THE BROOKINGS INSTITUTION

After Snowden—surveillance, protecting privacy, and reforming the NSA

September 22, 2017

CONTRIBUTORS:

HOST:

FRED DEWS

BILL FINAN

TIMOTHY EDGAR

Author, “Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA”

ROBIN LEWIS

Associate Fellow, Governance Studies,

Center for Technology Innovation

DAVID WESSEL

Director, the Hutchins Center on Fiscal and Monetary Policy

Senior Fellow, Economic Studies

(MUSIC)

DEWS: Welcome to the Brookings Cafeteria, a podcast about ideas and the experts who have them. I'm Fred Dews.

In 2013, Edward Snowden revealed thousands of classified documents from the National Security Agency to U.S. journalists, revealing that Agency's domestic surveillance and data collection activities. The news coverage and outcry raised significant civil liberties concerns and renewed interest in the rules that govern these activities.

On today's show, a discussion about Snowden and mass surveillance with Tim Edgar, a former ACLU lawyer, former deputy for civil liberties and the Office of the Director of National Intelligence, and former National Security Council adviser on cyber security policy. Edgar is now a senior fellow at the Watson Institute for International and Public Affairs. He is the author of a new Brookings Institution Press book "Beyond Snowden: Privacy, mass surveillance, and the struggle to reform the NSA."

After the interview, you'll hear another installment of Wessell's economic update in which David Wessel looks at one of Donald Trump's really big decisions whether to keep Janet Yellen on as Fed chair or who might replace her.

And then Robin Lewis talks about her research on financial and digital inclusion around the world. It's a big show, so let's get started. Here's my colleague Bill Finan, director of the Brookings Institution Press, and his conversation with Tim Edgar, author of "Beyond Snowden."

FINAN: Thanks Fred for that introduction, and Tim, welcome.

EDGAR: Thanks, It's great to be here.

FINAN: Your new book is called "Beyond Snowden," and it's also a story of your journey through the national security apparatus so a lot of it is about you, can you tell us what drove you to write this book?

EDGAR: I really wanted to shed some light on these issues of mass surveillance and privacy. We've had a huge global debate about them ever since 2013 when

Snowden revealed some of the deepest secrets of the NSA, how they collect up huge amounts of data and communications, and we've also learned a lot about the rules that govern them. And this is really what I've been doing since 2001, since I started as a lawyer at the ACLU.

And so my journey was pretty unique. I went from the ACLU as a lawyer working on surveillance and privacy issues after 9/11 in their Washington office to go inside what's now called the deep state our growing surveillance apparatus. And I did that in the late part of the Bush administration when we were first starting to learn about some of the changes that had been made to our surveillance programs.

FINAN: And that's the George W. Bush administration.

EDGAR: That's right, there was a reorganization of the intelligence community recommended by the 9/11 Commission and that included for the first time a privacy office. There was an understanding that with the threat of terrorism and the possibility of collecting much more information about Americans that we needed to pay more attention to privacy issues. When I went inside I really had no idea the extent to which our laws were out of date–that they didn't really protect our privacy. They were designed in the 1970s based on ideas and distinctions that really don't matter a whole lot today or matter a lot less than they used to.

FINAN: And your journey continued through the Obama administration?

EDGAR: That's right, so when Obama came into office I felt like "we're going to have a fresh start on issues of surveillance." I mean, George W. Bush we had a warrantless wiretapping program with the NSA, a lot of talk about.

FINAN: That's the National Security Agency.

EDGAR: That's right, that's the agency that scoops up so much of the world's communications. And with Obama he had promised to review those surveillance programs on the campaign trail, but if you looked closely at what he was saying you'd see the what his main concern was was not the surveillance itself and the privacy

questions there, but checks and balances wanting to bring in Congress and the courts to serve their proper role in overseeing surveillance.

And what he discovered when he arrived in 2009 when I went to the White House is that actually a lot of that had already happened that we in the Bush administration had put many of these programs, that started as deep secret programs pushed by Dick Cheney, that we had taken those programs and put them under the authority of the Foreign Intelligence Surveillance Court which is this secret court that sits in Washington and reviews intelligence surveillance. So much of the things that Obama criticized you know we're no longer really very relevant and then he kind of sat around and didn't do much to reform surveillance for the next five years.

FINAN: Let's take a moment just sort of pull back and use the term "mass surveillance" and you mentioned the National Security Agency. Can you explain exactly what you mean by mass surveillance?

