U.S. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

PUBLIC FORUM: DEBANKING AND THE RISKS TO PRIVACY AND CIVIL LIBERTIES

TUESDAY, DECEMBER 2, 2025

PARTICIPANTS

BETH A. WILLIAMS

Board Member

SAM BROWNBACK

Ambassador

LARRY ROTHENBERG

Board Moderator

ALEXANDRA HARRISON GAISER

Alliance Defending Freedom

DAVID IBSEN

Americans for Free Markets

ANIL KASHYAP

Stevens Distinguished Service Professor of Economics and Finance

Booth School of Business

University of Chicago

PROCEEDINGS

MS. WILLIAMS: Good morning. My name is Beth Williams, and I'm a Board member at the Privacy and Civil Liberties Oversight Board. I'm delighted to welcome you to today's public forum on Debanking and the Risks to Privacy and Civil Liberties. The PLCOB is an agency that was established in its current form by the 9/11 Commission Act of 2007.

The agency's mission is to ensure that the Federal Government's efforts to prevent terrorism are balanced with the need to protect Americans' privacy and civil liberties. Our forum today will examine how financial tools used by the government to fight terrorism may impact Americans' privacy and freedom.

Specifically, the forum will examine concerns that financial institutions may be encouraged to engage in the practice of debanking, which may deny financial services to certain individuals and organizations. And it will discuss the impact of President Trump's recent executive order guaranteeing fair banking to all Americans.

Especially since the terrorist attack of September 11, 2001, the flow of information between financial

institutions and the government has enabled intelligence analysis that has been used to identify, disrupt and prosecute terrorist networks. But some have argued that the growth of government power in this area has extended beyond counterterrorism, and that persons have been unfairly targeted for political or religious reasons.

This morning, our panel will discuss how the current system functions from both a national security and a privacy and civil liberties perspective. Panelists will offer their insights on the consideration of reputational risk and the impact that such considerations may have on the provision of needed financial services.

I'd like to express my gratitude to Ambassador Sam Brownback for delivering today's keynote. I also want to thank our three panelists, Dr. Anil Kashyap from the University of Chicago; Alexandra Gaiser from Alliance Defending Freedom; and David Ibsen from Americans for Free Markets, and formerly the executive director of the Counter Extremism Project for taking part in this conversation. Finally, I'd like to thank members of the public who have taken the time to share their thoughts on this issue with our agency.

With that, my great pleasure to introduce our

distinguished keynote speaker, Ambassador Sam Brownback. Mr. Brownback served as Ambassador-at-large for International Religious Freedom from February 2018 to January 2021. He served as governor of Kansas from 2011 to 2018.

Prior to that, he represented his home state of Kansas in the United States Senate and the House of Representatives. While a member of the Senate, he worked actively on the issue of religious freedom in multiple countries, and he was a key sponsor of the International Religious Freedom Act of 1998.

Ambassador Brownback currently serves as co-chair of the International Religious Freedom Summit and chairman of the National Committee for Religious Freedom. He has been an important public voice on the issue of debanking. Ambassador Brownback, welcome.

MR. BROWNBACK: Thank you very much, Beth. That's kind of you to introduce me and that wonderful introduction. And thank you all very much for being on this and your interest in this topic and your hosting of this event as well.

I think this is a serious topic, and it's one that

we really need to talk about and really need to delve into greatly. I was in the U.S. Senate on 9/11. I was there in the aftermath when we were looking at how did we get attacked and why didn't we do better at stopping this.

And that then proliferated a series of government tools, and of kind of breaking down of silos so that we could have better communications back and forth. And those were put in place, but there was also cautions mentioned at that time saying, "Could we be going too far? We want to protect civil liberties. We want to protect people's privacy rights."

Those were always in the discussion and balance, and so, I'm delighted that we're talking about this here now, because I think particularly in the area of debanking, my experience and the experience of a number of people who I've talked to after we went public with our debanking has shown that there's a problem here, and it shouldn't be that way.

Our issue started out, and I'll briefly describe it. In 2022, we had started this organization called the National Committee for Religious Freedom. I'd worked a lot on religious freedom issues externally, internationally, across the world.

And I start seeing more and more problems arising domestically, where there was more of an effort to not put people into jail, but to suffocate people that had traditional sets of values, is typically what the category would end up being in.

And so we formed this organization called the National Committee for Religious Freedom to stand up for religious freedom in the United States, and for people, again, as I say, that normally carry a traditional set of values that may be out of step with the current cultural issues and mood.

Formed that organization. We opened a bank account in Washington, D.C., at Chase Bank. We did it on April 15th of 2022, which may have been my sign that that was the wrong day to do it on, but we did.

And then, it's about 39 days, 40 days later, I go to put a deposit in an account in Kansas City in Chase Bank that the lady behind the counter told me, "I'm sorry, that account has been closed. It says here on the computer, it was closed at corporate. It is a nonrevocable decision. And that's all I'm supposed to say."

And I was stunned. I didn't know why did this happen to us. Fortunately, the executive director of the

organization we had had previously worked at Chase Bank at very low level, but had worked there, so he knew kind of the systems and the processes, and so we started inquiring of Chase Bank why this happened.

Now, we easily could have gone and found another bank, and we did go and find another bank. Bank of America took us, and we haven't had a problem since then. It was a 501(c)(4) organization, not a (c)(3). And some people, well, maybe they didn't really particularly care for that issue. But we started pursuing this, why did this happen to us?

And we went public with it as well, because a number of other people, when this happened to them, they just went quietly. They thought it would hurt the fundraising efforts of their organization if they were involved in some sort of public controversy.

But that it was the very reason we had formed the National Committee for Religious Freedom was to stop things like this from happening and then it happens to us. It was interesting too to me at that time that as we went public with that we had been debanked, I had somewhere between a dozen and 20 different organizations, most of them kind of faith affiliated organizations, contact me saying this had

happened to them as well, and they had just gone and found another bank and moved on.

But I said, "No. In this country that should not happen to you." So we started pursuing it with Chase. And we ended up bouncing up the chain of command to some degree. We bounced into their lobbying organization. We contacted them and we ended up getting five different reasons ultimately at different times.

One was we didn't fill all the forms out that they asked for. And I said, "Well, why didn't you give us time or notification of forms we didn't have? And why did you end us early from even the 60-day period that you normally give to people?"

And then they said, "Well, okay, it was sloppy customer service. It was just bad customer service." And I said, "Well, okay, what do we do from this point?" And it was kind of nothing. "We're not going to reinstate you." They said, "Well, we might consider reinstating you if you divulge all the people that are contributing to your organization and who you planned on funding."

I said, "Well, we don't have to give that kind of information out." And then they said, "Well, we're concerned about money laundering and terrorist financing,"

which I said, "You know, I've had top secret clearance for 20 years. I don't think I'm a risk for those types of items or things happening."

And then they said, "Well, we're concerned because you're a politically exposed person." And we looked that up, and that applied to people that were elected that were foreign officials. I said "I'm no longer elected at this point in time and I'm not a foreign official."

So -- and then we even took it to a shareholder issue was brought up. We lost on the shareholder just asking for an audit internally of Chase Bank saying, "How did this happen, and how do you stop it from happening in the future?" That was we lost the shareholder resolution. I still think Chase should do that.

I still have a question as to why did this happen? How did it happen? And can you put systems in place so this doesn't happen in the future? Which brings us to where we are today in President Trump's executive order. And my hope is that we won't see groups or movements that are out of step with the culture get debanked, deinsuranced.

