

University of Pennsylvania Carey Law School

## Penn Carey Law: Legal Scholarship Repository

---

Penn Program on Regulation Podcasts

Penn Program on Regulation

---

6-22-2022

### Race and Regulation Podcast Episode 5 - Racial Equity and Data Privacy

Anita L. Allen

University of Pennsylvania Carey Law School, [aallen@law.upenn.edu](mailto:aallen@law.upenn.edu)

Follow this and additional works at: <https://scholarship.law.upenn.edu/ppr-podcasts>



Part of the [Administrative Law Commons](#), [Internet Law Commons](#), [Law and Race Commons](#), and the [Privacy Law Commons](#)

---

#### Recommended Citation

Allen, Anita L., "Race and Regulation Podcast Episode 5 - Racial Equity and Data Privacy" (2022). *Penn Program on Regulation Podcasts*. 7.

<https://scholarship.law.upenn.edu/ppr-podcasts/7>

This Article is brought to you for free and open access by the Penn Program on Regulation at Penn Carey Law: Legal Scholarship Repository. It has been accepted for inclusion in Penn Program on Regulation Podcasts by an authorized administrator of Penn Carey Law: Legal Scholarship Repository. For more information, please contact [PennlawIR@law.upenn.edu](mailto:PennlawIR@law.upenn.edu).

## Podcast Transcript:

### Race and Regulation Podcast

Presented by the Penn Program on Regulation

Episode 5: Racial Equity and Data Privacy with Anita L. Allen

Released on June 22, 2022

*Music: Joy Ike's "The Fall Song"*

**Anita Allen:** For want of racially diverse lenses, the story of Black Americans' privacy has been under-narrated. Black people don't think about privacy the same way white people do in every instance. And we're seeing it not just in theory or in sociology, but we're seeing it in practice.

**Cary Coglianese:** That's law professor Anita Allen, delivering a lecture at the University of Pennsylvania organized by the Penn Program on Regulation. I'm Cary Coglianese, the director of the Penn Program on Regulation and a professor at the University of Pennsylvania. Welcome to our podcast, "Race and Regulation." In this series, we are talking about the most fundamental responsibility of every society: ensuring equal justice, and dignity and respect, to all people. Advancing racial justice calls for all of us to understand better the racial dimensions of regulatory systems and institutions. We're glad you can join us as we hear from Professor Allen, a professor of law at the University of Pennsylvania. She is one of the nation's leading scholars of privacy law. Her lecture was cosponsored by the law school's Center for Technology, Innovation & Competition. Many of today's privacy issues stem from innovations in digital technologies and the way so much communication and commerce take place via the internet. Professor Allen begins by acknowledging the omnipresence of the Big Tech firms.

**AA:** Online platforms—Facebook, Twitter, Google, Airbnb, Uber, Amazon, Apple, TikTok, Microsoft—have created attractive opportunities and efficiencies. We know that. Yet, these platforms come at a heavy price. Familiar platforms collect, use, analyze, and share massive amounts of personal data. They are motivated by profit with very little accountability and transparency. The social cost of information privacy diminution includes discrimination, misinformation, and political manipulation. The self-governance efforts of big tech companies have not silenced the criticism that platform firms prioritize free speech, interconnectivity, and

interoperability at the expense of equitable privacy protections and anti-racist measures. New rules, statutes, and authorities are needed, in my opinion.

**CC:** To understand what rules are needed to rectify racial inequities in today's digital society, Professor Allen explains that the first step is to identify the nature of the problem—a step that Professor Allen takes in a recent research project that resulted in an article published online by the *Yale Law Journal*. The core question: How are Black Americans distinctly affected by digital platforms and other information technologies?

