THE BROOKINGS INSTITUTION
The *TechTank* Podcast

‘Navigating Technology and National Security’ with author Justin Sherman

Monday, December 22, 2025

NICOL TURNER LEE
Co-host, The TechTank Podcast;
Director, Center for Technology Innovation;
Senior Fellow,
Governance Studies,
The Brookings Institution

JUSTIN SHERMAN
Guest, The TechTank Podcast;
Founder and CEO,
Global Cyber Strategies

[music]

CO-HOST NICOL TURNER LEE: You are listening to Tech Tank, a biweekly podcast from The Brookings Institution exploring the most consequential technology issues of our time, from racial bias and algorithms to the future of work Tech Tank takes big ideas and makes them accessible.

[00:00:24] Welcome to the Tech Tank Podcast. I am co-host Nicol Turner Lee, the director of the Center for Technology Innovation. At The Brookings Institution, founder of the AI Equity Lab, and editor-in-chief of the Tech Tank blog. Now many of us in today's conversations about artificial intelligence and emerging technologies, we're caught on these conversations on responsible, ethical, inclusive AI. I know I am, but one of the areas, what we don't talk enough about is national security. As concerns around data flow, supply chain, semiconductors, and cloud infrastructure drive U.S. national security policy, the government relies on a growing complex set of regulatory tools to protect critical technologies. And as I think about it, I'm actually not that far off from this conversation. Just last year I was part of a critical infrastructure group that was organized by former Secretary of Homeland Security, who brought together just a range of stakeholders to talk about AI's potential attack on critical infrastructure.

So I had to correct myself cause I know a little bit more about this than I probably think I did. But today I have an expert who knows more than me, and I've known this person for quite some time, so I know you will be delighted. he has an upcoming book, navigating technology and national security, which offers a clear and detailed look at these tools that I just talked about that are protecting critical technologies and in particular how they're shaping us, technology governance. Justin Sherman, who I'm gonna tell you a little bit more in a moment, he examines in this book key programs such as the Committee on Foreign Investment in the United States and Team Telecom and others to provide insights into how these systems work, why they matter, and what their future means for innovation and national security.

And honestly, what's becoming a rapidly changing world. I'm pleased to have Justin join us. He is the founder and CEO of Global Cyber Strategies, as well as a fellow at the Atlantic Council's Cyber State Craft Initiative. He's also an adjunct professor at Georgetown University's Master School of Foreign Service. He's advised companies and government on cybersecurity, data policy, tech governance. I know him from his days in civil, society where we often, were conjoined at the hip looking at issues related to data privacy as well as national security and the digital divide. So I'm so happy, Justin, that you could join me today. Welcome to the podcast.

GUEST JUSTIN SHERMAN: Thanks very much for having me.

CO-HOST NICOL TURNER LEE: I cannot believe that you also wrote a book. Justin, I wrote a book as well, right? You know that, right?

GUEST JUSTIN SHERMAN: Indeed. And I got, I have the book on my shelf.

CO-HOST NICOL TURNER LEE: Oh, thank you so much. And I have yours now, like in a PDF, so make sure I get a signed copy, okay. Of the book. Now I wanna ask you a question that many people often ask me when I'm talking about the book I wrote. And I, and again, I've known you for quite some time, and so I'm just so excited that you put pen to paper because I remember the days when. Both you and I had no time to put pen to paper. so I wanna know what motivated you to write your upcoming book? What gap in public understanding of policy did you like really wanna address? what got you to sit down and craft what I had found as I looked through the book and read it? something quite interesting in terms of that preview copy.

GUEST JUSTIN SHERMAN: It's always, as you said, such an interesting question for anyone who you know, writes something longer of this length. My motivation was really a couple of things. One is we hear a lot about how technology today, whether it's artificial intelligence models, whether it's robotics, whether it's biotechnology, is impacting. Security, geopolitics and so on. But, there's often a lack of understanding of how the U.S. government in practice actually approaches some of these challenges. And the second motivation for writing this book was, and obviously you've been, you and your colleagues have been a, huge driver of this as well. There's a lot of really important debate about. Technology regulation from the perspective of consumer protection, from the perspective of civil rights, from the perspective of, equity and so on. And so what I wanted to do with this was look as well at how the U.S. government. Actually already governs a lot of technology, but not for, unfortunately not as much for consumer protection reasons, but really for a lot of national security reasons. And also say that's what I, try to tell in this book is the history of how the U.S. government has come to govern so much technology, so much data through national security powers, why it does it that way.