What I'm seeing now, because we now hold a monthly meeting of the National Council for Religious Freedom, a

501(c)(3) organization, we hold monthly meetings with this group, and we constantly are hearing groups saying, "Yeah, the Community Foundation won't fund groups like us, or we've got deinsurance, we've got debanked."

We're not hearing as much about the debanking now as these other areas to suffocate people that are out of step with current movements or ideas within the culture. This is a serious issue because in this country, you want to solidly protect that First Amendment right to free exercise of religion, of people of faith.

It's often people of faith who are out of step with the culture, but can act as a conscience, can act as somebody that holds a different point of view that other people can look and see at in this dynamic culture that we have. And I think that's an extraordinary help.

I think we're much better off as a nation that you have Amish who may look at education in a different way, that we have Orthodox Jews that have their practices. I think we're enriched as a nation, and it clearly, clearly is a foundational principle in democracies that people can do with their own soul what they see fit. We may not agree with each other on what you choose to do, and that's okay.

You have a right to, as long as you're peaceful at

it, to do with your own soul what you see fit. And this is foundational to the United States. It's foundational to a free democracy. And those rights need to be protected, and they need to be protected in public and in private. They need to be protected in statute, in regulation, and in practice.

And that's why I think this is an important hearing that we delve into how that free exercise right is protected and continues to be protected, even with concerns about terrorism and other issues that may come up.

Beth, others, thank you again for hosting this. I'm delighted to be able to join you.

MS. WILLIAMS: Thank you so much for your remarks, Mr. Ambassador. We're very grateful that you were able to join us and share your perspective with us and your story.

With that, I'll turn this over to today's moderator, my counselor, Larry Rothenberg.

MR. ROTHENBERG: Thank you, Member Williams. And again, thank you, Ambassador Brownback. I think you really set the stage for what our three panelists are going to discuss and really dig into the details on. Before we

start the panel, I'll give a little bit more of an introduction to each one of them.

First, we have Ms. Alexandra Gaiser. She's currently the senior counsel at the Alliance Defending Freedom, an organization focused on the protection of religious liberties. She's a former general counsel at Strive Asset Management, was head of regulatory affairs at River Financial, and was an associate at the law firm Akin Gump.

She also worked at the treasury department under former Secretary Mnuchin during the first Trump administration as the department's executive secretary.

Next, we have David Ibsen. Mr. Ibsen is the executive director of Americans for Free Markets, a coalition of business and community groups working in support of free markets and economic growth. He has two decades of experience in national security, diplomacy, and nonprofit management.

Prior to joining Americans for Free Markets, he was the executive director of the Counter Extremism Project as well as president of United Against Nuclear Iran. He previously served as a policy analyst for the State Department and an advisor at the United Nations.

And third, we have Dr. Anil Kashyap. He is the Stevens Distinguished Service Professor of Economics and Finance at the Booth School of Business at the University of Chicago. And his research focuses on among other things, financial regulation and monetary policy.

He is the co-founder of the U.S. Monetary Policy Forum, which is the leading private sector conference on U.S. Monetary Policy. He is also a research associate for the National Bureau of Economic Research, and a fellow at the Center for Economic Policy Research, and he is also the co-director of the Chicago Booth Kent A. Clark Center on Global Markets.

Thank you all for being here today. We have an excellent panel of real experts on this subject, and each one will deliver a short opening statement. If we can please start with Alexandra.

MS. GAISER: Well, thank you so much for having me. And it's a real pleasure to be with you all today. And I appreciate, of course, the Board's work in examining the civil liberties implications of financial regulatory practices.

I want to begin by affirming that various

government actors do good work combating illicit finance, and I don't intend to diminish the seriousness of that mission. But the same tools that protect us can also be misused, intentionally and otherwise, in ways that carry significant risks for privacy, due process, and the equal treatment of Americans under the law.

I'm here today because of what we see at Alliance Defending Freedom and what I've previously seen in the bitcoin world and at the Treasury Department. Regulatory preferences, combined with vague concepts like reputational risk, have encouraged financial institutions to deny or terminate services for reasons unrelated to actual financial crime.

There is work to be done to protect privacy and civil liberties in the banking and financial services realm. This phenomenon which often starts as derisking and ends in debanking has real human consequences.

Our clients include religious ministries, nonprofit organizations, and individuals who have suddenly lost essential banking relationships with no notice, no explanation, and no avenue for appeal. Some only learned their accounts were closed when their debit cards stopped working. Others had payroll accounts frozen days before

employees needed to be paid.

And nearly all were told simply that the bank no longer wished to maintain the relationship. These are not people engaged in suspicious financial activity or criminal organizations. Instead, they are Christians and conservatives whose beliefs have been deemed by some to be unpopular, controversial or outside the mainstream.

Over the last several years, a bank fearing supervisory scrutiny or criticism from the public or its own employees may have found it safer to cancel them than to serve them. This is not hypothetical. It echoes what happened during Operation Choke Point when certain industries were effectively blacklisted without formal rulemaking or congressional authorization, and Operation Choke Point 2.0, which affected the crypto industry broadly.

Prior to President Trump's executive order, we saw similar chilling effects, but this time affecting religious organizations, nonprofit advocacy groups, and others engaged in constitutionally protected speech and association.

We've heard it both ways that this is something banks are doing sua sponte without regulatory pressure, and

that regulatory pressure including soft pressure, can be a major impetus behind debanking. In either scenario, there are harsh penalties for under compliance with various KYC AML regimes and no penalties for overcompliance.

So, unlike our justice system, which assumes everyone innocent until proven guilty, debanking acts on innuendo, suspicion and assumes everyone is guilty, then takes punitive action, and then because of the sensitivities around illicit finance, fails to provide the affected account holder with sufficient information about the actions taken against them or the reasons why.

A criminal conviction can be appealed. Loss of a bank account typically cannot. That is why transparency, notice, and due process safeguards are critical. Americans should not lose access to the modern economy because of opaque risk models, inaccurate government data, or misinterpretations of regulatory expectations.

My hope is that thanks to the President's executive order and the removal of reputational risk by the financial regulators, debanking will become a thing of the past. While banks may still close accounts, whether for criminal or other reasons, they should inform the account holder why the actions are being taken.

And unless criminal, those closures should occur only because of financial reasons, not First Amendment protected ones. Thank you again for having me. I look forward to your questions.

MR. ROTHENBERG: Thank you very much, Ms. Gaiser. We'll move on to David. Please go ahead.

MR. IBSEN: Thank you very -- thank you very much, Larry, and thanks to the Privacy and Civil Liberties Oversight Board for convening this important discussion. It's a pleasure to be here. As noted in the bio, I currently work for Americans for Free Markets, which is a coalition of groups working for economic growth.

But my background is national security and counterterrorism. So, I have worked with policymakers and law enforcement to strengthen the financial safeguards that keep violent extremist groups, criminal networks, money launderers from exploiting the U.S. banking system.

And so, I'm aware that banks for many decades have been government partners in these efforts through Know Your Customer procedures and the AML anti-money laundering laws stemming from the Bank Secrecy Act of 1970, amongst many

other statutes. Supercharged, so to speak, after 9/11, financial institutions have collected data and intelligence to assist law enforcement in uncovering and suppressing illegal activities.

Over time though, I think, you know, some of these frameworks, so though well-intentioned, have proven to be quite expansive and vigorous enough that lawful customers are having their financial data collected on a large scale. For example, most Americans may be unaware that cash transactions over 10 grand would trigger the creation of a currency transaction report or CTR as filed with the Federal Government.