**AA:** Well, until I undertook this project, I didn't have a clue, and I don't think anybody really understood well how we could succinctly say exactly what the vulnerabilities of African American people are. But today, I am prepared to offer a novel privacy and data protection framework for encapsulating the online vulnerabilities of African Americans. Let's dispense right away with the notion that Black people don't care about privacy. Black Americans often can't afford the technology that comes with the most data protection built-in. In addition to that, like everybody else, Black people are challenged by the terms of service and privacy policies that are lengthy, technical, and complex. Even us educated people have trouble dealing with exactly what their rights are and what their responsibilities might be when it comes to data protection on online platforms.

How much do African Americans even use the internet? How much are they on platforms? Answer: a lot. African Americans are active users of online platforms. Black Americans turn to the internet for all kinds of things. Communication. Housing. Education. Business. Employment. Loans. Government services. Health services. And recreation. And although a whopping thirty percent of Black households do not have a high-speed internet, and a significant percentage of Black homes don't have a personal computer, Black Americans are well represented among the four hundred million users of Twitter and the billions of daily users of Meta, now, formerly Facebook. African Americans accounted for nearly one-tenth—I was amazed by this—one-tenth of all the Amazon retail spending in the U.S. in 2020. African Americans who are active online, could greatly benefit from well-designed and, I would say, race-conscious efforts to shape a more equitable digital public through improved laws and legislation. A new generation of privacy laws would ideally include provisions specifically geared toward combatting privacy and data protection-related racial inequalities enabled by online platforms. American lawmakers should focus on the experiences of marginalized populations no less than other populations, than privileged populations.

**CC:** Professor Allen organizes the racial justice problems that this new generation of privacy laws should address into three categories. Together, these three form a system of privacy-related

oppression that she groups under the rubric of the *Black Opticon*. The first of these three comprises discriminatory forms of surveillance, or what Professor Allen calls a panopticon problem, using a term from 18<sup>th</sup> Century philosopher Jeremy Bentham. She illustrates the digital panopticon problem facing Black Americans by recounting a controversy over a private firm, Geofeedia, sharing individuals' location data with law enforcement officials.

**AA:** A long time before there was ever critical race theory, legal sociologist Alan Westin, in his 1964 mega-influential treatise, *Privacy and Freedom*, noted the special susceptibility of African Americans to the panoptic threat. It's so interesting that at the beginning of privacy scholarship, the special vulnerability of African Americans was recognized. Westin specifically mentioned African Americans' concerns over covert physical surveillance and discrimination by segregationists with then what he called a "white power structure."

In 2016, the ACLU reported that police departments were using software purchased from Geofeedia, following the Black Lives protests in Baltimore that were sparked by the death of African American Freddie Gray while in police custody. Baltimore police reportedly used Geofeedia software to track down and arrest peaceful protesters with outstanding warrants. The police deliberately focused arrest intimidation with a majority Black community, such as Sandtown-Winchester, the precinct where Freddie Gray was apprehended and killed.

The software that Geofeedia and the police used relied upon social media posts and facial recognition technology to identify protesters. How did they get the data? Well, they got it from Twitter, they got it from Facebook, they got it from Instagram, and nine other social media companies.

When there was public outcry, Twitter, Facebook, and Instagram backed off and discontinued, but Geofeedia continued to market its services at a time when the FBI was a client of theirs, and the FBI reported an interest in so-called "Black identity extremists" as a movement. And they felt it was important to be able to target and identify members of this movement. But the way they defined that Black extremist was so broad that a person just out on a Sunday stroll as part of a protest might be deemed a Black identity extremist. It was a problem. Alright, that's one example of how African Americans are under the attentive eye of the Black Opticon.

**CC:** The Black Opticon involves more than just the attentive eye of a governmental panopticon. The Black Opticon problem also includes, as its second facet, the exclusion of

Black people—or what Professor Allen refers to as the “ban-opticon,” a term coined by French theorist Didi Bigot.