What are the pros, right? Sometimes there are national security issues that maybe a consumer focused law wouldn't address. And what are some of the cons, right? National security law can be very secretive. right? It's focused on protecting a very particular set of interests that might not always equal, the public's interests or the interests of every American. And I wanted to untangle some of that, in this era because we're seeing. More of these debates than ever. And, shedding a light on how we got here I think is, critical to charting the next chapter.

[00:05:53] **CO-HOST NICOL TURNER LEE:** So that's what I thought was interesting in the book. Because this is a very vast regulatory landscape, when you [00:06:00] were putting this together and you were doing the research and coming up with your recommendations, were, are there any findings that particularly surprised you? because I- you and I know there are often misperceptions or misconceptions among policymakers, investors, industry leaders, that you're hoping to either correct, right. Or amplify within the book. So tell me a little bit more about that. what were your surprises?

[00:06:26] **GUEST JUSTIN SHERMAN:** It was really interesting to see. How many patterns on any historian listening is laughing that I find this surprising, but, but to see how many patterns repeat themselves in these debates. And I'll get to in a minute, things that are different and, misconceptions we, we need to fix in terms of what's new to today. But the book starts, before the United States was founded with, because the colonies actually, were already. the American colonies were already using export controls and trade embargoes to restrict the sale of different goods to foreign entities. In that case, Britain, and then goes forward from there, right through many more years of export controls. Looking at. In the seventies, the US started screening investments coming into the U.S. for national security risks through the Committee on Foreign Investment in the us. we now have programs that regulate telecoms for national security.

We have programs that regulate cloud, services, data transfers and so on. And so all to say it was very interesting to me throughout. The couple hundred years that a couple of themes have really persisted. One is that over time industry has pretty consistently complained about a lack of transparency into this governance saying. You're coming in and you're preventing us from selling goods to Germany or Korea or now China, let's say. Or you are investigating a lot of our business practices or you're blocking investments in U.S. companies for security reasons and throughout. This period, it's been pretty similar feedback from companies that they don't feel they have a good insight into how or why the U.S. government makes these decisions. Companies pretty consistently have asked over the years for, specific lists of, technologies that the U.S. government does see as a risk or doesn't see as a risk. and so anyway, so that was one interesting theme to see the same consistent criticism and pushback. Another consistent theme is that let's say we're regulating data, right? We could always have a debate about how much data. Is sensitive, right? Or what? What's that number at which data becomes dangerous? Or, in the nineties I talk about, this was the debate with supercomputers and Russia, right? Was during the Cold War, the U.S. government had a lot of export controls limiting the sale of supercomputers to the SSR. After the Soviet Union collapsed, the Clinton administration relaxed a lot of those export controls because they said, we want this burgeoning U.S. computer industry as they called it then, we want this computer industry to thrive, so we wanna sell more technology to Russia. It was the same debates then of that.

At some point you have to pick a number, right? And they, so they said, okay, this is the line where anything above it you can't sell. It's too dangerous. Anything below it, you're totally good to sell. but we've seen that theme again throughout these time periods is the government at some point has to draw a line around. What constitutes a national security issue with technology? What's too great a risk, what that number looks like? and so that creates interesting questions. The third thing I'll just say to wrap on this question is, you also had mentioned misconceptions. And one misconception among others that I highlight is how today when we talk about AI, we talk about software, we talk about data. Policymakers are talking about governing a lot of digital intangible things. AI model weights, source code, data points in a file, right? But a lot of the regulatory structure we have to govern technology. In this security area was built for physical, tangible goods, right? An actual device, copies of paper that had written on them. Technical schematics. military equipment, right? So one misconception I talk about is, okay, if we're going to have these debates today about how do we control the spread of AI, we're talking about modern issues, but the tools we have to address them are not always well-suited because they were built for an arrow where you couldn't just share information and upload things on the internet so easily.