Suspicious activity reports or SARs are another layer of government scrutiny, which banks have filed millions of just last year. And still other Americans have been driven out of the financial system completely, which is this phenomenon of debanking or government-driven debanking, which occurs when the financial institutions close accounts because regulators or policymakers may deem an industry belief system or ideology to be undesirable at the time or because of overly broad compliance rules, such as anti-money laundering requirements, which can sweep in otherwise lawful customers.

And this precedent of regulatory overreach in financial services traces back to Operation Choke Point 1 (phonetic). Under the Obama administration, regulators exploited the ambiguous concept of reputational risk to pressure banks into denying services to entire categories of lawful businesses from firearms retailers to small dollar lenders.

This practice grew under the previous administration, extended to cryptocurrency firms and certain conservative groups. So financially sound, legally compliant entities were cut off from financial services, often without explanation at great cost and disruption to their business activities.

And so, this reputational risk term was a catch-all that allowed regulators to pressure banks into cutting ties with legal industries. The term is vague, it's subjective. It's impossible really for banks to measure in most cases. So they erred on the side of closing accounts to the detriment of the American people. I think this was a clear abuse of regulatory power.

Financial oversight was used to advance ideological or political agendas aimed at dismantling industries that regulators and supervisory policymakers may

have opposed and inserting ideology into what should be a neutral financial supervision.

I think it's worth emphasizing that banks have various reasons why they might not open an account or keep an account open, including operational expertise and commercial reasons. And banks like any business are allowed or should be allowed to say that they can conduct business with the client if they have a commercial justification and whether it's -- if it's within the law.

The government shouldn't be involved in that decision. So, there has been a politicized -- a highly politicized regulatory environment in the past, which resulted in debanking, which is why it's important that steps are being taken now to ensure accounts are closed -- not closed for political reasons.

So the Trump Administration's executive order from August of this year prohibits the use of reputational risk and bank supervision and directs the Treasury to modernize outdated rules that fuel unnecessary account closures and ensures that regulators will follow objective, reasonable, and apolitical assessments going forward.

As the executive order itself makes clear, it's the policy of the U.S. that no American should be denied

access to financial services because of their constitutionally or statutorily protected beliefs. Banking decisions must instead be made on the basis of individualized, objective, and risk-based analysis.

I do not think this is a controversial assessment or statement. I think it's a principle that makes sense to the vast majority of Americans. So that executive order is a great step. It establishes a precedent, but it does remain vulnerable to reversal by future administrations.

So, you know, I think a national fair access standard going forward that prohibits banks from closing accounts based on political and religious views would help address the undue influence of federal regulators in the future.

A national standard would also eliminate the need for individual state laws that can make it harder for national banks to operate effectively across state lines.

And there is some pending legislation in Congress that would make this EO more permanent going forward, which I'm sure we'll discuss during the Q&A. So this would be a lasting solution so that regulation doesn't slingshot back and forth based on political ideology or who's in political power while letting banks remain free to run their

businesses, use their expertise to evaluate risk like other businesses, and cooperate with law enforcement in a very effective manner that stops high-risk illegal activity without ensnaring law-abiding Americans.

And this will ensure our banking sector remains sound and secure, and also that Americans have the fairest access reasonably possible. I'll stop there. Thank you.

MR. ROTHENBERG: Thank you very much, David. And Anil, please go ahead.

MR. KASHYAP: Yeah, well, thanks. I join everybody else in saying it's great that you're convening this discussion, which I think is important. So before we get into the details of the privacy issues, I thought it might be helpful to remind people how we got here.

And to that, you really do actually have to go back to the Banking Secrecy Act of 1970 that David just mentioned. That act was pitched as a way to combat tax evasion. And from the very get-go, there were privacy concerns that were raised about whether or not banks should be allowed to have this information and how they were going to use it.

One thing that is fascinating is that if you go back and read the initial litigation that was lodged against the BSA, there were Supreme Court decisions that were consistently split decisions, but they weren't split along party lines. There were certain cases where the conservatives objected. There were other cases where the liberals objected.

And the BSA kind of trundled along trying to deal with tax evasion for about 15 years. Then the war on drugs became a national priority in the mid-'80s, and the AML rules were expanded to follow the money in the drug trade. Okay. So that led to incremental expansions over the next 15 years.

We finally get to 9/11, and as everybody's mentioned, the AML rules were widened to add counterterrorism as an objective. And that then was supplanted in the last few years by additional protections or expansion of authority to support the use of sanctions as an AML goal, and now most recently, battling corruption and human trafficking.

So the result of this is if you look at the AML infrastructure, it's a super complicated system. It has multiple aims. It has dozens of enforcement agencies

involved. There hasn't really been a ground-up reconsideration of the whole system and an assessment of whether or not the tools and resources are adequate to achieve the various aims.

One thing that almost nobody talks about is that there's no systematic effort to measure outcomes consistently over time, which means you can't do something like cost-benefit on the AML system because we don't have the numbers that you would need to do that.

Now, the last big piece of legislation was the Anti-Money Laundering Act of 2020. We're just about 5 years past that now. Core parts of it that were supposed to close loopholes that had accumulated over, you know, 30 years have now either been abandoned or delayed. And so there are gaping loopholes in the AML framework right now that have been apparent for 5 years that are going to go unattended.

So I think the current arrangements are probably better than nothing, but there's big questions about the efficacy and whether or not, you know, the system's just grown too big and complex and need to be let go.

So with that perspective, now I think we could talk about some of the more detailed issues, but it's

important to put this in the whole framework. And so let me stop there.

MR. ROTHENBERG: Thank you very much, Anil. I think that was a really helpful background and especially your description of how the aims of the system have grown over time and how its complexity has grown over time.

I would now like to get into some of the details. We've discussed and thrown out some terms like suspicious activity reports, reputational risk, politically exposed persons. I'd like to dig into that a little bit more.

And perhaps, David, you can describe for us how exactly the system, this complex system works. What is a suspicious activity report? How is that used by the government? What are know your customer rules?

And give us a flavor of what happens when somebody who wants to set up a, say, religiously-based nonprofit organization goes to a bank and what scrutiny they might be subject to.

MR. IBSEN: Sure, sure. And I want to join you in thanking Anil for setting up that kind of predicate, because it's important to understand just kind of how vast

this AML architecture and the KYC architecture has become over the past few decades.

Just to, you know, expand on that, you know, just briefly, I mean, we had the Bank Secrecy Act, which was set up, as Anil says, for anti-money laundering purposes and really also to establish a paper trail for law enforcement, which they've continued to expand going forward.

You know, you have the International Emergency Powers Act of '77, the Effective Death Penalty Act, Anti-Terrorism Act of 1996. All these things are allowing the government to kind of increase their designation capabilities and to expand the AML network.

Concurrently, there's been this multilateral network, which has really expanded. And whatever you think about the efficacy or the importance of the UN, in the case of anti-money laundering, anti-terrorism guidelines, there are some statutes that have set a precedent there, including the International Convention for the Suppression of the Funding of Terrorism, 1999, and then UN Security Council Resolution 1373, 2001, which really kind of set the stage for this idea of capacity building, where financial services and treasury departments from various countries kind of almost had an obligation to go around to other

countries and instruct them on how to set similar kind of AML, BSA-relative frameworks.

So -- and then, of course, you know, 9/11, everything that happened there really kind of supercharged the BSA and expanded the use of suspicious activity reports and also increased the obligations on banks, including via civil penalties, for lack of compliance. So just a little more of the kind of the predicate there.

But on the suspicious activity reports, this is, you know, an obligation on the banks to identify not necessarily suspicious persons, but to look at their activities and identify -- and it's all kind of very vague, no one's really quite sure about what the guidelines are, but anything that's out of the ordinary in terms of their financial transactions.