EDGAR: So, I think it's important to understand when I say mass surveillance I'm talking about the scale of surveillance programs. There is a very specific term that the NSA uses called "bulk collection," and that's a technical term, it means that we're collecting all of the communications or data in a database or going across a wire without discriminating at all. It's literally indiscriminate surveillance. That's bulk collection, we collect everything. Mass surveillance to me is a broader, less technical term that captures the fear and the reality that so much data is being sucked up in large scale surveillance programs that's run by the U.S. government. That's what Snowden really was revealing in 2013.

And so some of those programs might be targeted from the point of view of the NSA analyst who has to come up with a target and put it into a system that retrieves those communications. But from the point of view of society as a whole, if we're talking about hundreds of thousands of communications like we are with this new law that Congress is reviewing this fall, than I suggest that just on a matter of scale alone that qualifies as mass surveillance.

FINAN: And we are talking about this in reference to something else a moment ago, but what is the legal basis for this electronic panopticon?

EDGAR: Well you've got different laws that depend on really where you acquire the data, who you're targeting, what kind of data it is, and many of these are very counter-intuitive and arbitrary.

One of things I wanted to do in the book is to help ordinary readers understand why these matters so much. And the reason they matter so much is because they matter to the agencies, they matter to the lawyers, but they may not make a whole lot of sense. And so that's kind of a difficult thing to understand sometimes, and I think it's absolutely crucial to understand the issue.

I'll give you an example of that. If I'm collecting data inside the United States and its content of communications I'm probably going to have to go get a court order to do that under federal law. I'm collecting the same kind of data, but I'm doing it with a partner overseas, even though there may be just as many Americans in those communications or just as few, I'm not going to have to get a court order. I'm to be able to do that under an executive order that just is the president's own authority.

That doesn't make a whole lot of sense to people but that is what the law says. Another example you know when you're talking about the content of communications that has some pretty significant legal protections at least when you're talking about domestic content. When you're talking about meta-data, that's the phone numbers that you dial, or the e-mail addresses that are at the top of your e-mail, that has much less protection. And when you put all this together, and I talk about this in the book, I talk about how this really does a terrible job of protecting our privacy in the 21st century. It may have made some kind of sense in the analog era, back when we had rotary telephones and no Internet, but today so much of our lives are online our lives, are often much more global. We meet more people from foreign countries, we travel more often, and we use the Internet, and we can you know have people from all over the world that we're corresponding with, and yet we still treat that as some sort of exotic international communication that doesn't get the same kind of protection that our domestic communications get.

FINAN: Your job in government after you left the ACLU was to oversee, in a sense, civil liberties aspects of mass surveillance—I think I have that right although it sounds a little bit oxymoronic—.

EDGAR: It is. I mean in a real sense my job was very much oxymoronic. You know a civil liberties and privacy officer for an intelligence community, the world's most intrusive intelligence community, was in some ways the definition of an oxymoronic job and that was the thing that I thought was so interesting about it was to figure out is there a way that we can get the benefits and value of some of these mass surveillance programs while still providing protections for civil liberties and privacy and it's a struggle.

FINAN: What have been some of the benefits and values?

EDGAR: Let me give you an example of what happened after the Snowden revelations there was a board called the Privacy and Civil Liberties Oversight Board. They conducted two reviews. One was of a bulk collection program involving all the telephone records in the United States, very intrusive, and they looked carefully at the examples that the government had been using to justify that program.

And they said, you know, we looked at your examples and yes you did thwart some terrorist incidents, but you didn't get a unique value from this program you already had this data, the FBI, other agencies had been able to get this data without having to collect everyone's telephone records. They looked at a different program, one involving looking at Internet communications primarily over the world, and they said you know we looked at your examples and you know you provided really unique value, you stopped terrorist attacks, you uncovered and thwarted the plot.

So there's clearly value to intelligence, and the question is, is the value worth the cost in privacy? And the only way to look at that, I say, is to first look at that value and we have too often failed to ask those questions.

FINAN: I once attended a talk by some of the women who formed a posse within the CIA to track down bin Laden after 9/11, and I remember to a person all of them argued that data that the government surveys and collects is far less personally problematic for individual citizens than the data that's collected by Google or Facebook,

and that their surveillance as it were is far more invasive and pervasive. How would you respond to that?