**AA:** This one involves discriminatory exclusion that obtains information from Black people to disadvantage them, to exclude them from something that white people and other races might have access to. For a time, Facebook allowed advertisers to choose, by race, which Facebook users could and could not see their advertisements. Now Facebook claimed, at one point, to have fixed the problem, devising a system that would recognize and not post discriminatory housing advertisements. And yet, in 2017, journalists at ProPublica were able to purchase housing advertisements that were designed as a test to exclude African Americans and people needing wheelchairs, in violation of the Fair Housing Act. The authorities caught on, and two years later, the U.S. Department of Housing and Urban Development actually charged Facebook with violating the Fair Housing Act and Facebook faced considerable damages. Well, Facebook now firmly and strongly, by its policies, prohibits discrimination based on race, at least officially.

**CC:** Finally, Professor Allen explains that the third facet of online racial inequity—that is, the Black Opticon—involves the predation of Black Americans, or their vulnerabilities to online scams and frauds. This she calls the “con-opticon.”

**AA:** This involves using personal data to target people of color for the purposes of including them, but including them in opportunities that are exploitative or scams or con jobs, where they would prefer not to be included, actually. This is predation. Selling and marketing products that don’t work. Extending payday loans with exploitative terms. Selling products like magazines that are never delivered. They do this especially to folks in prison. And also, very illusory money-making schemes that are targeted to populations, not just Black people, by the way, also Hispanics are targets of this. These are deliberate efforts to take advantage of the special vulnerabilities of people of color and marginalized people.

Recent litigation focused on a company called MyLife.com. MyLife.com is an online enterprise that sells profiles of individuals marketed for purposes that would include things like housing, credit, employment screening, decisions about those kinds of things. So, screening services. These services are particularly important to people of color who have limited income, weak credit, maybe criminal justice backgrounds and histories that are barriers to obtaining necessities, so they are tempted to use the services of such companies in order to find out where they stand in the world.

One thing the company was doing was to target Black people with the perception that there was criminal information about them that was available to other people, and Black people should sign up for additional services in order to be able to monitor and track exactly what this criminal history was when, in fact, there was no criminal history or there was history of a parking ticket or something of that nature. The Fair Credit Reporting Act does address problems like this. And in a very important lawsuit brought by the FTC and the Department of Justice, alleging that MyLife.com violated the Fair Credit Reporting Act, the company was, in fact, found responsible for failing to maintain reasonable procedures to verify, for example, how its reports were used, to ensure the information is accurate, and to make sure information, if it was sold, it would be used by third parties only for legitimate purposes. The suit resulted in an injunction and a very large twenty-one-million-dollar civil penalty for MyLife.com.

*Music: Joy Ike's "Wearing Love"*

**CC:** Privacy's racial problem, then, has three elements. The Black Opticon comprises state surveillance—the panopticon. It comprises exclusionary practices, or the ban-opticon. And it comprises targeted predation, or the con-opticon. How then can we solve this multifaceted problem?

**AA:** Calls for improved platform governance flow from many sources. Self-regulation by big tech itself just isn't enough. The advocacy group, Color of Change, credits itself with persuading Google to ban predatory lending apps from Google Play, to protect Black people from unreasonable terms, high default rates, and manipulation. And also Color of Change was able to get Pinterest to stop featuring plantation weddings and party venues that implicitly glorify the heinous slave economy. Well, these kinds of successful interventions are lovely, but there are few and far of them and I think a lot of this kind of stuff goes below the radar screen of the more national advocacy groups.

Changes in the design and enforcement of privacy law could potentially help combat the Black Opticon. Legislative reform is certainly in the mix of the proposed solutions, along with data trust, content moderation, social media councils, and other such approaches. Regimes of law, like antitrust law, intellectual property law, constitutional law, civil rights law, human rights law – they all bear on platform governance. Privacy and data protection law, legal measures, are also important as requirements of adequate platform governance.

The measures that I think are needed would have to be race-conscious. In addition to considering agendas that concern the general population, which are appropriate and foster strategic coalitions among different groups, policymakers should also welcome and rely upon group-specific, anti-racist agendas for guidance. They should articulate race-based rationales for reform measures intended to protect group data privacy.

