And what happens is victims go to these site operators-- there are over 9,500 of them in the country. They're all, of course, located in the United States, for the most part because why? We allow them to operate without any risk of liability.

So the most notorious revenge porn site, Anon-IB, shut down by the Danish police, where does it set up shop? Las Vegas, alive and well and tormenting individuals. So Section 230, it gives us a lot of great things. But it also has given us not just troubling speech, not just hate speech, which is fully protected by the First Amendment, but online assaults that drive people offline.

So cyber stalking, that is, the combination of defamation, privacy invasions, of threats of violence that silence people, that we have studies that show, at the Cyber Civil Rights Initiative, that the cost of online assaults, they fall on the shoulders of women and minorities, and often gender and sexual minorities. And they chase them offline. They make it impossible to live and work in an age in which Google is RCV.

And so there are speech costs that I think we don't wrestle with enough. And so I want to change Section 230, and we'll talk about how I think we should change it. So I guess I'm so glad you framed this for us.

That is, you're saying there's troubling speech. And maybe one way to get it isn't changing Section 230. But I don't think we're just talking about First Amendment speech. We're talking about all activity online, which isn't just ones and zeros. It's not just free expression and protected speech. It is speech we do not we-- I feel like I'm such a great faculty here. Oh, my gosh. Where's Fred Schauer and Leslie Kendrick when we need them? There's so much speech that we think doesn't come within the protection of the First Amendment. We know that there are 21 crimes that are made of just ones and zeros.

And so to be clear, it's not all speech. And Section 230 even protects the sale of guns and defective products, which is absurd. OK. So I'm going to stop there and let Rachel-- you can tell I have strong opinions about this.

MEGAN GRAY: But to be clear, I mean--

DANIELLE CITRON: Oh, no.

MEGAN GRAY: --it is not that 230 protects--

DANIELLE CITRON: Rachel, don't you worry.

MEGAN GRAY: --the sale of guns. It protects companies who are hosting--

DANIELLE CITRON: Right. But they are getting a cut of the sale of guns, and that's absurd. OK. I'm glad we agree on that one. OK, Rachel. We're ready for you

RACHEL LEVINSON-WALDMAN: All right. Thank you. Let me just give, as Megan did, maybe just a little bit of background on who I am and the work that I do at the Brennan Center. And then I can bring in my angle on social media, which is a little bit different.

So as you heard, I'm Deputy Director of the Liberty National Security Program at the Brennan Center. For folks who aren't familiar with the Brennan Center, it's an organization that's based in New York. It's affiliated with NYU Law School. We've been around for about 25 years, give or take. I'm in our DC office. We have a 15- to 20-person DC office. New York is now probably 125 people.

How I always describe the Brennan Center is that we're focused on kind of shoring up the systems of democracy. So whether that be access to the ballot, campaign finance reform, independent judiciary, ending mass incarceration, or in our program, Liberty and National Security Program, hasn't been around for quite as long as the Brennan Center itself, but historically, we've been focused on post-9/11 civil liberties issues. So that was privacy, secrecy, domestic intelligence gathering, over classification, Islamophobia, sort of a broad range. And those are still very much our bread and butter.

But over the last, now, almost seven or eight years, our footprint has kind of expanded to also include issues related to policing and technology and civil liberties and civil rights, in large part kind of coming out of a recognition that many of the issues, Fourth Amendment issues and just kind of privacy and First Amendment issues generally that we were seeing in the national security space very much transferred to the policing and technology space.

A lot of the technologies themselves kind of originate in the national security sphere and then are brought to domestic policing. And often the funding or justification for police technology also comes out of kind of a national security or counter terrorism footing. And then they are most often put into service in the war on drugs. But [INAUDIBLE] justifications we need this high tech technology because we're going to be kind of engaging in some kind of counter terrorism.

So [INAUDIBLE] a part of that shift to kind of opening our aperture to include policing and technology issues. Starting now several years ago, maybe three or four years ago, I started looking more at use of social media, starting really with how police departments were using social media, not in terms of outward communication or education, although there's a lot of that, that we're looking for this person, or we are hosting a block party on this date. We're really using social media to gather information. So that could be as part of criminal investigations, as part of situational awareness, part of just general kind of tracking and monitoring. It's used a lot to make determinations, often incorrect, about gang affiliation and gang designation.

