Brown ADVISORY
Thoughtful Investing.

NOW Podcast

EPISODE 8 TRANSCRIPT

Citizens of Cyberspace: Who is in Charge?

Host: Lauren Cahalan

Guest: Dr. David Edelman

00:00:01 **Ken Stuzin:** Hello. This is Ken Stuzin. I'm a partner at Brown Advisory. Welcome to our NOW 2020 Podcast. NOW stands for Navigating Our World. We are simply trying to understand the world better, to navigate some of the most pressing questions that are shaping our lives, our culture and our investment challenges. We are committed to sharing the views of CEOs and other leaders so that we can all learn from their perspectives on how to navigate the future. We would like to hear from you as well. We invite you to leave a review or take a moment to complete the short questionnaire on the NOW website so that we can learn from your thoughts, questions and feedback.

As we look to the future, whether we agree or disagree with each other, the one thing we know for sure is that none of us can figure this out on our own. At Brown Advisory, we are focused on raising the future, and we hope these NOW conversations will help us do just that.

00:01:11 **Lauren Cahalan:** We're living in a moment of great disruption. Our home lives, our work, our travel are unrecognizable compared to what we knew a few short months ago. And while we have always been dependent on technology and platforms, it has reached a new level during the pandemic -- Microsoft Teams connecting businesses, Apple connecting family through FaceTime, Google connecting us to updates in our communities, Facebook connecting friends through social media and Amazon connecting us to essential goods. We are more dependent on technology than ever before.

We also live in a world where these five companies have a combined market cap of $5.5 trillion, making up over 20% of the S&P 500. It is nearly unheard of to spend a day and not interact with at least one of these companies. Big tech is in a position where they are serving as gatekeepers of how we communicate, access essential goods and provide critical infrastructure for our data. This begs the questions: What role do platforms and social media companies play as arbiters of speech? How do we think about companies when they have more data than any government could ever obtain? What happens when companies fill foreign policy roles on the geopolitical stage that we never imagined? What happens when the market cap of a company is greater than the resources of a country?

Technology is no longer a siloed issue of debate. It is ingrained in every sector in the ways we communicate, connect, consume and collaborate. More than ever, the risks we are navigating are sight unseen, information moving across the internet and a pandemic traversing the globe, which leads us to some really difficult questions as a society. From data privacy to misinformation, these were difficult topics before current events, and they are even more challenging looking into the future.

I'm Lauren Cahalan. I'm an equity analyst at Brown Advisory, and I want you to meet David Edelman. David is an academic and policymaker who currently directs the Project on Technology, the Economy, and National Security at MIT. I heard him speak at a conference last year, and I was captivated. So it is my great pleasure to welcome him to the podcast today.

So, David, I think a good place to start is around the topic of data privacy. This is something that all of us can relate to. Can you explain to us where we were in this conversation pre-coronavirus and then how that has changed?

00:03:40 **Dr. David Edelman:** Well, the issue of data privacy is much more complex, I think, than most are really willing to give credence to. And the reality is that there's this ongoing contradiction -- there was before COVID and there still is -- of how at least we here in the United States tend to, as far as we can tell in the polls, feel about privacy. You take a look at the polling, and you see things like nine out of 10 Americans feel like they've "lost control" over their data. That's a lot of number. You can't get nine out of 10 Americans to agree on almost anything, and yet nine out of 10 feel like they've lost control of their data, and you can't blame them, right? I mean, statistically speaking, almost everyone listening to this podcast had their data breached in the last three years, whether it was in Target or Equifax.

00:04:21 **Media Clip 1:** Now, to the inside story of that massive Target data breach that touched as many as one in three American consumers.

00:04:28 **Media Clip 2:** Meanwhile, Hershey says a data breach may have compromised the financial information of visitors to its amusement park, hotels and other venues.

00:04:36 **Media Clip 3:** Another day, another data breach. This one is huge, involving one of America's giant bank combines, JPMorgan Chase.