This dual approach that I advocate, I call it policymaking for all and policymaking for some—it helps to ensure that the interests of marginalized racial minorities are not overlooked and aids in surfacing possible conflicts between the interests of one racialized group and other groups. For example, targeting Black men for high tech modes of data surveillance based on race may address concerns of the majority about freedom from crime but violate Black men's entitlement to freedom and privacy from racist social control.

**CC:** Professor Allen calls for public policies focusing on each of the three components that make up the Black Opticon: to reduce discrimination over surveillance, to reduce forms of exclusion, and to reduce discriminatory practices of fraud and predation. She illustrates the possibilities for legal change with three concrete examples. She first describes a new law adopted at the state level: the Virginia Consumer Data Protection Act of 2021.

**AA:** First of all, it's important to know that Virginia is not alone in enacting a privacy statute. Colorado and California also enacted statutes—California, a couple of years ago, Colorado this past summer. But the Virginia statute is particularly interesting and important from the point of view of the Black Opticon. And why is that? It's because Virginia is the only state of the three that was a part of the Confederacy, and because twenty-one percent of Virginians are African American. And because about sixteen percent of Virginians live in poverty and are vulnerable to financial exploitation and abuses. And because fifteen percent of Virginia Black adults did not graduate from high school. And only twenty-one percent of Black Virginians hold a college degree, which is the lowest percentage for any racial minority group or ethnic group that is reported in the state. So, discriminatory credit, employment, educational, and financial decisions are likely commonplace experiences for African Americans in Virginia, as they are for elsewhere in the nation.

Another feature about Virginia's statute that makes it kind of interesting is that the main sponsor, or they call them the "chief patron;" the chief patron of the statute was a man named Cliff Hayes, an African American, who was also a former public sector information technology professional and a member of the Virginia House of Delegates. He sponsored the legislation. His co-sponsor was a white man named David Marsden in the Virginia Senate. But in the House of Delegates, there were several co-sponsors of the bill; they were called "chief co-patrons," and these co-

patrons included three who were people of color—one African American, one South Asian American, and one mixed-race woman.

What is this statute that was born in a state that belonged to the Confederacy that was put forward by African Americans? What does it say? How does it do when measured against the equity agenda that I am proposing?

Here is what the statute is like. It's not a civil rights law by any means, but it is a statute that tries to enact fair information practices that are applicable to businesses of all sorts in Virginia, on behalf of Virginia consumers. Big tech firms like Microsoft and Amazon fully endorsed the statute, which ought to give us pause. Why would Microsoft and Amazon like this statute? The privacy group, Future of Privacy Forum on whose board I am now—I joined a couple of weeks ago—this organization supported the bill as a significant milestone. The Future of Privacy Forum is supported, in part, by Facebook, Google, and Twitter.

But many critics have described the Virginia law as weak and even empty. So, the policy features of the law are that it does prohibit the processing of personal data in violation of state and federal antidiscrimination laws. That's a good thing. It also prohibits providing goods and services on a discriminatory basis when it comes to prices and services, which is another good thing. But there are a number of concerning features about the Virginia statute. There are numerous exemptions. Many types of organizations are not covered by the statute. That includes state and local government, non-profits, schools, and any kind of data that might be covered by a federal statute, like HIPAA.

It exempts, for example, government entities, so it doesn't address the threat of law enforcement or public agency surveillance, monitoring, tracking, profile identification. Photographs and data based on photographs commonly used for facial recognition analytics are excluded from the definition of biometrics in this statute. While the use of photographic data has a place in law enforcement, machine and human errors in the use of such data disproportionately impact African Americans.

Also, that statute allows targeting advertising. You have to opt-out if you don't want that. Well, we know about opt-out complications. It's very difficult for consumers to opt-out, especially when they are not aided by the companies to opt-out by being informed as to what the reasons for opting out might be and how the process for opt-out works. Consumers can be charged a higher price if they opt-out of targeted ads profiling in the sale of their data.