We started looking into this several years ago kind of coming out of work that we had been doing on surveillance technologies in public spaces, and also predictive policing programs, and seeing how these came together in a lot of ways to produce this online but in public surveillance of social media.

And then, of course, there's another piece of social media that's somewhat less public that's about using undercover accounts to connect with people online. And we've also done work around how schools and school districts are using and collecting social media, how they're using third party social media monitoring tools to surveil students. And then so increasingly, how it is a really big source of information in the immigration and visa vetting space.

So as with many policies, that kind of collection use was initiated piloted and initiated, really, under the Obama administration, but was weaponized and force multiplied under the Trump administration, a lot of that coming out of the Muslim ban.

So in terms of-- as I say, this is a little bit of a different gloss. It's less about the kind of content moderation or content regulation aspect, although certainly there are intersections, and more about thinking about, OK, how do we think about governmental access to and use of social media.

And we can get into more detail on this. There's a lot to say. But just very briefly, there are a few strands that come into this. So one is the constitutional aspect, and whether there are Fourth or First Amendment arguments to be made about surveillance of social media. And we can get into that more.

And also, just generally, policy argument, and especially as the policy evolves and as the constitutional doctrine has evolved when we think about privacy protections in public. So probably most folks know even [INAUDIBLE] early in law school, this is an area where the Supreme Court has really shifted where it is and has started to think about what privacy in public looks like. And I think there are arguments that that applies in some ways, and doesn't necessarily apply, in some ways, to social media.

But in the meantime, there just seems to be really vast, widespread use of social media by police departments, and I can talk more about our research on that. So it's really kind of a burgeoning and growing area.

MAX LARSON: Great. Well, I think piggybacking off that before we open up into 230 more generally, I'd love to hear all three of your thoughts, but starting with you, Rachel, on what impact, if any, January 6 last year had on privacy. And are we seeing a chilling effect, the platforms that members of the far right and supremacist groups are willing to use. And what is the role that government versus private parties are having in restricting or not restricting privacy in the groups we saw involved in January 6 versus groups you studied after 9-11.

RACHEL LEVINSON-WALDMAN: Sure. That's a great question. Probably needless to say, the aftermath of January 6, in so many ways, has been a major topic of conversation within the liberty and national security program, and very much so these questions around use of social media.

So to give a little bit of landscape setting, both around the lead-up to January 6 and then what we've seen in the aftermath. So as people probably know, it's emerged that there had been a lot of planning online for January 6. It should not have come as a surprise to DHS, to FBI, to any number of law enforcement agencies.

And in fact, it doesn't seem that it did come as a surprise. It came out after the fact that was an FBI memo from the FBI field office in Norfolk, Virginia. There was certainly a ton of chatter online, including by people who had previously been involved in criminal activity. So this isn't just a matter of, well, people are talking, people are talking about protest.

Needless to say, I think there are a lot of issues. I would not endorse the idea of monitoring social media to find out about discussions about protests. But there were people who had been actively involved, including leading up to that. There had been a lot of activity, a lot of criminal activity at state capitals. And so for the people who have been involved in leading those, there was a lot of chatter among them about the lead-up to January 6.

Nevertheless, as we all know, there was really a woeful amount of under-preparedness going into that day. And so one of the things that came out of that is especially DHS, which has been very involved in social media monitoring, saying we want to kind of either launch a new initiative or at least expand social media monitoring work that we're doing. And this is in addition to the FBI talking about what sorts of authorities it has with respect to monitoring social media.

There was congressional testimony fairly soon after that in which an assistant FBI director suggested that the FBI is limited when it comes to monitoring publicly available social media. It's really not the case.

Under the FBI governing guidelines, there are actually very few limitations on use of social media, at least if you're talking about what's publicly available. It is certainly possible there are additional kind of practices or norms that are in place.