EDGAR: To an extent that's true, because Google and Facebook have so few rules that govern how they use our personal data whereas the government is overlaid with all sorts of rules starting with the Constitution, Federal laws, like the surveillance laws we've been talking about. The difference of course is that Google doesn't have an army of drones that can kill people. Google doesn't have the ability to prosecute people and put them in jail. Google doesn't impose economic sanctions on people. So, these risks to government's surveillance of abuse are much, much greater than they are even with powerful companies like Google or Facebook.

FINAN: The book brings Edward Snowden into it not only from the title but also its part of your story. Can you explain a little bit how your story parallels Edward Snowden?

EDGAR: Sure. I really joined the intelligence community around the same time he did. I left around the same time as he did. I never met him, but in many ways I was supposed to play that role, I was supposed to be sort of the official "Snowden" inside the government—the oxymoronic position of being a privacy advocate inside the intelligence community. And I tried to do my best to spot what the best ways of protecting privacy were, but part of the reason I wrote the book also is as a reflection on how little in some ways I was able to accomplish and how much Snowden accomplished. Through his clearly reckless and criminal action of leaking he sparked a massive conversation about privacy and that, that really is an indictment I would say of the intelligence establishment and to some degree of me as well because it showed that that system needed that shock to have these kinds of conversations and to have the reforms that we've had in the past three years.

I haven't talked so much about the reforms but there have been really substantial reforms to intelligence since 2013. I would say greater than any we've seen since the 1970s.

FINAN: In terms of safeguarding civil liberties?

EDGAR: Yes. You know for years we were arguing about the Patriot Act, with when I was in the government and when I was at the ACLU, but it wasn't until 2015 that Congress actually changed the Patriot Act to end this bulk collection of telephone records program, that was in the Freedom Act.

There has been an enormous amount of transparency the government has released thousands of pages of documents shedding new light on surveillance, making this book possible. This book could never have been written before Snowden because those programs were highly classified. I couldn't talk about them and now I can. The government has been forced to reveal more about what it does.

And then, I would say the biggest change is that in response to some pressure from foreign governments and from American technology companies like Google and Facebook, President Obama has extended privacy protections for non-citizens. First time ever in any kind of intelligence collection programs that we've had privacy protections that don't care about whether you're an American or a foreigner. And this is the Presidential Policy Directive 28. It doesn't quite follow trippingly off the tongue but it's a major shift in the way the intelligence community thinks about privacy.

FINAN: When I've mentioned to people, especially those who hold security clearances, that one of the arguments you make in the book too is that Snowden should be pardoned the first response I get is almost visceral anger that anyone to even suggest this. Have you you've encountered that too, I'm sure?

EDGAR: I think it's a very tough call. I'm not one who thinks that Snowden was a hero and whistleblower in an uncomplicated way, but I do think that it's clear that his disclosures jolted the intelligence community out of a sense of complacency, force needed reforms, very significant reforms, and that many of these reforms actually strengthened the intelligence community, made our country safer by giving our intelligence programs a stronger basis in law in some cases greater access to necessary data. And in fact that may not have been entirely what he wanted to accomplish but it's what happened as a result. And my sense was that we're in sort of this war between you know those who view the United States as, you know, just the world's chief spy and as a threat to the Internet, and the U.S. which is trying to adapt to

new threats. And that Edward Snowden in some ways is kind of a rebel in this battle and given the results that happened it seemed to me that prosecuting him made very little sense. It just wasn't in the national interest. You know we've had earlier examples of presidential pardons, you know the famous example of Ford pardoning Richard Nixon, of Jimmy Carter pardoning the draft dodgers in Vietnam, and it seems to me this is a similar case. Where having Snowden living in Russia, you know saying “I'm the champion of freedom against the United States” was certainly not in our interest and it would be much better to simply say “OK you're certainly not going to come work and hold a security clearance again, but there are benefits that have resulted from the disclosures that you made.”

So one thing that Snowden's critics often talk about is well he should have made his concerns known through the system rather than by leaking classified information. And I can say from firsthand experience, no he really couldn't. These concerns were broad concerns about the building of a mass surveillance state. I was raising these issues for years inside the government and we made some progress on them.

But it's very clear to me that without having leaked that information to a number of very good journalists who could put it into some kind of perspective Snowden's impact would have been absolutely nil. And so to me that's an indictment of the system. Not so much a question of does it respond to whistleblowers, but does it respond to a need to change from the inside. And the answer is not as much as it needed to. I worked on the inside trying to change that system and it's difficult to do so when you're in a culture of secrecy.