**CC:** Of course, these features of the law, allowing consumers to opt-out of the sharing of their data, apply to everyone. A separate question, though, arises about race, specifically about whether companies and other institutions can use data sets that include demographic information on a person's race. Professor Allen tells us that the Virginia law specifically addresses this use of data on an individual's race.

**AA:** Another feature is that race is presumptively sensitive under the statute. Now, you're like, and that's a good thing, isn't it? If race is treated as special or sensitive information when it comes to data processing? I have mixed feelings about this. On the one hand, we don't want race to be used in a way that encourages or enables discrimination. On the other hand, we're not Europe, and we have never as a country had the European approach that treated race along with trade union membership as sensitive data. And I am afraid, and many people are saying that they are afraid as well, that these statutes might end up, like Virginia's, might end up making it difficult to do affirmative action to benefit minority groups who need the kind of attention that affirmative action confers in education, employment, and in health services. On the other hand, the statute does exempt educational institutions from the coverage of the statute. So maybe we don't have to worry about that problem quite as much. People can opt-out of that protection if they want to, which is also a little bit strange because if it's such a sensitive matter, why do you let people opt-out of it? If it's important, why do you get to opt out of it?

Finally, a lot of people think that it's a big problem with the statute that it doesn't provide for a private right of action. If you feel you have been harmed and you want to sue, you have to rely upon the attorney general. The Trial Lawyers Association of Virginia didn't like this part of the statute. Of course, they do have a self-interest here because they would like to be able to make money by bringing lawsuits. But they make a good point about the fact that in a state that has a history of being a part of the Confederacy, for example, and where racism still pervades in many sectors, it may be a problem that Black people are left to the political whims of the day in terms of whether or not the attorney general will take up their causes and pursue their cases. So, it might be better to have a private cause of action. This statute, which is a landmark, it isn't clearly giving us what we needed. It's promising, but in certain ways, disappointing.

**Music:** *Joy Ike's "Wearing Love"*

**CC:** If a state law like Virginia's is not fully satisfying, are there other options? Professor Allen turns to two policy developments at the federal level, the first of these is taking place at the Federal Trade Commission, or FTC.

**AA:** The FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States. The FTC does not have a great track record of pursuing enforcement actions against platforms whose unfair or deceptive business practices target consumers belonging to marginalized communities, like African Americans. They have gone after, though, Twitter, Google, Facebook, Snapchat, Ashley Madison—they have done all that. But I think that there is the potential for the FTC to really focus on people of color. They could and they may, because of a confluence of three things. One, continued diverse leadership. Two, dedicated funding for a privacy bureau. And three, they have got a commitment already to addressing the problems of communities of color as a strategic priority.

In terms of diverse leadership, President Biden appointed a man of color, Alvaro Bedoya, Commissioner of the FTC. He was the founding director of the Center on Privacy & Technology at Georgetown University, and a former chief counsel of the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law. He is an immigrant from Peru and a naturalized U.S. citizen. I believe that Mr. Bedoya has a demonstrated understanding of the problems of racial minority targeting surveillance, privacy concerns, setting priorities, and enforcing privacy laws.

The second thing is that there's this great, new possible source of funding. Last September, the U.S. House Committee on Energy and Commerce voted to appropriate one billion dollars to create and operate a bureau to accomplish the work of the commission related to unfair and deceptive practices related to privacy, data security, identity theft, data abuses, and related matters. This bureau's mandate to address data abuses might well signal that they are going to be able to handle the kind of abuses that are experienced by African Americans. Hopefully, in line with my recommended online equity agenda, the FTC would, with this new funding, be able to be even more aggressive when it comes to people of color issues.