And the thresholds are quite low. This is a problem because it goes back to 1970s. So you have amounts that are over $2,000 or $4,000, depending on the combination of monies or the transfer that's involved. If it's out of the ordinary for somebody, that would trigger a suspicious activity report or a SAR.

And that would be filed by the bank with Treasury Department or with FinCEN. That is interrelated to

customer due diligence and know your customer standards that banks are implementing.

So when you go in, Larry, to answer your question, there's going to be a series of questions when you're opening account, whether it's for a business or an individual or for a nonprofit organization, where they're going to want to know where your funders are coming from, where your lines of credit are coming from, who your vendors are, what are your basic transactions that you're engaged with on a regular basis.

The banks want to know who you are, obviously. That's kind of part of their just derisking strategy. So they obviously want to know, you know, who you are, what your sources of funding are, what your credit worthiness is, what your liquidity risk is, all those different things. So they want to know that anyway.

But this also KYC process sets the baseline for subsequent suspicious activity report filings. So now they know what your business or your nonprofit or your personal finance operation looks like, they have a template from which then to identify suspicious activities, which is what becomes the basis of the SAR.

Now, when these SARs are filed, one thing that was

referenced, I think, in Alexandra and Anil's comments was the confidentiality regime around these suspicious activity reports or SARs. And this leads to a lot of different problems with the public.

So after 9/11, Title III of the Patriot Act expanded the Bank Secrecy Act and the process for filing SARs, which meant that the banks and the financial institutions are prohibited from divulging any information about the SAR, not just what the suspicious activity report contains, but whether or not there's been a SAR filed at all.

So when you hear these stories about people calling the bank in response to having an account closure or a suppressed transaction or a transfer held up, the fact that they're getting these kind of anodyne, very basic responses from the banks is a result of these legal requirements that they have.

Now, if you're a customer who's wondering why what you think is your routine financial activity has been discontinued by an institution that you might have been doing business with for many, many years, and the bank then tells you, "Hey, you know, there's no information, we made a decision based on this," blah, blah, blah, and you ask

follow-ups, you don't get any information, it's human nature to then kind of assume the worst.

So then people start to assume that it's because of my political activity or it's because of what I'm posting online. And this leads to a lot of suspicion towards the banks, and it leaves the groundwork for a lot of confusion about what the bank's obligations are under the law, and it leaves the customer without any recourse to remedy the account closure. So there's a lot of frustration there.

MR. ROTHENBERG: Thank you very much for that. And I think that leads right into my next question for Alexandra. You've represented some folks who this has happened to, and you also worked at the Department of Treasury, so you have kind of a unique view of this.

Can you expand a little bit on the frustrations that your clients have had and what you're doing to investigate and try to figure out how the system that seems to have arisen out of legitimate purposes might have been misapplied or even abused?

MS. GAISER: Sure. So I'll take those in reverse

order. I think what David said about sort of the SARs process is exactly right. And when I was at Treasury, granted almost 5 years ago, it was a pretty open secret that FinCEN was drowning in SARs. There were more –

MR. ROTHENBERG: Sorry. Can you just explain for the audience what FinCEN is?

MS. GAISER: Yes. So FinCEN is the Financial Crimes Enforcement Network. It's a bureau of Treasury, and they are very, very, very good at finding and fighting financial crime. So just like what David talked about, the way that different types of accounts are going to have different expected activity, FinCEN is really good at tracking that, and they're really good at figuring out, hey, wow, this account is doing a lot of small dollar transfers.

That is not normal for this kind of account. What's going on? Are they money laundering? Are they doing some other sort of nefarious business? Let's investigate. So they're excellent at what they do. Part of what they do is they review the suspicious activity reports sent to them not just by banks, but by any FinCEN

regulated financial institution.

So this includes check cashers, money transmitters, mortgage loan originators. I mean, anything that touches money is obligated to send in a suspicious activity report when they see suspicious activity. There, at least, again, at least when I was there, there were more suspicious activity reports than you could ever hope to read.

So there is too much information sloshing around. You've got a lot of noise. And again, FinCEN, to its credit, is pretty good at finding the signal in all that noise. The problem that should concern us is all of this noise is coming from Americans' bank records and their financial activity.

And it is every time you send it, it gets a little less secure. And incredibly, and ironically, often the account holder is the last to know, if they ever know, that their information has been sent. And they probably have the least rights in determining what was said and why, because there is a concern that if you have had a suspicious activity report filed on you, maybe you are under investigation. Maybe you're committing a crime. We're very nervous about tipping off criminals that we're

onto them, which makes sense.

You also have the 314(a) and 314(b) information sharing regimes. These come out of the Patriot Act. 314(a) is mandatory. It's between financial institutions and the government. 314(b), though, is voluntary. Financial institutions can and are encouraged to send each other information about account holders.

So when I worked at River, a bitcoin company, we were not a bank, but we were a regulated money services business. We were a money transmitter. So we could often see our account holder's bank information. If we had to file a SAR on a customer, then there was a question, should you send the SAR information to that customer's bank as a heads up?

This was a real question for us. There were big fraud issues in the industry. If you hit fraud, typically we were on the hook for that. So you wanted to stop fraud and you wanted to ultimately find a payer with deep pockets. But we also really cared about our clients' privacy. We didn't like sharing information with their bank that may be completely innocent.

And so this is sort of the big backdrop to what's been happening in debanking. But our clients here at

Alliance Defending Freedom have a lot of similarities in their stories. They're almost never given notice. Their accounts are typically either frozen or closed. Sometimes that includes the funds in those accounts.

So I think one of our clients got a check for the balance of their account. Oftentimes the financial institution will freeze those funds as well. I believe that happened to Ambassador Brownback. And then when they call, they're usually given a rote response. So let me tell you some of these stories.

Indigenous Advance was a -- is a Memphis-based Christian organization. They do a ton of work with orphans in Uganda. They also support a local church. One day, their account was closed. The bank said, "You no longer fit our risk tolerance." They were long-term clients of the bank.

Timothy 2 was another Christian ministry. They train pastors in over 65 countries in some of the world's poorest countries. They were also told, "You're operating a business type we've chosen not to service." Their account was closed, even though they had held it for about 10 years.

The Idaho Constitution Party, in March of 2024, in

an election year, abruptly had their long-term account closed with no rationale offered other than they got a check for the remaining balance. So again, pretty lucky here. And the local branch would only say, the bank just decided to quit doing business with you. And they were not allowed to open a new account with the bank.

Melania Trump talks about in her memoir that her bank account was closed after the January 6th riot at the Capitol. She also notes her son, Barron, was prohibited from opening a new account, which, again, seems like political discrimination. Michael Flynn had his credit cards canceled, allegedly because the company was afraid of the reputational risk associated with giving him credit cards. They walked it back after a lot of public pressure.

But again, these are the sort of flimsy arguments you see time and again. Defense of Liberty had to cancel an event because they got debanked right before they hosted an event with Donald Trump Jr. Here, Chase said that they were -- they had violated the terms of service, that they were promoting hate violence, racial intolerance, terrorism, and/or the financial exploitation of a crime. Eventually, Chase backed down, but it was too late for Defense of Liberty's event.

MR. ROTHENBERG: Alexandra, can I -- sorry.

MS. GAISER: Moms for Liberty got debanked by PayPal. Again, it's not only banks that can debank you. And good luck to you if you're an organization with Liberty in the name.

MR. ROTHENBERG: Well, I don't mean to interrupt, but you mentioned reputational risk. Earlier, we heard about politically exposed persons. There's some terms that perhaps, Anil, can you give us some deeper explanation of those terms? Where do they come from?