But there is a piece that, actually, an intern of ours and I published in Just Security earlier this year really kind of digging into what are actually the practical rules around the FBI'S access to social media. And the answer is they can do a lot on social media even before any kind of criminal investigation has started up. At DHS, what started to come out in reporting, and then actually in disclosures from the department itself, a lot of social media monitoring through an office of DHS that's called Intelligence and Analysis, or I&A. This social media monitoring initiative coming out of I&A is focused on narratives.

And so the DHS's sell behind this narrative focus is, we're not focused on individuals. We're not trying to do broad-based social media monitoring to identify specific people, although certainly down the line, that could be a part of it. If they actually identify overt criminal planning, information could be shared with the FBI or state or local law enforcement. Their [INAUDIBLE] is that they want to look for basically narratives that could lead to violence.

MEGAN GRAY: Rachel, when you say that are you talking about pattern spotting in the sense of just how much has the chatter increased? Are we seeing certain themes? Is that what you mean by narratives?

RACHEL LEVINSON-WALDMAN: So that's a good question. I think there is probably a lot more to learn about what exactly is meant by narratives. In conversations that we've had with DHS officials, which were not off the record, their description of the narrative monitoring has been-- an example would be, from their point of view, we are seeing not just an increase in volume, almost thinking about it as metadata, where you would watch the hills and valleys and be like, oh, there is a hill, something's going on.

But it's actually more content-based than that. So the idea would be like, we're seeing chatter about how a Jewish community or a Latino community in this city is really organizing around welcoming Afghan refugees. And this group of people over here, this group of white nationalists or white supremacists, is angry about that. And there's increased conversation about these particular efforts and this particular community.

So the way that it's being couched is really more about understand what the threats are, not necessarily to go after the people who are issuing them, although obviously that could come into play, but more to pursue protection for the communities that are potentially [INAUDIBLE].

So before we get on to the next thing, I think it's really important to add a gloss and a perspective on the civil liberties and civil rights gloss on this, which is that I'm certainly sympathetic to the [INAUDIBLE] in general, given where we are post-January 6 as well. And really, I think what seems like a rise in white [INAUDIBLE], both in general, and also, frankly, within law enforcement. One of my colleagues, Mike German, has done a lot of research and writing on this, on actually how embedded white nationalists are within some law enforcement departments or agencies.

I think that there are real questions that we have not-- I don't have an answer to about--

MEGAN GRAY: But on Max's question on whether or not privacy has changed following the January 6 events, I don't see any change. I'm not sure that's a good thing. I don't see more privacy. I don't see less privacy. I actually haven't seen, other than a bunch of teeth-gnashing, any differences, any actual changes in how we're approaching this, or from the people who are advocating for the overthrow of the

government, the Stop the Steal. I haven't seen them go underground, which would be the smart thing to do.

It's very hard to scale, which is why there was an initial foray trying to find other social networks, but that seems to have stopped, and they're all back on Facebook and such again. So I don't know. I haven't seen it. But I'm curious if folks have a different perspective.

DANIELLE CITRON: Rachel, I'm going to join you because I think the question is, who are we watching. And so Rachel, in your work throughout, and then our joint interest in fusion centers, the question is, who are we watching, not that we're watching.

And so whether there is an increased mass in the aggregate amount of watching, I think it's fairly clear-- and Rachel, tell me if you agree-- that we are watching and continue to overly watch communities of color, Muslim communities. That is, we haven't changed that. So fusion centers busy watching, arresting Black Lives Matters protesters-- you know that interesting Oregon case, Rachel, which I'm pretty sure the Brennan Center has some great posts about-- where we're overly watching First Amendment activities. The Privacy Act says you can't store that information but except, of course, for law enforcement purposes, which maybe just changes the whole dynamic. You can do it.

And so I don't know if you think there's-- I guess that's your question, Megan, which is are we doing more of it? Is it same? It's a whole lot of pervasive dragnet surveillance. But within the dragnet surveillance, we tend to, and have, with significant civil rights and civil liberty consequences, watching communities who are long been watched.

So I guess, can we ask that to you, Rachel? I don't want to cut you off, but I thought it would be interesting to--

RACHEL LEVINSON-WALDMAN: No, no, no.

DANIELLE CITRON: [INAUDIBLE] question, in a way.