The FTC does already have a race-conscious antidiscrimination agenda that could be pivoted to more focus on online equity for African Americans and other people of color. They released a report in 2016 called "Combating Fraud in African Americans and Latino Communities." The FTC's comprehensive strategic plan, which reported on the outcomes of strategies to reduce fraud in Black and Latino communities. And very recently, in 2021, they issued another report called "Serving Communities of Color," which described the Commission's strides in addressing fraud in Black and Latino communities and expanded efforts to include other communities of color such as Asian Americans and Native American communities, and other non-fraud related consumer issues that also disproportionately affect communities of color.

So, promising things at the FTC. What we don't know, though, is whether the jurisdictional limitations of the FTC will make them be able to really address the civil rights concerns that are at the bottom of the Black Opticon. And also, whether future agency enforcement priorities will be the same as, I think, current ones seem to be. The future is somewhat uncertain and, of course, politics, politics, politics.

**CC:** Finally, Professor Allen turns to the prospect of addressing the problem of the Black Opticon through congressional action, specifically the proposed Federal Data Protection Act of 2021.

**AA:** This exciting bill, introduced by Senator Kirsten Gillibrand, Democrat, of New York, this bill would create a federal data protection agency with three branches—a civil rights branch, a research branch, and a communications branch. The Office of Civil Rights would ensure that collection processing and sharing of personal data is fair, equitable, and non-discriminatory in treatment and effect. Bravo! Right on! Does it mention Black people? It could help Black people.

The office would also aim at developing, establishing, and promoting data processing practices that affirmatively further equal opportunity and expand access to housing, employment, credit, insurance, education, health care, and other aspects of interstate commerce. And then, finally, the office would coordinate the agency's civil rights efforts with other federal agencies and state regulators.

This would be a phenomenal sea change in the way we think about and pursue privacy data protection in the United States. To have one of the main units of a federal agency focused on civil rights would be quite amazing. And we hope they would focus on race-specific and group-specific civil rights problems. I think by naming the problems, the Black Opticon, the equivalent in the Hispanic community, Native American community, et cetera, we would begin to enable more targeted remedies and approaches to addressing the problems that we are all facing.

The research division would also, I think, further civil rights goals because they would be charged with helping to identify and measure disparate impacts and privacy harm. We want to make sure that those neutral-seeming laws are, in fact, not having a non-neutral impact.

The complaint communication division would have its ear to the ground and hopefully, those grassroots concerns of African Americans could be heard at the highest levels of the federal government.

Those are the good things and the positive things. The not-so-positive things, of course, are that passage of this bill is very unlikely. There are probably a dozen privacy bills pending in Congress right now, and this is the only one that has a privacy agency at its core. Most of them are simply privacy bill of rights, fair information practice type bills on the national level. But I think it is going to be very unlikely to pass. Now, it does, I think, have value as a model for what the law could aspire to. And even if the agency did get created, its efficacy would be uncertain because we don't know how—whether the bureaus and the units that are created to do all this good work would actually be able to do them in the long run, requiring the right expertise, the political will, et cetera.

I think the future of any kind of privacy law in the United States has a big question mark on it. We've waited so long!

*Music: Joy Ike's "Wearing Love"*

**CC:** To move forward, the first step is to recognize the Black Opticon problem, and then to build considerations of race into privacy law and policy, argues Professor Allen. Precisely because policy change will not come easily, it requires that advocates and policymakers clearly specify the goals for regulatory change.

**AA:** There are some promising possibilities here, but the path forward is challenging. And it will require, I think, that we have race-conscious state and federal regulation in the interest of non-discrimination, anti-racism, anti-subordination.

To be vague about what we're trying to do in the name of non-discrimination, I think it's not going to work. We have to really focus on what the problems are. The Black Opticon is one framework for really focusing our attention on what the problems are for one of America's most marginalized minority groups.

Toward escaping the Black Opticon prison, a pernicious, biased, and watchful inattentiveness, African Americans and their allies are continuing the pursuit of viable strategies for justice, fairness, and equity in the digital economy. The conversation is ongoing, and we are going to make some progress.