00:04:45 **Dr. David Edelman:** At the same time, though, you see consumer behavior act in a somewhat puzzling way. The truth is the number of Americans that have actually severed a relationship with a company that they did business with because of a data breach, because of a sense that their data was being abused, is actually pretty low. And more Americans have uninstalled an app because they felt it was creepy, right? You know, we've all been there. The app says we'd suddenly like access to your contacts. No. Why does this pizza app need access to my contacts? You shouldn't have that. We've all been there. But in terms of changing our consumer behavior, right now, we haven't seen at that level a major shift. We haven't seen a major shift in terms of companies being punished in the public markets for these major data breaches. They tend to come back pretty quickly, and it's certainly true that we are in a somewhat new era in the sense that today, which was not true 10 years ago, we have seen Fortune 500 CEOs lose their jobs over a data breach, but not all of them -- in fact, not even most of them. In fact, not even the ones who were at the center of some of the largest data breaches.

And so there is, from the standpoint of our relationship with companies, kind of a complex relationship going on here. And so what you saw happen in the last couple of years was a sense, a bipartisan sense led by the Senate and the House -- particularly the Senate, Republicans and Democrats -- that it was time to increase what I call that low watermark of privacy. These things take time. It takes time in part because privacy is the sort of issue that I think we all care about when we really think about it, but for very few people is it dinner table conversation. And so it tends to consistently be pushed down in the priorities list. And so figuring out where that constituency is for privacy is a really important moment, and I think there are two. And one of them is ultimately influenced by COVID.

The first is a concern about big tech companies generally. And this is, of course, the sort of flavor of the month, of the year, of the last three years. It might be of the decade, but this idea that there's concern about some big tech companies getting too big. And here, it's probably right to have some caution, because if there was one market effect that we saw from GDPR [General Data Protection Regulation], it's that GDPR actually had the perverse effect of concentrating the advertising market, not causing more and more entrants to come in. Why? Because it raised compliance costs. It raised the barriers to entry to being in aspects of the advertising market.

But the second piece I think is making people really wake up to just how important it might be to have fundamental privacy regulations here in the country is the fact that suddenly, post-COVID, in the middle of COVID, so much more of people's lives aren't just online. They've always been online for many people, but they're visibly online. There's something visceral and something real about the fact that suddenly, the only way we can interact is mediated by these devices. And we're in the middle of substantial social movement as a result of, you know, what they're seeing on the streets, and much of that is transmitted by social media. It's also, in many cases, causing some real concerns about the contours of social media, but the recognition that the issues that we care about, the business that we do and so much of the lives that many of us lead are happening online I think is creating an unusual moment, maybe a unique moment for us to actually get

behind something as complex and technical and controversial as comprehensive privacy regulation. I think this may be the moment for that.

00:08:20 **Lauren Cahalan:** What would a concrete data privacy plan look like, and could the pandemic be the catalyst for actually getting it done?

00:08:26 **Dr. David Edelman:** The truth is we've known for a long time what it takes to bring our level of individual risk down by maybe 80% or 90%, and these are all things that are familiar to you and me and everybody who is listening to this podcast, right? You know that you need to have two-factor authentication on your email, and you need to have it on your bank accounts as well, right? The reality is it hasn't moved the needle that much, but what has moved the needle are a few things.

First, individual companies are becoming more and more aware of the need to lock things down within their workforce. A lot of people take their work laptop home. A lot of people's phones are managed by a company. And more and more IT professionals are actually getting through to the CEOs and saying, "If we care about our data, if we care about our customers' data, if we care about our employees' data, we have to take these steps."

You know, the second is that companies really have gone to great lengths in many cases to make it easy and user-friendly now to install some of these basic tools. It used to be very hard to set up two-factor authentication. There used to be very few banks that were able to provide it. But now today, most major providers do this. And those that don't, particularly financial service entities that don't, are engaging in malpractice, and they know that. And so if you want these tools, they're available.

But the third piece, and the piece that we're seeing happening more often now, is setting up security by default. For instance, now, if you want to log onto your bank without having two-factor installed, it will annoy you about every couple of weeks about the fact that you don't have this installed. It's about sort of nudging people into better security practices in the same way that, "Look, we've been here before." People didn't buckle their seatbelts when seatbelts were first invented. A lot of people don't have a habit of locking their doors if they don't live in a high-crime area, but these are habits that we can get into that become muscle memory that actually don't take up that much time.

You know, the last one, of course, is COVID, and COVID has created this moment where I think there has been not just individual recognition of the security risks -- and indeed, there has been a massive spike that some have reported in spearfishing attempts to try to, you know, hack computers by, you know, for instance, open up a malicious email, a malicious attachment to an email. But even more important than that, it's provided a greater clarity of reporting on when companies aren't living up to the standards that they advertise or the standards that you'd expect on security. And I think a fascinating window on this, and probably a sign of what's to come, is what we've seen in the last two months with Zoom.