[00:11:14] **CO-HOST NICOL TURNER LEE:** I think what you're also leading into is the maze, right? That has come with U.S., the U.S.'s national security regulatory landscape. there are key structural features of this maze, and it's challenging, I think for, not just industry and investors, but even for, policy makers to understand that. And I'm very sensitive to your comment that you just made around, our tech policy. Really being, closely aligned with national security interests as to whether or not we're gonna support or strip right U.S. infrastructure, particular technologies, which maybe we can get into a little later. But like, how would you describe that maze that I'm suggesting? there are other features of it that are worth mentioning, Justin, that you also talk about in the book.

[00:12:02] **GUEST JUSTIN SHERMAN:** Yeah, it's a good question. A lot of these, there are a couple general, if we say, okay, what are we actually talking about with these regulations on this governance regime, there are a couple models for how these laws and, regulatory regimes work. One is a licensing based regime, which is a U.S. company building a certain technology or doing something in the tech sector, can't do a certain thing unless the government explicitly provides permission. So one example is export controls, right? This is how they've worked for some time. a company generally making chips, let's say, or certain kinds of microelectronics might be prohibited since 2022 from selling that technology to Russia or to certain countries known to share technology with Russia. But the U.S. government, if it wants, could say, here's a license, you are permitted to actually go forward with this particular sale because we've granted you an exception.

So they set up these blocks on what the private sector can do, and then you can get case by case exceptions. the. The data, the bulk data transfer program set up in the Biden administration. I worked a lot on this, was set up to similarly control how can companies share and transmit Americans' data in large data sets overseas. And it's similarly based around licensing, right? So certain things are blocked by default, but then there's a licensing process where you can get an exception. a second model of this maze is. That the government will actually go do case by case reviews of particular business decisions. So I mentioned the Committee on Foreign Investment in the U.S. (CFIUS). I put that in this bucket where if a U.S. company is taking an investment. Let's say from an Israeli venture capital firm or maybe an Australian private equity fund, or perhaps a state owned entity in Eastern Europe, they might have to alert the U.S. government to that investment if they're in, if certain sectors, let's say a critical. Military technology, or even just a cloud company broadly, they might have to report that investment. The U.S. government will review it. this is also how summary cable licenses work. A company wants to hook up one of these undersea cables to the U.S. they similarly go through a review process, right?

It's not a license with an exception. They have to go through a case by case, basically audit. also say it's very much is a maze because these different programs the U.S. has set up over time overlap, right? Some of this is new technologies. We didn't have, cloud computing as we do today 50 years ago, we didn't have even though, as you've written about and talked about at length, so, please correct me, a lot of the, while some of the AI techniques and methodologies existed a while ago, we didn't quite have LLMs like we do today. So some of this maze is hard to parse because of new technologies. but part of it, as I said, is also the challenge of we're taking these years old laws and regulations and trying to apply them to a world of hacking and really global technology and a really complicated, and fast moving threat and technology landscape.

[00:15:31] **CO-HOST NICOL TURNER LEE:** and that makes sense. I think this is something that we're seeing across the board that our policy, regimes are not necessarily structured right for these emerging technologies in which we're seeing and your research Speaks to why it is we need to have this regulatory toolkit. I think that's one of the benefits of the book. It's like there are these blind spots, that we have to address and there are tools that, do not either get as much attention as they could be applicable, to this new landscape. And then there are some tools that we might need to create ourselves in the, in this context and time. I wanna talk to you a little bit about that because. Come on, Justin. The regulatory toolkit is something that we as policymakers, this is part of our speak, right? In terms of trying to make sure there's something that everybody can find a resource that works for them in the policy and regulatory landscape. Talk to me a little bit about why we still need to stay tethered to this idea of the regulatory toolkit and then where you see some of the major weaknesses though, or blind spots of doing such.