So, that's one of my main reasons I think for signing onto the letter urging a pardon for Edward Snowden, is that I just think that the system produced him made it necessary for Snowden to come along to create this conversation about privacy and the reforms that we've had, and that as a result the system sort of didn't have clean hands to go after him and the way that you would for many other kinds of lawbreakers.

FINAN: And throughout the book you come back to that problem that you encountered of not being able to speak to the system and whether you should have said something yourself as a conflict that tells you that those early chapters.

EDGAR: That's right. And I think one reason is simply that when you're in that system the reality that you're up against is you're only going to be able to make very incremental and modest changes. And you know without having that broader national or global conversation those broader changes just can't happen. And that's why one of the major reforms I think that we need to make to surveillance is transparency. And we've gone a significant way towards a more transparent conversation about surveillance over the last several years and Snowden was a huge part of that. And I think that's the benefit that he provided, not only to the critics of the surveillance state, but actually to the surveillance state itself. It needs this criticism in order to adapt and in order to do its important function of collecting intelligence while maintaining the support of a democratic people.

FINAN: What is the likelihood of a pardon today?

EDGAR: Well less than zero. Trump's CIA director has said on the record as a congressman that he believed Mr. Snowden should be executed, and others who championed him want to put him, in fact have put him, on a pedestal. I talk about in the book a sort of an activist public art display of Snowden's head on the top of a pedestal in a public park. I think the truth is somewhere in between these two. And my main feeling about the pardon was really just that when people that I knew and respected in the intelligence community would say, you know I'm kind of glad that this happened because it allowed us to improve some of our intelligence programs, it allowed us to have this conversation about privacy, It strengthened some of our oversight and privacy protections, and at the same time, well let's go put him in jail, it just didn't seem to make sense to me.

FINAN: One of the things that came up in the book for me and that's fully discussed in a chapter entitled “libertarian panic,” is that the people you worked with or observed in NSA and the so-called “deep state” were principled people, people who weren't looking to violate the law that, they took it as a matter of personal pride and personal principle not to violate the law, but with the advent of the Trump administration your concern and the concern of others is that they would be pushed to do that.

EDGAR: That's right, and when a clever lawyer can exploit ambiguities in the law, we've talked a little bit about how complex it can be, but in the hands of someone who doesn't respect basic constitutional values this mass surveillance apparatus that the United States has established is a very, very dangerous thing. And you know really we're just sort of hoping, in the words of Edward Snowden, someday a tyrant is going to be elected a new president will be elected and they'll flip the switch and we'll end up with using this for tyrannical purposes.

And I kind of don't like the fact that our position right now is well let's sort of hope that Trump doesn't find the switch, and maybe hasn't found it yet, but he might. And the lawyers that could be persuaded, ideological and zealous lawyers, to try to exploit those ambiguities to further open the gates to domestic surveillance of groups for example like black lives matter or other groups that are demonized on the right as somehow having connections to radicals overseas. The Muslim community I think is particularly susceptible to this kind of danger.

At the same time I think there's a danger of an overreaction by the deep state. And I talk about that. In the first few months of the Trump administration, we saw an extraordinary avalanche of leaks of not just classified information, but of surveillance transcripts of Americans talking to NSA or other government surveillance targets. Those were constitutionally protected communications, and even if the surveillance is legal, it's certainly not legal to leak it. Those protections exist to help protect the constitutional rights of Americans who are talking and yet that behavior seem to have been normalized somehow by those who felt that they were resisting the Trump administration. So I think the danger could come from not just the Trump administration himself, but also from those who are resisting the Trump administration.

EDGAR: I've said many times that I think the danger of abuse of surveillance power in 2017 is probably higher than it's ever been despite these reforms that I'm talking about. I think that we have a lot farther to go to get surveillance under control.

FINAN: Tim I'm going to leave it there with that note a concern, thanks for coming by today to talk about your new book “Beyond Snowden.”

EDGAR: Thank you very much.

DEWS: You can learn more about, and purchase the book on our website Brookings.edu/Beyond-Snowden. Up next, Wessell's economic update. But before hearing from David, I want to introduce a new concept for the Brookings cafeteria.

I talk to a lot of experts about a wide range of public policy challenges and solutions, but I'd like to hear your story, how the topics I discuss with experts in the studio are present in your life. If you have a story send me an email, or better yet an audio recording. I'm at BCP@Brookings.edu. I'd love to hear from him. And now here's Dave.