RACHEL LEVINSON-WALDMAN: And I certainly don't want to monopolize the conversation at all. I mean, I think the question about how is privacy being impacted. I think part of the answer is we don't know. I have no idea how broad the scope is of, for instance, who DHS says it's watching.

The description of their [INAUDIBLE] is actually very broad. What they have said in conversations is actually, we're [INAUDIBLE] kind of narrowly in terms of the kinds of platforms or the kinds of sites we're looking at. We know there's no inspector general report yet. There is no internal-- there's no privacy office or civil liberties office report on this yet.

Certainly-- the one thing I was going to add is that our concern always is, and it's because this is borne out over and over again in history, to Danielle's point, is that regardless of the-- I guess for the monitoring, it absolutely will end up falling on activists and on communities of color. So today's [INAUDIBLE] for a long time is white supremacists. But authorities, both in terms of [INAUDIBLE] authorities and surveillance capabilities [INAUDIBLE] to target communities of color.

DANIELLE CITRON: So you're not monopolizing a thing, just to say, Rachel, we love this.

MAX LARSON: Great. I'm curious, then, to follow up on the 230 section, who are you looking at for the biggest harm? Is it private actors? Is it government at the intersection? Is it what's being done or is it what's not being done as the biggest threat to democracy and privacy today?

MEGAN GRAY: What a question

DANIELLE CITRON: I wish you were still at DuckDuckGo. Just saying, I'm glad you're advising companies, Megan. But you're our privacy protector in the private sphere.

MEGAN GRAY: Well, I didn't go to work for Google and Facebook. So--

DANIELLE CITRON: That's what I'm saying.

MEGAN GRAY: One of the few who did not. The question on 230, so 230 is for civil liability against private companies it doesn't have any impact on government actions.

DANIELLE CITRON: Just federal criminal, right? So it does impact--

MEGAN GRAY: I'm talking about liability against a police department. It just protects private companies. Now in terms of how 230 has or has not impacted democracy, there is a very good case that Danielle and others have made is that by virtue of having 230, this incentivizes companies to allow speech that gets people excited about Stop the Steal, which foments insurrection, which undermines confidence in the election. That is absolutely true. That's the nature of free speech. You can have conspiracy theories that get traction and adherence.

It also leads to viral amplification of things like the #MeToo movement and BLM that you wouldn't have had before when you had pre-internet, and it was primarily just pockets of activism that was very hard to spread throughout the United States when you had the printing presses controlled just by a few companies.

So the question for me is not whether or not there's problems on the internet. It's what are we going to do about it, and if there is a way to do something that doesn't entail throwing the baby out with the bathwater. And I think that is just a much harder thing to do because if you dislike Stop the Steal but you like #MeToo, in terms of regulation or enforcement and legislation, it is very hard to distinguish between them. And between the two, if I have to take the Stop the Steal crazies with the #MeToos, me personally, I think that is better for society. I think there is an argument that can be made on the opposite side. I just don't happen to hold that belief.

MAX LARSON: I want to do a quick follow up there. Do you see, either in the government or private parties, any distinguishing between those two? Do you think that they treat Stop the Steal different from #MeToo? Or are those it's all outside of 230? So do we see any difference?

MEGAN GRAY: So if you take, for example, Twitter, I think now you have seen some of these large companies decide on their own, without any government regulation or enforcement, that they are not going to be free speech bastions, that their corporate values are such that they're going to censor the Stop the Steal. They're going to kick off Donald Trump. And that's going to cost them some money and some market share. And that is a choice that they have made.

And then you'll see other companies who make opposite choices. And that's what you should see. You should have companies who have different ways that they want to operate their business. And it kind of comes back to an issue that we haven't talked about, which is competition law and antitrust enforcement and monopolization.

And I think it is very shortsighted to talk about privacy and online speech without bringing that into the conversation because that, ultimately, is one of the levers that can help solve some of these issues-- not solve, but ameliorate. If you had a privacy law, if you had greater number of platforms to choose from, all of that would help even out and stop this kind of runaway train of toxicity that we have right now.

MAX LARSON: Do you want to weigh in?