Now, Zoom is a company that, by its own admission, was unprepared to deal with the onslaught of traffic and unprepared to deal with the onslaught of security scrutiny that they have gotten, because suddenly this company is, and I don't mean this technically, critical infrastructure. Suddenly, this company is the way in which the U.K. prime minister is holding cabinet meetings. And so suddenly, the security of Zoom matters a lot more than it did. And so what you have is an onslaught of journalists who were actually looking under the hood.

00:11:31 **Media Clip #4:** Weeks intoa worldwide lockdown, the company Zoom has emerged as a new home staple, but there are growing concerns about Zoom's security. The CEO and founder --

00:11:43 **Dr. David Edelman:** That's going to be a little window into what's to come. More and more companies, as they find themselves in the spotlight and as they find themselves getting popular, are being asked by their users, but also are going to be asked by investors, and not just public investors -- private investors in particular, right, the private equity firms that are thinking about scaling a firm -- is your cybersecurity posture such that you're going to be able to scale? Previously, for early-stage companies, it wasn't a terribly high priority. Now, I think, just as it's essentially a basic management practice in corporate America, I think it's increasingly table stakes for having a company that's going to be capable of scaling.

00:12:24 **Lauren Cahalan:** So how do you think these increasingly important roles, and, as you mentioned, as we interact with technology in different ways and it becomes ingrained in our everyday lives, has this changed people's perceptions of big tech?

00:12:37 **Dr. David Edelman:** The question that is now coming to the fore and has been part of certainly the Democratic presidential primary, I think is increasingly going to be part maybe even of the main presidential election is not just what are we going to do about big tech -- and that will probably lend itself to a few bullet points -- but what are the actual problems that real people are experiencing that you want to solve? We have to have a national conversation that actually gets to the bottom of what is concerning to the American public and to the elected leaders that are working on their behalf, because right now, what we've seen is a lot of generalized anxiety, some of it very well-placed, but very few by way, I think, of concrete solutions that get at something that resonates with the American public. And so that's what I think we can look to next.

There are some real potentials for game-changers here. The truth is, you know, for those of us that are spending time around researchers in machine learning and AI, for instance, some of those researchers feel like little data is the new big data. A lot of researchers and folks who are working at the forefront of AI are actually wondering if a world in which these massive volumes of data that could never be really meaningfully processed and include lots and lots of noise, whether they're really the future of personalized recommendations or of prediction, or whether we just need smarter algorithms working on smaller data sets. If that's true and the future really might be able to operate on smaller data sets, not just massive amounts of data being crunched by incredibly expensive machines that only a couple of companies have access or the resources to do, well, that could be an economywide game-changer for the future of what data values mean within this economy.

Let me ask you this, though. Are you on Facebook?

00:14:26 **Lauren Cahalan:** I'm on Facebook. I don't use it very often, but I'm on Instagram. So given that Facebook owns Instagram --

00:14:33 **Dr. David Edelman:** I do this poll with my students. I ask them, you know, how many people are on Instagram, how many are on Facebook? And when I get to the Facebook question, they'll roll their eyes and say, "My parents are on Facebook," which I think is unfair. OK. So you're on Facebook. You're on Instagram. Do you feel like a citizen of Instagram?

00:14:49 **Lauren Cahalan:** No. I wouldn't -- yeah, no.

00:14:52 **Dr. David Edelman:** This seems like a crazy concept. Twenty-five or 30 years ago, this was not a crazy concept. If you go back and you look at some of the fundamental political statements about the internet back in the day -- I would recommend to everyone go on YouTube today and look up John Perry Barlow. The name sounds familiar because he was a lyrist for the Grateful Dead. Look up John Perry Barlow, Declaration of Independence of the internet.

00:15:19 **Lauren Cahalan:** OK.

00:15:19 **Dr. David Edelman:** At Davos, not a place you'd expect declarations of independence of any sort to be written. At Davos, John Perry Barlow a long time ago wrote a manifesto of the early internet age. And it said things like governments, you have no purpose here. We are citizens of cyberspace. We are united. It went on to essentially describe the ways in which the internet represented a distinct space that was disconnected from our national identities and disconnected from every aspect of our lives as we came to understand them.