[00:16:36] **GUEST JUSTIN SHERMAN:** There are. I appreciate you asking this 'cause it's good to, it's good to make me put a fine point on it. There are lots of, reasons to have governance and regulation of technology that specifically focuses on national security. Part of this is that we live in a really complicated global environment where, you know, as, we hear about all the time, technology's very interconnected. It's very easy for people around the world to hack into all kinds of systems, and so there's a need to look at. The private sector tech landscape and say, okay, what are the threats facing different companies that are building innovative technologies, that are collecting lots of data, that are really big drivers of the American economy, or provide really critical services to, let's say the health care sector or, for traffic light systems or water treatment plants. So there's, a real reason given. hackers in China and Russia and cyber criminals and other threats to look at the technology in the U.S. and understand how we can better protect it. Another reason to have a lot of these regulations is that companies, different companies have different motives, but [00:18:00] generally most of the large tech companies, in this country obviously are driven by profit, right? And and I'm not, and I'm not suggesting, and I say this in the book, I'm not suggesting that U.S. companies should make all their decisions based off what the U.S. government wants. like I'm not saying that, and I think in the current moment we're seeing how bad that can be. but it's still true that, if a cloud company wants to break into the market in China, for example, their first thought might be how do we expand our market share?

Not, what are the security risks of this activity? Similarly, there are lots of really innovative companies. That are competing to build, AI systems to improve health care image analysis. Or maybe they're building new biotech innovations or robotic systems and they want to grow their company. So they look to take investments from foreign investors. They look to build into global technology stacks, and it's not actually out of any malice or, or, or sort active neglect, but just they're just not aware of maybe some of the national security implications of what they're doing. So I'll to say, I think these are real strengths of these regulations is these are opportunities for the U.S. government to say, you know what, when a Chinese investor bought Grindr. The gay dating app, which happened a few years ago. They got access to tons of sensitive data and were actually concerned there. Or, Hey, you know what, if you're actually gonna export this semiconductor or this other technology to this country in Europe, FYI, you might be actually passing it off to, the Russians who might put it in a missile they fire at a hospital in Ukraine. So there are lots of these real examples where, there's real reasons to have it. Again, though, as I've mentioned. Anytime you're governing something and it relates to national security, you're also gonna have issues like limited transparency. It's harder for companies to navigate because of that. And so like anything, as you joked in, in our policy, wonky land, there's lots of trade-offs that come with the toolkit that we have.

[00:20:10] **CO-HOST NICOL TURNER LEE:** and it's so interesting too, because one of the things that I've said, as it related to national security, is that privacy or data privacy is a national security concern. And I, wanna go down this path, because I know you've written extensively about this, in the past as well, about privacy and data protection as it relates to national security. If Congress were to create a baseline federal privacy law, wouldn't some of these elements that you're discussing also be addressed? The Grindr example is a great example where we see what started out as more of a consumer issue becoming more of a national security issue and we could even get into AI, right? And how that's made it even more complicated when you start to think about this relationship between technological assets. And, the type of data disruption that we're seeing and data corruption that we're seeing in, these spaces nowadays. So what do you think, does baseline private or privacy solve some of this Justin, or is it, the toolkit in national security sort of has to be the one that sort of leads this discussion going forward.

[00:21:17] **GUEST JUSTIN SHERMAN:** I think you're right. And as you said, we've been banging this drum and, many others have been banging this drum for years at this point. the privacy is a national security issue. I agree completely. I write in here, that I think the, primary approach we should be taking to tech governance is not a national security one, right? Because first and foremost, we should worry about American's privacy, right? We should worry about inherently, right? We should worry about. Issues like access to technology can, different types of people. again, back to a lot of your work, the equity issues, competition is another big one, right? I think a lot of Democrats and Republicans are on the same page about this in terms of we need to break up some of the choke hold that only a few companies have on the tech sector. So there are lots of reasons to me to govern tech that don't have anything to do with national security. You help national security by doing it. I think as you said, with Grindr or something else, it would be helpful to have a comprehensive privacy law when the law that, of course covered a lot on this show, when the law, when Congress passed the law last year to ban or divest TikTok, when they, originally wrote the law, I met with, a number of the, staff as they were doing it, and I made the point that. I don't disagree, that there are security issues to look at TikTok, but to the point you just made, Nicol, I said to them, you're basically saying that if this company is in U.S. hands, there's no data problem. And I pointed out to them under the law as they had written it, I said, you realize that you're in this law itself, you're saying.

That if a U.S. company owned TikTok and sold all of the data to a bunch of data brokers, that would be completely fine. But you're so focused on the ownership of China issue that you're missing it. So I, I say that as an example where if we have the comprehensive baseline, I think that helps us on the security front. On top. Sure. We might need a few extra controls, right? If you're trying to protect data from a criminal. You're gonna need additional protections to protect it from a foreign spy agency. That's just a difference in the magnitude of the threat. but I agree that we wouldn't need a lot of these complicated national security regulations for tech if we really doubled down on actually having comprehensive consumer focused, rights focused, governance for technology.