When were those first started to be used in considerations for risk and potential debanking within this large counter-financing of terrorism and anti-money laundering system that you've described? How do those concepts play?

MR. KASHYAP: Again, so you need to roll back a little bit. From the very beginning of the anti-money laundering laws, the law enforcement wanted paper trails and they wanted to have this know your customer requirement

that was proposed starting in the '70s, but never enacted.

So there was no requirement to know your customer in the United States all the way until the Patriot Act. The Patriot Act blew down the industry opposition to imposing these requirements. And immediately from there on, the banks were required to know their customers.

Now, once you've got that standard in place, it comes naturally that you might say, if we're going to have to know stuff about our customers, it's not going to be one-size-fits-all. If somebody's perhaps more risky or poses different types of risks, you might have different requirements. So a politically exposed person is somebody who's deemed to have heightened AML obligations due to the potential for them being involved in either corruption or bribery.

So, I think the ambassador said it's only for foreign people. That's not true. Anybody in the United States that you think might be someone you want to bribe would be somebody or, you know, that could be involved in corruption is somebody that could be designated as a politically exposed person.

MR. ROTHENBERG: And who designates them? When

you -- you were saying you might be concerned about. Is this also the bank to decide?

MR. KASHYAP: I guess the bank has to certify that you don't fit this. I don't know 100 percent whether that's still the case, but the presumption is when the bank first takes you on, they have to decide if you're subject to this sort of risk.

Once you're in that category, then they're obliged to apply enhanced due diligence. And this is where the key comes because the enhanced diligence requires they know the source of your wealth and that they're continuously monitoring your transactions to make sure that nobody's trying to bribe you.

So, let's now make this a little bit real. As Alexandra just said, the First Lady was reportedly debanked. It's easy to see why that could happen, because think about trying to monitor her sources of wealth and the transactions that would be flowing in and out of a bank account.

Suppose it's the case that she has a trust that was set up some time ago with pretty vague origins, without a lot of documentation that she's willing to supply.

You see foreign entities potentially putting money in and out of that trust. If you're a bank, would you want to deal with that kind of risk? So, they could easily conclude that in that hypothetical, I'm just making all this up, I don't know that any of that's true, but you could see why a bank would say, you know, somebody comes along later and says, "Do you know that that was money from some Middle Eastern company they had business in front of the United States government that's putting money into this trust?"

It goes in many other domains. Ben Bernanke, after he left being head of the Fed, was earning money, I think through speaking fees. He went to try to get a mortgage and was told that, you know, "We don't think we can grant you a mortgage." I was pretty surprised to learn that.

So, it's different people in different circumstances, but it ultimately stems from this idea that if you want to go after money laundering and you want to worry about corruption, you've got to be able to follow the money, and that's going to be pretty intrusive for people.

And if you're not willing to live with that level of scrutiny, then you're going to have somebody in the

business of deciding are we going to cut these guys off or not? Or are we going to take the risk that after the fact, something comes to light that shows, yes, there was a bribe that was in this account?

And you should have been able to tell from the country that it was coming from or the people making the money that this was something you should have reported.

And so, if you've got a very opaque banking account where somebody's trying to defend their privacy, you're going to have this trade off. It's unavoidable.

MR. ROTHENBERG: Now, what can someone do when that happens to them? It sounds from what Alexandra said and what David has said, that there's very little one can do. I'll throw this question open to all of you.

Can an individual or an organization protest to the bank, protest to the government, file a lawsuit? Presumably Alexandra, that's some of the work that you're doing.

Are there established systems in place to challenge unfair decisions about whether someone is politically exposed in the way that you just described, Anil? Are there protections in law or in regulation?

Please, whoever wants to comment on that, I'm very curious about what one can do to remedy unfair situations like this.

MS. GAISER: So, what we've seen has been the most successful is raising a media firestorm, which is typically a little easier if you're a higher profile person. It makes it very challenging if you are someone, like, running a nonprofit or a charity that gets debanked. You're probably just an everyman.

This might not even be your full-time job. And so, knowing the ways to raise a stink to get -- to essentially embarrass the financial organization and to get them to restore your account can be quite tricky.

The law is tough here. The Supreme Court heard a case and decided it last May, I believe, called NRA versus Vullo. And this held that essentially, if you can -- if you get enough information, usually from public statements where you can tie a government official back to the debanking efforts, where you can say, "They're not just trying to debank me. They're trying to chill my speech." That is a First Amendment violation.

This was a 9-0 Supreme Court decision saying that

the former head of the New York Department of Financial Services, which is a massive financial regulator, had intentionally tried to deny banking services to the National Rifle Association, the NRA, that this violated the First Amendment.

So, the tricky thing here is, because of the BSA, the Patriot Act, all of these sensitivities around the law enforcement efforts, it is typically quite difficult as a client to get any information about why your account was closed. Is this a business decision? Is it a terms of service decision? Is it because of suspected criminal activity? Is it because of disfavored First Amendment activity? It's very hard to know, and it's hard to know if it's coming again from the bank sua sponte or at the behest of a regulator.

If you can tie it to a government actor, your chances of getting in court are much better. But this is because of a constitutional violation that they are violating your free speech rights. It's actually not really about the issue of your account getting closed.

MR. ROTHENBERG: Would -

MR. IBSEN: Larry, I would just add -- I would just add, you know, and because of the issue with the supervisory instructions to the banks and with the closest with which the banks are overseen by the regulators, you know, the banks are going to over comply. They have very little incentive to under report SARs or any other kind of activity.

They are very incentivized to over report because civil penalties can be quite steep. And even if someone engages some activity at a later time, they can still be on the hook for that. So, you know, from a personal liability standpoint, if someone wants to pursue that with the bank, there's the confidentiality issue where you can get the information about the circumstances of your account closure. But then, also, you know, the bank is generally acting at the behest of a supervisory agent from the government.

So, the liability issue there isn't as clear. You know, President Trump made this point -- some point in the White House in the last year when he was talking about the supervisory function and the regulatory function in the financial sector.

You know, he said, "You know, when a regulator

comes to you and makes a suggestion about what to do with an account, it's really not a suggestion. It's more like an instruction." And that's kind of how the banks are operating here.

And I would say this is why the executive order works on this a little bit. But it would be really good to have something codified in law that actually, you know, prohibits the closure or suppression of, you know, availability to financial services based on First Amendment rights, you know, speech, political beliefs. That way, you would almost then -- the banks would be liable under the law if they actually closed an account because of your protected First Amendment rights, right?

And then, everything else would become a business decision. And it would provide some clarity there.

MR. ROTHENBERG: I think that it's important to talk about those constitutional rights, but it also seems that there are other reasons one can be debanked, perhaps based on inaccurate information or -- I mean, are there any -- or whim or arbitrarily with no opportunity to correct the record, are there no opportunities or no checks within the system that Anil has described for that sort of redress

process?

In other words, do the Bank Secrecy Act, the Patriot Act, the various supervisory regimes of the banks impose only obligations, but not also protections for customers?

MR. IBSEN: Like –

MR. KASHYAP: I think the thrust of what –

MR. ROTHENBERG: Go ahead, Anil. Yeah.

MR. KASHYAP: -- they've said is right. There's not much of a way to appeal this stuff. You have to have a little sympathy for the banks. The banks are continuously supervised by the bank -- by their supervisors. They can be routinely passing their money laundering tests. And then, after the fact, be fined 5 years later saying you flunked.