DANIELLE CITRON: Sure. You know I'm not shy. I feel like my students know what I think. No, but I think you're right that this conversation, if we're going to solve for any of it, we have to be talking about privacy legislation without question, that we can't-- certainly amending and changing section 230 in the way that

I'll describe is not going to solve for the woeful under-regulation of the collection, use, sharing, amplification, exploitation of our personal data. There's no question about that.

So every time I feel like I give a talk, I say, yeah, yeah, Section 230. We're talking about privacy legislation, right? And then staffers look at me like, no, that's too hard. And Section 230 can be hard. So I don't want to get rid of it. You said we don't want to throw the baby out with the bathwater. I think that's right. I don't want to get rid of Section 230.

But I'd like to condition the part of the statute that relates to the under filtering of content. So that's Section 230C1. So what I would do is keep the immunity, which only, of course, applies to the providers and users of interactive computer services, just to use the language of the statute.

Now so you have this immunity, this legal shield, so long as you're engaging in responsible content moderation practices, including amplification vis-a-vis clear instances of illegality, by what I mean is under the laws on the books that causes serious harm.

And so what that's going to do is say, look, you good Samaritans, you get it. Act like good Samaritans. And so one thing that I have been exploring, I've argued for this reasonableness to be addressed in the courts. So Ben Wittes and I-- I first wrote about this proposal in 2008, and it was not popular, I have to say.

So I presented it at the first Privacy Law Scholars Conference. And all of my friends, including one-- serious civil libertarians, also privacy friends-- said, you want to jail Communists. I'm not talking to you anymore. And I was like, huh? What do you mean, Michael Frumkin? What are you talking about? So he was very mad that we should ever touch Section 230.

So it is kind of a sacred-- we think of it, in a way, it's been valorized. And that's not to say--
MEGAN GRAY: It is very weird, I will say, this sacred cow of 230. I also think-- and this may come off as odd, but I also think that we didn't need to have 230. I think there was enough First Amendment precedent in case law that actually, that one case that motivated--

DANIELLE CITRON: And then the other, also stupid.

MEGAN GRAY: Probably would have gotten to the same outcome. So it is a little odd that we're putting so much emphasis on 230. And I'm not sure that we needed it. It did allow some space to for new companies to save on litigation costs. And that, again, gets back to the antitrust thing.

So any changes you're going to make to 230, it may solve the problem that we have with Facebook and their like, the companies like them. But I'm less worried about that. I'm much more worried about what the changes will do for emerging companies.

DANIELLE CITRON: But that's why reasonableness is such an effective tool. That is, what's reasonable for a platform with five billion users-- let's just take Facebook-- is different from what's reasonable of a startup. But you know what, that startup, let's say, hosts really destructive content, including child predators that they know about and have notice about.

MEGAN GRAY: I think the value of 230 is that you don't have to litigate. It's a motion to dismiss.

DANIELLE CITRON: You know what they call it? Too bad, so sad, friends. There's a whole lot of harm on the table that has been externally borne by pretty vulnerable people who have been silenced.

MEGAN GRAY: Understood. But the outcome is that the emerging companies, who don't have the resources to litigate whether something is reasonable or not, they're going to be unable to grow and compete. And they're going to have not very attractive business models and platforms. But the Facebooks of the world will.

DANIELLE CITRON: But wait. The startup that has the investment from big VCs, I'm not going to cry a river, I have to say, over the startup that's not well-funded because it's not a great business model. Does that make sense? I think we say startup as if they have no funding. It's just like two kids in a garage.

MEGAN GRAY: Yeah. But not all startups are--

DANIELLE CITRON: No, I'm not suggesting that they are all funded by the Kleiner Perkins of the world. But nonetheless, that is, you can do a whole lot of harm with just two people. And so I think that if you had a standard that required the internalization of some of these costs, and creating a reasonable approach to what is not protected speech, illegality, that shoves people offline, whose speech costs we don't account for, that you have to have some litigation costs. That's called business, literally business.

The idea that there's no litigation costs for companies is a frankly absurd notion as we sit here at the University of Virginia Law School. There is for most, if any industry, litigation costs because when you do harm-- not to valorize Holmes, but I don't mind-- when you do harm, you wreak havoc, you have to internalize those costs.

MEGAN GRAY: So what is the illegal speech that you're thinking of?