[00:23:52] **CO-HOST NICOL TURNER LEE:** Yeah. and I think that's like such a great point, right? That sort of spills into the national security debate, which actually I love your book because it should also be something that we're thinking about as we append some of the regulatory strongholds we've had in this space. I'm also thinking about, this data broker issue that you just mentioned and bringing in other countries outside of China. Because that's all we talk about is China. in this country you've written about Europe's data broker market and its risks as well, and I'm, just curious how you see the EU landscapes creating spillover risks for U.S. security and what can transatlantic partners do together? Because again, and you and I both know this, whenever we talk about national security, it's like us against China, right? And the "us" is usually everybody else right outside of Russia. So I'm just curious, can we look at how Europe has dealt with that data broker market and see if there are things that the U.S. can actually benefit from on the transatlantic side?

[00:24:53] **GUEST JUSTIN SHERMAN:** There's way too much, that the U.S. should be doing with allies and partners in this area. I think the, China example. you, just named as a great one where just the fact that so many countries might have, a feeling that they're being pressured to pick, are you with China, are you with the United States? I think speaks to the importance of having these strong relationships. And that's a very reductive view of looking at it. And I don't think. That policymakers should push that framing. but also say, I think that, it underscores the importance of the partnerships. The, Europe data broker issue is interesting because GDPR, in Europe is obviously so often pointed to as a gold standard for privacy legislation. It was roughly copied, by Brazil. It was roughly copied by India. There are lots of other countries that look to it as a model, and there are lots of, there are parts of it that I think are really good in that respect. But, there are also lots of issues. And I think one problem that, Europe has had with technology, in my opinion, is actually. They're really focused on the consumer and the market questions, which is very important. We have failed to do that properly in the United States, but in doing so, there's much less attention to the national security issues. So I had written recently, for instance, about how there are lots of data brokers operating in Europe right now that are actively selling data on european defense organizations that are actively selling data actually about the U.S. military from when the U.S. military has a base, let's say in Germany, and the European data broker will collect and sell all this data about those U.S. troops. So it, it was an interesting illustration I think, of this dynamic.

You're drawing out where we can work more with allies and partners to address these shared data challenges. We can also, as we're doing right now in the U.S. say, you know what? We're gonna do it alone and Europe doesn't know what they're doing and we don't need to work with you. but then this creates opportunities like this for adversaries to say, oh, there's a great gap. Maybe in a different world. Europe's combining its thoughts on consumer privacy. The U.S. is bringing a different perspective, including national security, and we continue to figure out a way to make that mesh, but instead we have these issues that are left, currently unaddressed for both the Europeans and us in the United States.

[00:27:27] **CO-HOST NICOL TURNER LEE:** and that seems so interesting 'cause I know in your work you've advised just to taken it to the, space that you're in, both government and the private sector, and then on the company investor side, all of what we're talking about just creates so much ambiguity, For people to understand it. Which is why I think your book will be just a useful resource as well for many people trying to get their handle on, get a handle on this. what practical steps Justin, should people be taking now in light of these regulatory developments? they're one day hot, one day cold. and I think the national security space is not exempt from some of that, ping pong that's going on right now. what would you say, honestly, to your people about how to navigate these, regulatory developments that we're seeing both in the United States and globally?

[00:28:15] **GUEST JUSTIN SHERMAN:** I'd say a few, and I do say a few things. One is to make sure you hire a really good, group or reference a really good group to track. All of the back and forth on tariffs and executive orders I gave up. That's right. I was gonna say, I gave up, I joked to clients. I gave up three days in, to this year in trying to track it. But there are obviously are lots of, Brookings, other think tanks, CSIS, others that, that track it, that, that do the day by day. So I recommend folks stay on top of that. The, second thing is even if there are shifts currently, it's very volatile with what's going on. Nvidia can sell chips to China. No they can't. Yes they can. Or in the last two administrations, a lot of people saying it's a national security risk to do too much AI or cloud or chips in Saudi Arabia and Qatar because of, and UAE because of all the China connections.