So, if that's the world we live in, then -- well, how would the bank respond if it's a close call? You know, you don't want to say there was a footfall here. Never mind if you can be -- have your leg amputated for a

footfall. So, the banks have pretty strong incentives, and there's no protections written in. I think some of these cases are harder than we're making it seem.

I agree completely that the First Amendment stuff should be off the table as a reason to debank. But suppose somebody just really wants to keep their business private, and suppose they are involved in international transactions with, you know, offshore money centers that are well understood to be where a lot of money laundering happens, they have the right to do that.

Does the government want to say, "Okay. We're just going to turn the other way." That's a hard call. And we should acknowledge that that's part of this conversation is, where does the protection against the terrorism and money laundering stop and the privacy start? It's not like there's a clear boundary. And the edge cases aren't that hard to think of. So, I think it's (cross talk).

MS. GAISER: Well, I think -- I would push back on that a little bit. Under the Bank Secrecy Act, it's very clear that if you make the choice to use a bank, that bank is treated as a third party. It's viewed as though you've

waived your privacy interest by engaging with a third party. And I think this is quite shocking.

Most Americans who assume that their transactions with their bank are private and that they are, you know, that they own those, that they own that information. And so, in your example, I think it's the government's stance is, well, you made the choice to use a bank. So, now, it -- we've made the choice that we get to see everything you do. And so, this is an area where Americans have almost no privacy.

And I think that that is a real problem, because here again, the government holds all the cards. On the one hand, they get to look into everyone's accounts. The banks, you're exactly right, are under tremendous pressure to over comply with every piece of the KYC, AML regime, all of this. And then, if your account gets closed, the bank is typically prohibited from telling you why.

Now, they may decide -- they may decline to tell you why for their own reasons, but it's very, very difficult to be a consumer in this regime.

MR. KASHYAP: I agree, but the argument you just made went before the Supreme Court in the '70s. And the

Supreme Court held that the bank has the right to that information. So, this was 50 years ago. This was settled turf.

What's interesting is when the geolocation on your cell phones was potentially contested, and whether or not law enforcement should be able to see that on exactly the same arguments as the banking, the Supreme Court subsequently said, "Well, actually, they don't get to see your tracking information on your phone."

So, Supreme Court hasn't been completely consistent, but I don't think we can relitigate this. This is settled, and it's a matter of fact the bank information is to be shared. So, if you get cut off, you're kind of out of luck. It's very doubtful that you're going to be able to win your bank account back.

MS. GAISER: I do think –

MR. ROTHENBERG: That brings us to -- that brings us to potential reforms, including as a lot of folks have mentioned, the executive order, although, again, as David mentioned, the executive order could be changed by the President. So, maybe there's some -- if not everybody can

go to the Supreme Court. And if the Supreme Court weren't going to revisit the issue, then perhaps there are executive order or statutory reforms that could be made.

I was really struck by all of your explanations of how there's so little recourse for someone who can be affected by this, either for First Amendment rights or for other reasons.

David, can you tell us a little bit more about what you think the -- an effective reforms to this system that would recognize the legitimate reasons why the government might want to track illicit financing or -- but also these privacy and civil liberties concerns? How do we strike that balance?

MR. IBSEN: Sure. So, I mean, just relating back to the previous just discussion, and Anil noted the Supreme Court decision. And I think that was settled. One element of that discussion, I believe, when they were actually considering this initially, and some of the discussion, it was like, you know, we're not sure about this Bank Secrecy Act thing.

And this seems kind of invasive, but, you know, the amounts are so low -- or so high, sorry, it's not

really going to affect people. And that amount being, you know, $2,000, $4,000, and then $10,000 for a currency transaction report. That was in 1970.

If you adjust that for inflation, that's like $77,000, now $80,000. So, you know, just one simple reform, and this is being contemplated in some of the legislation that's been introduced, is finally raising these thresholds. It's been 55 years since the Bank Secrecy Act, and you still have people gobbling up all this information for $2,000 transactions. $10,000 would buy two Corvettes in 1970, right?

I mean, it's just -- it makes no sense now for all of those that the same amount, the same threshold to be scrutinized in the same way.

Just by raising that threshold, you would eliminate so much of the noise and the excessive collection that's going on. And although Americans aren't really aware of it, you would be liberating them from so much government scrutiny on a daily basis. So, just raising those thresholds I think, I think the confidentiality issue is something else that could be addressed without totally dismantling the Bank Secrecy Act.

And I think financial institutions would really

welcome this. They would like to tell customers, "Hey, here are the reasons that's going on. I need more information on where your funders are coming from. I need you to explain this one transaction. You've been making $5,000 deposits for 24 months. Now, all of a sudden, there's two $50,000 deposits. What's going on? I need those."

And so if you could provide that information, I actually think that it would be a nice reform, but it would also help kind of defuse all of this debanking discussion because so much of it is based on uncertainty and people making assumptions about why their accounts are being impacted right there.

And then, I think just, you know, I talked about it before, but something to codify the reputational risk and the fair access stuff that's been approached in the executive order, so that we're not whipsawing back and forth between Choke Point 1 (phonetic), and then reform, Choke Point 2, and then reform.

Just kind of make fair access something that's codified in law, where, you know, you have access to banking services for lawful activities that are protected by the First Amendment while reserving the right of

financial institutions as banks to evaluate customers on their own risk-based assessments, right?

And then, if they don't want to service the customer, provide them the reasons why. So, I think that would be very, very good threshold, confidentiality, and codification of some of the stuff in the executive order.

MR. ROTHENBERG: Alexandra and Anil, would you like to weigh in on those ideas or some others that you might propose?

MS. GAISER: Yeah. I think –

MR. KASHYAP: Go ahead.

MS. GAISER: Oh, go ahead.

MR. KASHYAP: No, please.

MS. GAISER: So, I agree. I think raising those thresholds is a very important piece, and it's something where I think that it may actually make sense to try to relitigate this. The world is meaningfully different now

than it was in 1970. And so, the privacy considerations, I think, have changed.

You're aggregating much more information at much lower thresholds because they haven't been inflation adjusted.

And two, it's a different world. Your data can be across the world in a matter of seconds. That just wasn't the case in the '70s. And so, the amount of information, the amount of data that's collected and to what we can learn from it, is just so much more expansive than it was at the time.

So, I think revisiting the BSA, both its constitutionality, but also some of these basic regulations and provisions here, simple measures like adjusting for inflation, revisiting privacy, are really great.

I think too enabling the banks, maybe requiring the banks to provide information, even if it's something as basic as, you know, about why your account has been closed would be a meaningful help. You know, to David's point that maybe some of this is a big misunderstanding, it's hard to know. And I think over the last 20 or so years, there are reasons to be suspicious.

We've seen lowest learners (phonetic), IRS, the

two operation choke points. We are starting to see deinsurance going after disfavored nonprofits. Audit services are a big issue in cryptocurrency. Nonprofit discounts being applied in a discriminatory fashion.

There are a lot of ways where, if you are considered to be outside of the mainstream or someone's preferred point of view, that you can just be cut off from all sorts of financial services.

And I think Americans deeply understand that that isn't right. That isn't what we signed up for, and nobody voted for that. And so, when we're thinking about how to make reforms, that a little notice, a little transparency really does go a long way. And I think would, again, help to level the playing field, which right now is very, very asymmetric against the consumer and against privacy and civil liberties.

MR. ROTHENBERG: Anil, would you like to comment?

MR. KASHYAP: Yeah. Look, I -- the indexing thing is a no-brainer. I don't know anybody that doesn't support that idea. I also like David's carveout of the First Amendment protections to make it clear that everybody has

that right in the financial services domain, and that if you can show that you were debanked because of those things, I think that's fundamentally different.