DANIELLE CITRON: Threats, cyber stalking, violations of intimate privacy, facilitating child predation, just to take some examples.

MEGAN GRAY: So the illegal speech is the underlying speech that you're worried about, not the hosting or facilitating.

DANIELLE CITRON: I'm worried about the enablers of--

MEGAN GRAY: But the enabling itself is not illegal.

DANIELLE CITRON: Well, it depends. It could be a tort, like the negligent enablement facilitation of crime. Klein, who loves that case. I'm sure I have a lot of takers in the audience. No? Landlord tenant negligent enablement of crime. People, come on, friends.

But there are torts. So you're right to point out that not all speech is liability-inducing. And so in some respects, some of this, oh my God, hair on fire, Section 230 freak out is on a presumption that everything is strict liability. That is, platforms will face strict liability. And that's totally wrong. Take the first year classes. There is no strict liability, so that it's also, I think, an overestimate estimation of the cost. So I take your point really well that a lot of what happens, though not everything, is plausibly related to some forms of speech, and speech, by what I mean legally protected speech. So it's true we're going to have error costs in a reasonableness standard. And I think the error costs, we have to take into consideration lots of speech we already lose under Section 230 that exists as it exists today.

RACHEL LEVINSON-WALDMAN: So if I can ask a question-- and I should be very frank that I am not a Section 230 expert literally in any way. We've certainly done a fair amount of work on content moderation, but in a lot of ways, we've steered clear of Section 230. So this is really just to ask a question, and I think this is to what both of you were just speaking about, that kind of dialing back on the Section 230 protections could then-- I guess-- let me rephrase.

Danielle, you were making the point that we're not in a neutral space. There's already speech that is being lost. So we can't say, well, we're in this fine neutral space where there are Section 230 protections, and thus all the speech that should be out there is out there, and it can battle itself out in the marketplace of ideas.

And I think that alone, talking about the concept of a marketplace of ideas and whether that still has any real force or salience now, I think that could probably take up the whole hour itself. But I guess I'm wondering how you do account for-- it's going to push the other way right.

So there are some kinds of speech, presumably, that would come back in, and then other kinds that would be pushed out. And in part, I assume, because platforms would become much more enthusiastic about their regulation. That seems like that's always been one of the concerns is that they would draw those far are too widely. And obviously they can draw boundaries wherever they want. I guess one of the beauties of Section 230 is that there's actually a lot of regulation they can do.

I guess I'm wondering how you would see that playing out, or if there are ways of those concerns are mitigated. Partly there's some horrible abusive speech that's lost, you know? No big loss. What about the other speech of value that ends up being dragged along with it?

MEGAN GRAY: Right. I mean, I think that's the nuances and the trade-offs that any of this has to address. And Danielle-- correct me if I'm mischaracterizing you-- believes that the value of the marginalized groups who have been silenced and who aren't able to exercise, really, the place that they should have in society and the speech that they should be vocalizing because of the harassment and bad behavior and illegal acts that they suffer from, that having those voices brought back into the public sphere is more valuable than the over correction that will inevitably happen for some of the speech that is currently there.

And I just make a different value choice. But I think both perspectives have value. I'm not sure that there is a right and wrong here. I just, from my perspective, I'm not sure that the voices that are currently missing from the debate, that they will be part of the debate. Even if you kick off all the Nazis off the internet, you're going to have poor communities that don't participate in public debates and aren't on Twitter and Facebook for a whole host of reasons that have a lot more than just the fact that it's maybe a toxic environment for them. There's a lot of reasons why they're not participating in that.

And so because I'm not convinced that this is necessarily going to be the outcome, but I do feel pretty confident that there will, in fact, be people kicked off the internet that we don't want kicked off as a result of over and misplaced good Samaritan-type systems. That's how I weigh it.

DANIELLE CITRON: Just to intervene just a little bit here, when you say the costs are only speech-related, you're not sure if we're going to see marginalized people take advantage of that, that's not all that it is. If only. Under assault online, you lose your work opportunities. That is, one cannot work with Google CV that's full of defamation, impersonations that suggest you're a prostitute, nude photos. You just can't get a job.