WESSEL: I'm David Wessel and this is my economic update. Donald Trump may have trouble getting his tax and spending proposals through Congress but he has an opportunity, an unusual one, to significantly reshape the other major player in economic policy, the Federal Reserve. The Fed of course sets the interest rates, they influence the rates we pay on car loans and mortgages, the rates that businesses pay to borrow, the direction of the stock market, and the value of the U.S. dollar. And the Fed is the first responder in the event of a recession or a financial crisis of some sort.

At full strength the Federal Reserve Board in Washington has seven members. Today there are only four, and one of them will leave in October. That gives Mr. Trump four slots to fill. So far he's nominated only one person, Randy Quarles, a Bush Treasury official and former finance executive who is awaiting Senate confirmation. But the really big decision facing Mr. Trump is whether to reappoint or replace Janet Yellen whose term as Fed chair ends February 3rd 2018.

Along with picking someone for the Supreme Court, picking a Fed chair is probably the most consequential personnel decision any president makes. Although major Fed decisions are made by a committee, the Fed chair is more than just one vote. He or she sets the agenda commands one of the world's largest armies of economists and moves financial markets with almost every adverb or adjective uttered in public.

Now it's hard to predict to whom Mr. Trump will turn to run the Fed, heck it's hard to predict what Mr. Trump will do on almost anything, one thing seems nearly certain to

me though, Mr. Trump would prefer a Fed chair who leans towards lower interest rates. Real estate developers and presidents almost always do.

Now for a while Gary Cohen, the former Goldman Sachs executive who heads the White House National Economic Council, was said to be the leading choice. But his shares have fallen after the president was reportedly displeased by what Mr. Cohen had to say about the president's reaction to the events in Charlottesville.

That's boosted the chances that Mr. Trump may turn to Kevin Warsh, a former Bush White House official and Fed governor, who is quietly campaigning for the job. But as the Economist magazine put it recently, quote “Mr. Walsh has skills at making friends seem stronger than his monetary policy acumen.” Other contenders include Glenn Hubbard, another former Bush aide and now dean of Columbia Business School, John Taylor, the Stanford economist who also did a turn in the Bush administration, though both of them probably would push interest rates up faster than the Fed has been pushing them.

Also mention in the Washington whispering and the market speculation, are former commercial banker John Alison, Larry Lindsey and other former Fed governor, and perhaps Neel Kashkari the ambitious president of the Minneapolis Fed. In an ordinary administration, the president would announce his pick in September or October so the Senate has time to hold hearings and a confirmation vote long before Janet Yellen term is up in February. But this is no ordinary administration, so this could drag on for a while. And that has boosted the odds that Mr. Trump in the end will nominating Janet Yellen for a second four year term.

On one hand that wouldn't be a huge surprise, every president since Ronald Reagan has reappointed his predecessor's choice for Fed chair. There's something to be said for continuity at the Fed, and as Mr. Trump himself has observed Janet Yellen is a low interest rate person.

On the other hand, unlike some Trump appointees and Republicans in Congress, Janet Yellen has made very clear that she opposes undoing the tougher financial rules that were put in place after the financial crisis. And reappointing President Obama's pick

for Fed chair would surely further antagonize many Republicans in Congress. Though she'd probably get all 48 Democrats in the Senate and enough Republicans to get through.

This is a big call for the president, it’s one that matters for all of us, and we should know soon what he's going to do.

DEWS: You can listen to more Wessell’s economic updates on our soundcloud channel.

Finally today, financial and digital inclusion around the world. About two billion adults worldwide do not have a bank account or other access to a formal financial institution. Robin Lewis, research analyst and associate fellow in the Center for Technology Innovation at Brookings, discusses her new report with Darrell West and John Villasenor on financial and digital inclusion.

LEWIS: About 2 billion adults around the world do not have an account with a bank or other formal financial institution according to the World Bank's Global Finance Database. Being excluded from the formal financial ecosystem can make it much more difficult for individuals to save for the future, pay their bills, and generally invest in their family's financial health and well-being.

My name is Robin Lewis and I am a research analyst and associate fellow in the Center for Technology Innovation in Governance Studies program at Brookings. Along with John Villasenor and Darrell West, I am a co-author of the Brookings Financial and Digital Inclusion Project report which we just released at Brookings.edu.