And now they're saying, oh no, no issue here. So the second thing I say is. a lot of people, including in the administration currently are actually not happy with some of these decisions. As you noted, there's a certain, hard line that a lot of policymakers have towards China, and so that's the second thing I say to companies now is even if there's gonna be a brief period of attempts at a trade deal with China, or talks of a trade deal with China, in this administration. Over the long, and I'm talking 10, 20, 30 year horizon coming up. The general bipartisan consensus though is to have these restrictions vis-a-vis China. So that's my second piece I say to companies is, you can act now if there's a gap. Obviously that's your decision, but you should also [00:30:00] plan for in the long term a lot of these controls are gonna come back because even if we can't get our consumer act together, some of these national security issues including on China remain, pretty strongly if you talk to these members of Congress and such privately, pretty strongly, bipartisan issue.

[00:30:18] **CO-HOST NICOL TURNER LEE:** I wanna just go to one more question in your book, which I think would be really interesting to the crowd. Particularly as we see, cloud computing become even more prominent. In your book, you write about know your customer protocols for cloud computing, and I find that to be such a great title as well as a chapter.

Because what you're doing is with Frontier AI increasingly relying on vast cloud compute. Darrell West, my co-host and I just talked about data centers and compute. I'm curious what you think successful regulatory regimes or corporate safeguards will look like for monitoring training, and then what efforts are gonna be needed to push this through the Trump administration 'cause I find, with cloud computing becoming much more prominent, there's like this implicit, notion that the cloud will be okay. when in essence what we're actually seeing with some of these, challenges we've had over the last few weeks with the cloud going offline, it's a pretty vulnerable asset as well. And I'm just saying that as my own experience of not being able to get on some of these websites because the cloud was down, for some of these, over the last couple of weeks. So just tell us a little bit more about like. How a successful regulatory regime will look like, and, how you massage that in this, piece around know your customer protocols. And I wanna hear what you think the Trump administration will do, if anything. Because it is, again, becoming very prominent in terms of the cloud, as a huge element of dependency for the type of technology we're expecting with AI.

[00:31:56] **GUEST JUSTIN SHERMAN:** Huge dependency. and so the know your I'll, go in order of your question. So the Know Your Customer concept basically is that. the Commerce Department. and this was actually initiated, under the, Trump administration one. And it just took a while, but, to come to fruition. But, the Commerce Department said, we want to take the concept that was. Really implemented a lot after 911 to counter terrorist financing In the financial sector, we wanna take the concept of know your customer, know who you're doing business with, and apply that to, cloud companies, specifically IAAS infrastructure as a service, providers in the United States so that they also know their customer so they're not in the commerce department's concern for unknowingly, helping an Iranian defense university perhaps train a bunch of drone related AI on a Microsoft Cloud system. I'm making this up right, but, or, accidentally have someone in China use it that they think is a security risk and there's concerns about the, concept of an AI race, which I don't entirely like, that, that was the motivating dreason, and so this program says to cloud companies, you're gonna have to set up, as you noted some monitoring, some regimes internal to your company to look at who are we selling to, what are they doing on the system? The challenges here are that there's a lot of industry pushback, which as we know under the Trump administration to get to your last question really resonates with this administration.

When there is industry pushback, there's a lot of cloud companies saying, we don't like this idea, that say we have a hard enough time as it is selling in certain countries because they still think. 12 years on from the Snowden leaks that were basically an arm of the U.S. government. Like we don't wanna have to go into these sales meetings and say, oh, by the way, we monitor half of what you do constantly on the system and track it so the U.S. government can look at it. That's not something that the industry likes very much. there's also a challenge of implementation, right? As you said, AI and everything is moving so quickly, there's a lot of dependence on these cloud systems. They're important economically, they support critical sectors. So how do we ensure that what's being proposed here from a policymaker view is actually implementable on the technology side?

So I'll just say I think the Trump administration is gonna be obviously really receptive to those industry arguments. deregulation is the name of the game right now, and so I would be. I don't think the program's gonna go away. A lot of this has been put in motion, but I would be shocked if the Trump administration started really enforcing these KYC rules anytime soon.