So what I refer to it as, we at CCRI describe ourselves as, we are advocating for both civil rights and civil liberties online. That is, all of life's key opportunities are contingent on these technologies that are with us wherever we go. And so there are meaningful costs that, as an empirical matter, at least we have some information about the-- we do, at least as the cyber stalking and invasions of intimate privacy, we do have a sense of the economic, emotional, psychic, community costs.

But the broader question, empirical one, about what would this ecosystem look like if we conditioned liability, that if we had liability, if you weren't engaging in reasonable content moderation practices-- and I suppose that we'll have to wrestle with should that ever happen.

And one thing that I think is worth considering is having-- I've been convinced by Blumenthal's office that maybe the courts aren't the right actor, that if we gave the FTC enough funding, that if-- which I love the idea, and this big package that we might give the FTC a whole lot of funding--

MEGAN GRAY: It'll never happen.

DANIELLE CITRON: Oh, please. Can't we just pretend for five minutes? That we might see an expert agency set forth evolving-- not stuck in the mud-- reasonable practices in the face of clear illegality that allows for flexibility and nimbleness and change.

And what's interesting, Rachel, you're saying it does worry me, also, when you hear someone like Zuckerberg say he's welcoming Section 230 change, which honestly is nonsense, because his whole business model are likes, clicks, and shares. He didn't shut down FaceTime Live when people were getting murdered on FaceTime Live. Why? And internally, it's clear. It was making money. There were millions of people watching the death videos.

So the idea that he really wants 230 reform is truly a talking point by my lights. So I do wonder. But I do think we have to, as we think about reform, do be really careful, as Megan, you've urged us to, is to think about the difference and the shoulders on which it falls, and how there's a big difference between-- and I didn't mean to disparage startups. Forgive me, anyone who's interested in representing startups, all very honorable things to do.

But there is a difference, of course, between, the behemoths. They big. I'm not going to cry a river for Facebook for 5 five seconds, or Twitter, or any of these companies, the big ones. They are monetizing our eyeballs. They make money off of selling everything we do and think and see and engage with online.

MEGAN GRAY: That's almost the entire internet, though. They've just been much more successful at it.

DANIELLE CITRON: Well, because they're advertising-- like Twitter, its advertising part of its arm is a huge moneymaker. Same with Facebook. Facebook knows what you're doing on your period tracking app even if you have never, ever, ever had a Facebook profile. Why? Because they're an advertising company.

MEGAN GRAY: Right, but I mean, you see this all over. Etsy. You see it with Yelp. You see it with Pinterest. It's very hard to try to-- at least I haven't been able to come up with [INAUDIBLE].

DANIELLE CITRON: So are you giving into the model of advertising?

MEGAN GRAY: No, no, not at all.

DANIELLE CITRON: I had a feeling no, because DuckDuckGo.

MEGAN GRAY: DuckDuckGo knows nothing about you. So I prefer a privacy law that bans surveillance advertising. But it's hard. And I'm not very confident it will happen. But the larger issue is, OK, practical. If we're not going to have a privacy law, and if we're not going to change the First Amendment, what do you do?

And I would love to do something with Facebook and Twitter and Google but I don't want to hurt the kind of lower tier companies that are the only possibility that some of these big tech problematic companies are going to face in the next 10 years. So that's where I always get stopped.

And I do actually believe that Facebook would like a Section 230 reform. I actually do. I think they have the resources. I think they see it as an opportunity to stall, at least, the growth of any burgeoning companies. And for them to kiss ass on the hill, and they can perfectly-- not perfectly-- they can easily implement a reasonable content moderation program.

And if that's what it takes to get Congress off their back with antitrust cases, that is a good trait for them. So be careful what you wish for, I guess, is where I come out.

MAX LARSON: I do want to stop us. There's a great poking the bear pause point. I want to open it up to the room for questions.

MAX LARSON: Thank you. I think, unfortunately, we are over, so we have to conclude here. But thank you again to each of our panelists. This was wonderful.

DANIELLE CITRON: Thank you so much. I'm going to miss this.

[APPLAUSE]

MEGAN GRAY: I'll be here for a while if anybody has questions.

MAX LARSON: Thank you.