I'm guessing most of the people watching this don't know that the U.S. is routinely rated as the easiest place to launder money in the world despite all of this. Why is that? Well, we've not got a beneficial ownership database that shows who's behind a trust or a shell corporation.

It took 10 years of legislation to try to get that enacted. It was part of the 2020 Money Laundering Act and it was abandoned this -- earlier this year.

So, business is wide open for money laundering in the United States. And if you're going to talk about enhanced protection for privacy, you have to understand that's going to make it even easier to launder money in the United States. That's why some of these things are in conflict with each other.

And I think the privacy concerns are real, but so is the risk for money laundering. I mean -- and it's frankly embarrassing that the United States can't get its act together on something so basic as just saying there's got to be a beneficial ownership database so you can track

the bad guys.

MR. ROTHENBERG: I would like to get back to the value of the system, the anti-money laundering and counterterrorism financing system. But I want to look at something else now that has come up in all of our discussions, which is this relationship between the government and the banks and the supervisory role of the government, as I think David quoted the President, quoting that when the government suggests something, it's not really a suggestion.

So, we have the Bank Secretary Act, the Patriot Act, other statutes that require certain things of banks. We have, as Anil was explaining, I think you said dozens of agencies that enforce those and also have their own regulations.

What's the check on the government in terms of their suggestions, other than we know from the Supreme Court case involving the NRA, but are there other standards? Are there other regulations? Are there other policies that determine when the government or who in the government is going to make a "suggestion to the banks"?

Or is this an area where there's too much

discretion on the regulators to make these decisions and thus be open to potential abuse?

MR. KASHYAP: Okay. I could say a little bit about that. I mean, one of the problems with having multiple, multiple sets of regulators is the enforcement is vastly unequal across domains. So, in a lot of what the money laundering landscape looks like, the primary authority rests with FinCEN or in the Treasury, and then they delegate to the Internal Revenue Service the job of following up to chase money laundering problems.

Now, the IRS has lots of stuff on its plate. Going after money laundering is just not at the top of the stack. So, when you find a money services business, like, you know, think of Western Union or somebody like that, that gets fined for money laundering, there's a huge amount of recidivism because they just know the enforcement isn't going to be likely to come after them again.

So, you see some parts of the system that are kind of open for business and the enforcement's very loose. And then, you see other parts where it's really, really aggressive, like in the banking sector mostly, as much as we've been talking about how the banks are, you know,

problematic, it is true that they're supervised pretty tightly and AML is a big priority.

So, I think one of the biggest problems is just the playing field not being level across areas. And of course, water flows to the lowest point. The weakest point in the system is going to be where the most money laundering happens.

And so, you know, you can't just keep adding, you know, one mandate after another without stepping back and looking at the resources and priorities and think you're going to wind up with a good system. That's kind of where we're living now.

MS. GAISER: So, Larry, to your original question, I would sort of add to what Anil said that there is a dual system. We have both federal and state banking and financial services regulators. And so, often a financial institution, especially a money services business, is going to be regulated by both of those.

States are often on a every 2 or 3 year schedule, I believe, for examinations. And that has a lot of discretion. So, the state banking examiner comes in, they can ask you for what they want to ask you about. They can

make their determinations. By the way, nobody gets a 100 percent. Nobody.

So, if you know that you're going in and you're not scoring 100 percent, no matter how good your compliance regime is, no matter how thorough your KYC AML is, you are at the mercy of a state regulator to enact whatever reforms they think are appropriate based on however they happen to understand your business. And this is something we dealt with in the crypto industry. They didn't really understand the business.

And so, again, I think you have these maybe more stringent requirements at the Federal level. FinCEN applies across the board. And then, you have state regulators. In Vullo, it was the NYDFS, the New York Department of Financial Services. That's a state regulator, a very big one. A lot of people are subject to NYDFS. This is -- to your original question, there's no one watching the watchers in this regime.

MR. ROTHENBERG: David, would you like to weigh in on that?

MR. IBSEN: Yeah, no, there's a proliferation of

oversight and regulators to a certain extent. I mean, Alexandra just mentioned the New York State Financial Services Division. I mean, this didn't exist until 2010 or 2011, whenever it was. And somehow the country got along just fine. And they had to send them a whole new department, which then needs to be staffed. And then, they have to find things to do.

You know, it goes back to the issue of reform a little bit also, Larry, is that sometimes, and I'm not saying anyone in the panel is doing this, but sometimes I just hear, you know, people, you know, like to beat up on banks and beat up on financial institutions.

But the banks are actually doing a lot in terms of CFT and AML. You know, I have colleagues at Merrill Lynch. Their compliance department is, you know, 20,000 people, right? I mean, they're working just on all these compliance elements.

I mean, there was close to 35 or 40 million SAR in currency transaction reports filed last year. The banks are gobbling up a lot of information on clients. They're looking at transactions. They're giving them to the government.

There should be more of an expectation of what the

government's doing because, you know, banks do a lot of things. They're not counterterrorism experts, right? And they're not law enforcement.

And so, I think some of the scrutiny should be, you know, what is the government doing with all this information? And how are they interacting with the banks? So, for example, are the banks and the regulators -- are the regulators going to the banks periodically and saying, " Hey, let's do an examination of everything that you filed from a SAR perspective in the last 6 months, year"? You know what, you don't need to file that.

I would focus your attention maybe here, right? I would look, you know, let's disregard that area. You know, I don't think a lot of that's going on. So, the banks are just gobbling, gobbling, gobbling.

It's going to FinCEN or other regulators. Some are just sitting there. And I think the public should be expecting the government, one, to do the government job of, you know, national security, counterterror finance, anti-money laundering work, right?

And then, also being -- if you're going to deputize the banks to basically do law enforcement, make sure that you're providing them with the guidance that they

need to do it effectively.

MR. ROTHENBERG: I think that's an excellent point. And one of the things that PCLOB in our previous work on these issues is looking at when the government collects information, what are the standards, for example, for access to that information? If there's a giant database of U.S. person's information, who can access it? For what reasons? For what purposes?

What standards can they use to perform a query for information of that database? How long does the government keep that? Do we know anything about what the government does with these 35 million SARs that are collected each year?

MS. GAISER: Mostly wait for Russian hackers to access them.

MR. ROTHENBERG: Okay. Well, that actually –

MS. GAISER: I mean, so, this is –

MR. ROTHENBERG: It's not funny. I mean, it's --

one can chuckle at it, but in fact, this database -- cybersecurity for the databases that are -- that of U.S. person information that is collected is in fact a major issue.

MS. GAISER: It's a huge issue. And so, this is something where, again, there's a real -- really uneven playing field between what banks are expected to do and what the government is expected to do. Banks have to have a cybersecurity regime in place.

And you'd prefer it to be SOC 2, but they have to keep customer data secure. This is a massive issue. And we've seen big fines levied for banks failing to keep their data safe.

This is not true for the government. Again, there is no one watching the watchers. And so, as the government is collecting this information, you don't have particularly robust regimes for cybersecurity, for data flushing and discarding of data.

Again, there's, you know, both David and Anil have talked about, you could get fined as a bank for something that happened 5 years ago. Well, you know why? Because everybody is sitting on these files for years and years and

years and years.

And so, you're creating these honeypots of very important financial data for Americans that is highly private and highly lucrative. It's a massive attraction for hackers and it's a huge privacy issue.

And again, I think this goes to what we've all been saying about raise the thresholds, redirect the attention to the most important matters for your suspicious activity reports, your cash transaction reports, focus on where the problems are, go after money laundering.