[00:34:53] **CO-HOST NICOL TURNER LEE:** Yeah. No, it's uncertain if they do. But at the same token, it, it's, to your point, it's Do we really need to do that right at this moment? I wanna end with where do you expect the biggest changes in the U.S.'s regulatory direction? spin your crystal ball here and let me know. Stronger data broker oversight platform risk reviews, new rules for cloud and AI access, or others. What signals should our listeners be watching for Justin, because this has been a fascinating conversation and I cannot wait for you to tell us more about how to get your new book, but just gimme that pro, prognosis of where you think we're headed in terms of the biggest changes of regulatory direction.

[00:35:38] **GUEST JUSTIN SHERMAN:** I'd, boil it down to three things. One we just talked about, which is the U.S. has this pretty big toolkit. CFIUS, team Telecom, the Cloud, KYC, the data broker program I referenced. there's now outbound investment review. So if you're a VC firm, for example, investing in semiconductors in China, you will also now have to go through a review. So you know, the first point would be, as we were just talking about, we have this big toolkit. It's probably gonna be underutilized in the Trump administration, but it's still sitting there. it's not good that it's on a shelf, but whoever is in office next, and probably the several after that will pick that toolkit back up and start using it. So that's the first thing. The second is, I think anything related to China and data seems to be really salient for policymakers, but also, state attorneys general and others who can actually bring lawsuits and litigation. We've seen. States that have been pretty active across the board against Meta, Google, TikTok pretty evenly in terms of suing for privacy violations. Then we've had other state attorneys general and other regulators that. Seem to, in my interpretation, care much more when it's temu or when it's TikTok than when it's Instagram, right? So there's this salience to, and we, and I could go on for 10 hours, which I won't do about if that's right or wrong, but, but, but that's seems to be salient, right?

That if there's the China connection. The third thing I'll mention is, kids, right? And maybe this is now, I'm not so much talking about, my book, but just as a general. point is anything related to kids, right? We've seen, and I think a lot of this is great, right? We've seen a lot move around how do we address chatbot harm to young children, especially young women and young girls, especially LGBTQ plus children and so on, right?
How do we think about kids' privacy and there's also concern about China and kids' privacy. So I think that would be the third, kind of prediction, if you will, would be anything related to kids and protecting children, obviously incredibly, vital to do, is gonna drive a lot of U.S. regulatory direction in the next decade plus.

[00:38:03] **CO-HOST NICOL TURNER LEE:** Perfect. I think we've got a plan, folks in terms of just things to keep an eye out on, and I'm so excited again about your book, "Navigating Technology and National Security." Tell us where we can find it and is it out yet? Can we get a copy of it and. Four where we could touch it.

[00:38:23] **GUEST JUSTIN SHERMAN:** as you said, Nicol, you and your team will certainly be getting, a hand delivered set of copies, but yay if this, if this ends up airing pre, pre-December 16th, then you can pre-order it and if this is after that, then you can go ahead and just order it. Amazon, Barnes and Noble, wherever you get your books.

[00:38:42] **CO-HOST NICOL TURNER LEE:** Perfect. we will definitely be waiting for our package and, putting this out so others can hear about just how important this conversation is. We've talked about a lot of different areas here and I could have gone on and on just even about, some of the other things that you shared during the podcast in terms of export controls, et cetera. But, we'd need another hour, Justin, to go through all that stuff. Thank you so much for joining me.

[00:39:07] **GUEST JUSTIN SHERMAN:** Thanks again. I appreciate it.

[00:39:10] **CO-HOST NICOL TURNER LEE:** Listen, folks, this is what we do at the Tech Tank Podcast. We bring to you in-depth content. and if you want to hear more about this, please, follow our tech policy issues at Tech Tank Newsletter, which is available on the Brookings site, which is accessible at brookings.edu. Your feedback matters to us about the substance of this episode and others. So please leave a comment, share it. Let us know your thoughts. Suggest other topics you'd like for us to discuss in future episodes. This concludes another insightful segment of the Tech Tank podcast. We make bits into palatable bites. Until next time, thank you for listening.

Thank you for listening to Tech Tank, a series of round table discussions and interviews with technology experts and policy makers. For more conversations like this, subscribe to the podcast and sign up to receive the Tech Tank newsletter for more research and analysis from the Center for Technology Innovation at Brookings.