**CC:** In moving forward, tradeoffs will have to be made, just like in any area of the law. The key, Professor Allen says, is to make sure that in making these tradeoffs, policymakers do not further overlook or discount those groups that have already been marginalized.

**AA:** My concern is that in our society, too often, finding the middle ground is not really finding the middle ground. Finding middle ground is finding a compromise that satisfies some people but may still not satisfy the needs and interests of all people equally. Or that may marginalize some people in trying to seek that compromise or that “balance.” I think it’s very common for African Americans to be on the short stick of the compromises and the balances that our society comes to in trying to reconcile competing goals. All of this thinking is actually not necessarily going to ever get to the heart of the matter for African Americans, which is to really undo the trauma of slavery and racially enforced segregation.

**CC:** Policymakers and the public need to think more inclusively. Professor Allen points the way forward, in the end, by returning to the panopticon problem. She says that the challenge is not merely one of less surveillance but of more racially attuned decision-making about surveillance. Decision-making that takes all perspectives and all interests into account.

**AA:** Surveillance, per se, is not necessarily either good or bad. It’s what the surveillance is doing and how much surveillance needs to be done depends upon the context. That’s my view. I would never advocate an end to all surveillance. That would be stupid. But we have to find forms of surveillance that actually are respectful of the legitimate claims and interests of our polity in an inclusive way.

For example, putting up cameras in housing projects where people of color live is a kind of surveillance that sometimes—oh, it has a very beneficial goal. It makes the neighborhood safer; it gives people and allows police to investigate and solve crimes. And it deters wrongdoing. All those things are sort of true. It doesn’t mean that the privacy interest people have who live in housing projects will allow the degree of surveillance that may have good purposes. The thing is, what do you think privacy is? Is it a fundamental right that acts as a trump against utilitarian

purposes sometimes? Or is it always just another factor to be weighed and balanced in the weighing and balancing?

I think it's important to connect the concerns about minorities and people of color with concerns about what is the nature of privacy. Is it something that is just always subject to balancing? Or is it something that is sometimes a trump to—even if we could achieve good public purposes or good private purposes, we sacrifice—we don't do those things because doing it would adversely impact people's privacy to the extent we just cannot tolerate as a free society.

I just want to say that I try to avoid locking myself into these perpetual battles between surveillance or non-surveillance, or free speech or privacy because I think that we have to negotiate this terrain, but we have to negotiate it in a way that it doesn't always put people of color on the bottom. We have to figure out a way to do that. And we're trying to center, to a great extent, the concerns of the marginalized groups and to take their interests and needs, as they understand them, as we understand them, fully into account and then see what kind of a society we end up with, what kind of schools we end up with, what kind of online platforms we end up with when we have really truly taken everyone's interests to heart and taken as much into account.

*Music: Joy Ike's "Walk"*

**CC:** Thank you for listening to this episode of "Race and Regulation." We hope you have learned more about the racial dimensions of privacy law in the United States.

This podcast has been adapted from a lecture delivered by Professor Anita Allen in February 2022. She spoke as part of the Penn Program on Regulation's lecture series on race and regulation, co-sponsored by the Office on Equity and Inclusion at the University of Pennsylvania Carey Law School.

Her lecture was also cosponsored by the law school's Center for Technology, Innovation, and Competition. The Center's director, Professor Christopher Yoo, moderated the lecture. Professor Ezekiel Dixon-Román, of Penn's School of Social Policy and Practice, offered exceptionally illuminating commentary following Professor Allen's lecture, which you can hear and watch in the unabridged version at our YouTube channel.

I'm Cary Coglianese, the director of the Penn Program on Regulation. For more about our program and free public events, please visit us at [pennreg.org](http://pennreg.org). You can also find other episodes in our Race and Regulation series wherever you get your podcasts.

This podcast was produced by Patty McMahon, with help from Andy Coopersmith, our program's managing director. Our music is by Philadelphia-based artist, Joy Ike.