And the big shift over the last 30 years, maybe the depressing one to those of us that were around back then and on that wonderful open, promising internet, was that it didn't quite come to be. It didn't come to be in the way that many of us anticipated. And I think, you know, most of the world, and certainly those of us that were working on internet policy were not quite as techno optimistic, even when those words were being penned as they were, but this idea that companies, if they haven't taken on the identity of citizenship -- they definitely have not from the standpoint of us thinking that we're citizens of Facebook. Although, if you go back and look at some of Mark Zuckerberg's early quotes, I think you can find the intonations that that

might have been the case. What you are seeing is that some of these companies do have the diplomatic and political significance of countries. That's a new shift. A world in which by virtue of their size, the number of people they employ, and they control they have over what the Russians would call the information space, what we might just call our day-to-day media lives and social interactions, by virtue of all those features, suddenly, companies are finding themselves in positions that even 10 years ago were reserved exclusively for governments and nation-states. You're seeing it play out in the geopolitical context. After all, it was Russian infiltration of Facebook and social media generally, Instagram, and I don't even know how this is possible, Pokemon Go. Somehow, the Russians got into Pokemon Go among others.

00:17:26 **Media Clip #5:** It was just reported that even Pokemon Go was used by the Russian-linked election meddling effort. We should have seen this coming. No, we should have seen this coming.

00:17:35 **Dr. David Edelman:** That was the place they decided to go to have this effect -- not to the corners of Washington and Seattle, San Francisco and New York, or try to get into the newsrooms of the various companies, not to try to start small political movements in meetings on corners or in church basements. No. The new version of that is to create those movements online. And you had unwitting Americans who, in many cases, attended rallies that were organized by someone sitting in a windowless room in Moscow. That's nation-state-level significance.

Likewise, you know, you have Sony, a massive U.S. company that, because they offended the North Koreans, because they released a movie that I'm not sure I can recommend to you -- but it's called The Interview, a movie, the plot point of which is the North Korean dictator being assassinated by a couple of hapless buddies in that movie. It was so offensive to the domestic political constituency as filtered through the Kim regime of North Korea that they decided they had no choice but to engage in what was effectively a major cyberattack against a U.S. company.

00:18:41 **Media Clip #6:** Today, Sony Pictures pulled the movie, including on DVD or on-demand, according to Variety. Tonight, we're learning that federal authorities are all ready to point the finger for it all at the North Korean regime.

00:18:52 **Dr. David Edelman:** Think about that relative to the Cold War. Back in the days of the Soviet Union, Soviet paratroopers were never dropped onto Coca-Cola headquarters in Atlanta to dig through files to find dirt on executives, or to just burn the filing cabinets down, or break the conveyor belts and disrupt that distribution. That didn't happen here on American soil. And yet, change the actors, and you've nearly just described what the North Koreans attempted to do to Sony. They held a U.S. company hostage from almost 6,000 miles away, or, in another context, you have companies that have some of the best visibility of what's happening on the whole internet. And when a major hacking operation happens, they may be the first people to see it. And as a result, they also are in the position to be the first to attribute it, to tell the world about this maybe state-based attack on another state.

Now with that decision to attribute, they're going to make that decision based on their business needs. But in reality, they're also making it on behalf of the government of the country that they're in. So you've had cases where cybersecurity firms decide when and how to attribute what, in some cases, for some governments might be perceived as an act of war. And the knowledge of that act -- it's not always coming at a time and place of the government's choosing. It's coming at a time and place of the company's choosing. We're in a new paradigm where these companies are potential victims of geopolitical disputes, attributors -- not unlike the State Department or law enforcement -- and defenders of protecting national critical networks. These are completely new roles, and we have to reckon with the fact that what were previously across every one of those areas monopolies of government are no longer monopolies held by the government. They're roles that companies are playing a major role in as well.

00:20:45 **Lauren Cahalan:** I want to transition into a discussion on content moderation, misinformation and kind of the role that these platforms play in kind of everyday society with the backdrop of, you know, the 2020 presidential election coming up, coronavirus, and then you also have protests both in Hong Kong in the U.S., if you can make kind of international tie-ins kind of across the world of how these platforms are used, what content moderation means and looking at misinformation moving forward.