Beyond advancing individual welfare, financial inclusion is also a key ingredient in advancing sustainable development goals such as poverty reduction and gender equity. This is why the Brookings financial and digital inclusion project, or FDIP, has spent the past three years examining how different countries around the world are making strides toward financial inclusion which refers to access to and usage of quality affordable financial services.

The objective of our project is to provide policymakers, private sector representatives, non-governmental organizations, and the general public with information that can help improve financial inclusion in the FDIP focused countries and around the world. So to help achieve this objective we examined twenty six diverse countries and a series of annual reports and score cards.

The score card assesses countries across four dimensions of financial inclusion including country commitments, mobile capacity, regulatory environment, and actual adoption rates of selected traditional and digital financial services. So what exactly do we mean by digital financial services? Some examples include services that are very familiar to many consumers in the U.S. including debit and credit card usage. Others like mobile money might be less familiar.

When we talk about mobile money, we are referring to financial services accessed using a mobile phone independent of whether or not the customer has an account with the form of financial institution like a bank. In many places, especially those with limited banking infrastructure, mobile money can be transformative since mobile phones are much more widely accessible than traditional financial institutions. For example, in 2016 the GSA, a trade body that represents the interest of mobile operators worldwide, found that 30 countries have 10 times more active mobile money agents than bank branches. This brings formal financial services within reach of millions of previously under-served households.

According to the GSA, sub-Saharan Africa has led the world in the number of active mobile money accounts over the past decade with Kenya being a particular standout. Kenya has robust rates of mobile money adoption, especially among traditionally underserved groups, helped propel it to the top of the FDIP score card for the third year in a row.

The other top performing countries on the 2017 score card were very regionally diverse. And looking beyond the score card, we highlighted three key overall findings from our research.

First, we found that there has been considerable growth across our 26 countries, and recognition that financial inclusion is not just important for individual's welfare, but it can also contribute to macro economic growth and sustainable development goals. For example, for the first time in the history of the project all of our focus countries are members of financial inclusion oriented networks such as the Alliance for Financial Inclusion. With that said, while countries participation in these groups is important it is crucial that these memberships translate into action.

This is why we urge countries to establish clear measurable financial inclusion goals and where possible, consistently provide detailed, publicly available data to help track progress toward their goals.

Our second finding is that FINTECH, which the World Economic Forum describes as the innovative use of technology to design and deliver financial services and products, provides tremendous opportunities to accelerate progress toward financial inclusion. Using technology well can enhance the accessibility and utility of financial services for customers and make these services more cost effective for providers.

Countries like Indonesia and South Africa have worked to develop guidelines and regulatory frameworks for FINTECH. And creating regulatory sandboxes can also allow innovators to test their products and business models in a supportive and secure environment.

Our third key finding is that countries must amplify investments in cybersecurity to fully reap the benefits of these innovative services. After all, many of the newer players in the financial ecosystem may not have the resources infrastructure or experience to ensure that these services are secure.

Banks are also not exempt from cyber security threats, particularly when they have outdated or centralized systems. So we encourage all financial service providers, and other entities that has financial data, to invest in bolstering the security of their systems. Policymakers, regulators, and financial service providers should amplify

discussions surrounding these issues and coordinate with technical experts in order to develop a menu of options and technical assistance for advancing cybersecurity.

Overall, tremendous progress has been made, and we hope that the report and scorecard provide useful pathways and examples for anyone hoping to further improve financial inclusion in any of our 26 focus countries and around the world. You can find the report and scorecard online at Brookings.edu.

DEWS: The report is on our website, and also you can download and listen to a recent episode of the Intersections podcast featuring a discussion between Camille Busette and Darrell West about financial inclusion in the U.S. and abroad.

And that does it for this edition of The Brookings Cafeteria brought to you by the Brookings Podcast Network. Follow us on Twitter @policypodcasts. My thanks to audio engineer and producer Gaston Reboredo with assistance from Mark Hoelscher.

Thanks to Brennan Hoban and Chris McKenna for production assistance. Bill Finan does the book interviews. Our interns or Pamela Berman and Julian Chong. Design and web support comes from Jessica Pavone, Eric Abalahin, and Rebecca Vizer. And finally, thanks to David Nasser for his support.

You can subscribe to the Brookings Cafeteria on Apple podcasts or wherever you get podcasts, and listen to it in all the usual places. Visit us online at Brookings.edu. Until next time, I'm Fred Dews.