00:21:13 **Dr. David Edelman:** Sure. And look, let's start with an executive order penned by the president, designed to put attention on and maybe even motivate some enforcement around the way in which social media companies moderate. Now, that executive order was premised on an attempt to shift the conversation specifically to what the president alleges is political censorship on that platform. Now, you can go take a look at studies of political censorship on those platforms, and I think there may be less here than meets the eye or that might normally meet a presidential executive order. But what the president was getting at in that EO is a conversation that is actually happening across the political spectrum and is happening regardless of politics. And that conversation is one about what sort of roles and immunities exist or should exist for these large social media players.

And the reason this is coming to the fore, of course, is that whether by their own lack of planning, or an inability to understand what was happening on the network or a sense that there was no need, and everyone has a different view on what the reason behind it is. The Russians were able to successfully infiltrate U.S. social media platforms and use it to attempt to sway a U.S. election. That is not open to debate. Those are the underlining facts of the case. Whether or not it had an effect on the U.S. election, that's what will be debated for decades and decades going forward, but it cast huge light on this major challenge. And it's worth noting that this particular issue really came into the U.S. public consciousness in part because of this Cambridge Analytica scandal. You might remember hearing about this. Cambridge Analytica was a company that claimed they had the ability to -- I think they called them psychometric graphs of U.S. voters and to pinpoint down to the individual voter. But mostly what they were doing was buying up data that was sort of ill-gotten from, in this case, some researchers that were breaking Facebook's terms of service in trying to collect data from individuals and their social graphs.

Well, that was portrayed in the media as a data breach. It wasn't a data breach. It was just a violation of Facebook's terms of service. But the reason why it became an issue that took up untold pages of newspaper space for months and months was that it struck at the core of a new dimension for these social media platforms, which is the extent to which they are now increasingly becoming critical democracy infrastructure.

And if you go back to 2008, Barack Obama would be the first person to say -- and did, in fact -- that he believed his political movement could not have gotten off the ground had it not been for the internet, had it not been for social media. The other side of that is I think the folks running the Trump campaign would have said the same. And so you have this incredibly powerful tool for communication, also for mobilizing groups, for finding affinity. And like anything else that helps people find affinity, it also creates real problems when we don't like those affinities.

And, you know, the extent of political censorship is almost -- it's the tip of the iceberg. It's the way in which I think individuals can help realize that this is an issue, that gets to the core of their civic identities. But what's bigger here is the question of how do you curate, how do you keep safe, how do you appropriately manufacture a product that people want to use that also becomes a principal medium of communication? I mean, just last night here in Washington, there was an image that was circulating on Twitter and Facebook and elsewhere of flames that were rising as high as the Washington Monument as part of these protests. It wasn't true. The photo was manufactured. It was completely misinformation designed to sew discord and to create the impression that what at that particular moment were largely peaceful protests had escalated into massive riots in that particular part of town. Now, several of the social media platforms were, diligently and as quickly as they could, taking down that image. Facebook, as I understand, did actually a pretty rapid job of doing so. And as tends to also be the case, Twitter did a somewhat less than rapid job of doing so, probably not by lack of desire but by lack of capability.

Interestingly, you are now seeing -- and I think COVID, again, brought this to the fore for us -- little flags, little checkmarks, little screen blurs that give you an opportunity to take that breath before you consume passively and then register in the part of your brain that will recall it but won't remember the context -- that particular piece of information, right? I mean, how many of us have been scrolling through our feed, and we see something that looks very outlandish, but it kind of aligns with these crazy times in which we're in? And so we believe it's true, and then six weeks later, we mention it to a friend, and they go, "Well, wait, that was a hoax." I mean, a lot of us have been there. And I think the companies deserve some credit for now being much

more aggressive, much more aggressive relative to the status quo, of when they find those debunked rumors. And they're particularly useful with COVID, because there is a scientific ground truth they can point to of saying, "Warning: This suggestion that you crunch down on Tide Pods is not going to cure COVID." It's good that Facebook and other platforms give you a warning with things like that. That's appropriate in my personal belief, and some will disagree with that, but I happen to think that is a social good.

Things get really complicated when it comes to political messaging and politicians lying, which they do. Perhaps they're doing more of that now than we're used to, but politicians lie. But let's not let the fact that we're uncomfortable with these platforms adjudicating politicians' truth get in the way of the reality that they have both an obligation and an opportunity to help us sort through the junk in the nonpolitical world too, because the truth is they have tremendous power to do that. They've been traditionally shy to exercise that ability, and yet, deep down, these companies run a business. And before we sort of get up on a soapbox and talk about how these platforms, you know, cannot be in the position of ever interfering with any aspect of our speech, let's also remember they're private companies. And the First Amendment protects us from government interference with speech. And so, does this provide an opportunity for new or other social platforms to come to the fore and maybe play more constructive roles in our lives? Maybe. You know, we're certainly seeing a generational shift in the way in which people use some of these platforms.

You know, when we think about this notion of what kind of curation needs to happen, how we need to be focusing in these areas, let's not make every intervention about fighting the last war. Let's not make every intervention about the narrow intersection of Facebook and politics and Facebook groups, because the more interesting, the more challenging and maybe the more promising areas that we're actually going to be able to engage in are the new social media platforms that are coming to the fore that a lot of younger people are using, but also some of the lessons that we've learned on how, in fact, Facebook can take some action.

00:28:41 **Lauren Cahalan:** So, David, what role do you think technology issues will play in the 2020 election?

00:28:45 **Dr. David Edelman:** I think it's fair to say that in the middle of an economic downturn, unlike any we have seen since the Great Depression, in the middle of a pandemic and like any we have seen since the early 20th century that technology is not going to be at the forefront of the minds of most Americans in this election -- rightfully so. Most Americans are going to be focused on paychecks, going to be focused on fairness, going to be focused on the vision of the future of what this country is and what it stands for. I don't think most of the presidential campaign is going to be spent talking about the finer points of telecommunications regulation or of the comparative merits of the GDPR versus the CCPA [California Consumer Privacy Act] and privacy. But I think what you are seeing is a recognition of a few underlying realities. I have what I call Edelman's three phases of government technology, and the third one is nirvana. But the first phase of government technology is, oh, who cares about this technology stuff? And by the way, this could be cybersecurity. This could be data privacy. This could be any issue, like, who cares about this stuff? Just give it to the young staffer. And so that government official finds the youngest-looking staffer they possibly can and gives this issue to them, hoping to never see or hear from it ever again. Then phase two happens, and phase two is the "Oh, my God" phase. Phase two is, oh, my God, cybersecurity, for instance, or data, our data is all gone, or something else. What are we going to do? It's a panic. It's a crisis. What are we going to do? We'll appoint a czar, and then they breathe a sigh of relief, because they've appointed a czar. They're just there almost as a sort of security blanket to government officials that, again, in their heart of hearts hope this issue would go away but fundamentally know that it's not. But the third phase, the phase that I am optimistic we are moving toward in the U.S. government and hopefully around the world, is the third phase at which every government agency realizes that technology is a core part of their mandate and the way in which they do their job. In other words, in the same way that you wouldn't have the defense secretary walk into the Situation Room and proudly chuckle, "I don't understand this economics stuff," because it wouldn't be done, because there's an expectation that even the defense secretary has a recognition of and a sense of responsibility for the American economy. So too would you not have someone proudly walk into the Cabinet Room and chuckle: "Well, I don't understand this tech stuff. I have a kid over there for it." And that's where I think we can be headed and where we may be headed -- I think increasingly, we are headed as a society whether we know it or not.

00:31:25 **Lauren Cahalan:** Thank you, David, for walking us through that transition. It's really helpful to put these conversation into a broader context.

00:31:30 **Dr. David Edelman:** All due to fantastic questions, so thank you so much. I appreciate it.

00:31:35 **Lauren Cahalan:** As part of my role as an investigative equity analyst, I have spent the past year studying challenges facing the tech industry. From antitrust investigations to data privacy legislation and content moderation, these are complex issues. And it is conversations like the one we had with David today that provide us with an opportunity to challenge our thinking, condense fact from the vapor of nuance and make informed investment decisions for our clients.

00:32:04 **Ken Stuzin:** Hello again. This is Ken Stuzin. Thank you for joining us as we continue this journey to seek out insights that help us to better understand a rapidly evolving world. If you enjoyed listening, we encourage you to subscribe to the podcast. We will be back with another episode next week, a conversation about investing for impact with Lynelle Cameron, CEO of the Autodesk Foundation, and Brian Rice, portfolio manager at CalSTRS, one of the largest public pension funds in the world. Until then, be well and stay safe.