You don't want to be drowning in this noise where everybody's financial data is just sort of swimming around waiting for somebody to come steal it. You want to get more focused. You want to get lean and mean so that you can go after the criminals and stop criminal activity.

MR. ROTHENBERG: I think another aspect of this collection of data, which goes back to Anil's description of the origins of the system, is that there's usually a general principle in privacy and civil liberty is that information that is collected for one reason is not going to be repurposed for another reason. And at least not without the consent of the person whose information was

collected, notice to that person and other protections.

And Anil, you described earlier how this all started out -- the whole system started out in order to fight tax evasion, and then it went to the war on drugs. Now, it's being used for human trafficking, of course, counterterrorism as well.

But then, I was really struck by what you said, Anil, that we don't actually have any measures of how successful it's been. And of course, it's hard to strike the right balance between protection of privacy and civil liberties and protection of national security and fighting crime when you don't actually know what the values on that equation are.

Can you describe a little bit more where that -- why there's a lack of information about the value? And are there any ways of demonstrating the value or increasing the value or measuring it in some way? Because I think that would be an important part of the discussion of reforms to the system.

MR. KASHYAP: Okay. So, there's several problems that contribute. First of all, we don't know the size of the underground economy and how much money laundering is

being attempted. And so, why don't we know that well? Because the crooks don't want you to know.

So, if I just tell you how much money has been trapped through money laundering operations and the government files those numbers, if it's a small number, does that mean you're doing a great job because there's nothing going through or you're not catching it? That's the first point.

Second point is, think about the SARs. The government, once they find a pipeline that's being used for money laundering, doesn't want the crooks to know that they figured it out. So, even in court cases where a SARs led to them figuring out something, you won't find in most court cases, a disclosure that says, oh, and by the way, the way we caught these guys and got onto them is through this. Okay?

So, that means that you don't see when these things are successful, where the success comes. They don't want to tell the banks, focus on this and not focus on that because then the crooks have a back door through the other way. Some of this is genuinely hard, but some of it is we just don't make an effort to measure.

So, there's no sense that some of the regulators

take this obligation seriously to try to generate statistics that would be comparable over time so that you could measure efficacy and you could measure whether or not things were working out. And I think it's a combination of genuinely hard problems and then under-resources.

And finally, one thing that we should understand is FinCEN has -- they may be pretty good conditional on their size, but they don't have nearly enough resources to do this if you were going to take it seriously. I suspect half of FinCEN's personnel time over the last 5 years was building -- trying to get the beneficial ownership records thing built, and then it was abandoned.

So, you know, there's something like 250 people that work at FinCEN. Think about the one private sector company that's got 20,000 people trying to do it. And then, they feed it to 250 people, they have to monitor the whole world. That's not going to work.

Now, you could replace a lot of it with technology, but do we think the government's going to be the leader in getting AI in and doing this and doing it in a responsible way and not violating stuff?

MR. ROTHENBERG: Right. Using AI for that purpose

would raise its own privacy and –

MR. KASHYAP: Yes.

MR. ROTHENBERG: -- civil liberties issues.

MR. KASHYAP: As would a no-fly list. What would the banks really like? They'd like a list that just says you can't bank this person. You think these privacy issues are bad? Imagine getting on that list by accident. So, there's no –

MS. GAISER: They have that list. It's called the OFAC sanctions list.

MR. KASHYAP: Well, yes, but they -- there's a whole bunch of people you can get fined for doing business with that aren't on that list. And so, some of this is just hard. Some of it's lack of resources and incentives.

MR. ROTHENBERG: Well, coincidentally, just to -- for the audience and for our panelists, PCLOB did in fact, publish an extensive report on the terrorist watch list

earlier this year. It's available on our website where we discuss many of these issues and in fact, redress and notice to people who are affected by it are some of the major issues. We also discuss some of the legal issues in terms of due process that are affected by it.

I'd like to turn now in our last few minutes to the executive order, which we've made a number of references to. The executive order is -- imposes a number of deadlines, which are in fact, coming up for government regulatory agencies to revise their systems, to remove reputational risk, to eliminate or amend any regulations that could result in politicized or unlawful debanking.

There's also cabinet agencies are supposed to develop a strategy to prevent it. And in fact, they're supposed to review current supervisory and complaint data to identify any financial institution that's engaged in unlawful banking on -- debanking on the basis of religion and refer such matters to the attorney general.

So, it seems that this is a very strong executive order. As the last question to each of you, I'd just like for your comments on whether you think this will have a big impact and what we can expect to come out of this really in just the next few months as we see the responses from the

financial institutions to the executive order. Anybody, feel free to jump in.

MR. IBSEN: I'll start. You know, I think it's -- you've already seen the impact of it. I think just the announcement of this, you know, from the White House, the specific citation of the reputational risk element and the instruction to the SBA to then filter down through all these different agencies to remove the reputational risk from the supervisory evaluator handbook, so to speak, I think just kind of immediately ended the politicized environment that had permeated the regulatory system for the previous 4 years and then before that with Operation Trump 0.1 (phonetic).

So, I think it's already had that effect. I believe FDIC and OCC have already announced the different adjustments that they've made to their rulemaking. So, I think it had a powerful impact, but, you know, I've said it two times probably before I'll say the third. I mean, the issue is that until you have something that's, you know, really codified legislatively, I think, or something different statutorily that comes out of the Treasury Department to make sure that you have something related to

fair access, you know, going forward, you're always going to be subject to a repeal of this executive order or being overwritten by something else. So, I really do think that's an important next and final step.

MS. GAISER: Yeah, I think it's encouraging to see too that they want to lean in to find out more about people who were debanked and to get those accounts restored. It sounds small and sort of obvious, but that really has not been an available mechanism up to this point. So, while I agree with David that this is in some ways a temporary measure, removing reputational risk from those formal exam requirements really does take some pressure off of banks.

And then, you -- you're starting to see teeth on the other side that there could be penalties for debanking people for noncriminal reasons. And so, this, again, I think is a really helpful roadmap for fixing some of the inequities that we see in this system and helping to restore the correct balance between people, banks, and the government.

MR. ROTHENBERG: Thank you. And, Anil, you'll have the last word.

MR. KASHYAP: Well, look, I think it's good that some of this is underway, but I'm not terribly optimistic. I think this system is kind of out of control and it's got so many inherent conflicts of aims and objectives that until we get to the point where we're really going to step back and look at the whole system and put some options on the table for taking things out of it and just say, "Look, we can't do everything for everyone. Here are our priorities that we need to get right, and here's where we're going to make a system that's more durable and robust," this isn't going to work.

This is going to sound like a fad that is popular right now, but I agree with David. It would be better to have some legislation, but it would be even better to go back and say, let's take a big national commission, look at the whole AML regime, let's try to streamline it, simplify it, prioritize a few things, do that well, and then let some of the rest of it go. That's where I think we really need to move. And I hope we can get there, but I'm not terribly optimistic.

MR. ROTHENBERG: Okay. Well, on that happy note,

but I will -- I'll actually have the last word. I want to thank you, Anil Kashyap, David Ibsen, Alexandra Gaiser, and of course, Ambassador Brownback for starting. This was an outstanding discussion. I learned a lot. I hope it was valuable for our audience as well.

And I want to remind viewers that the video of the forum along with the full transcript will be available on our website. And PCLOB is accepting public comments on the matter through the Federal Register until the close of business on Friday, December 12.

Providing information to the public by holding public forums like this, issuing public reports, taking public comments is an important part, in fact, one of PCLOB's statutory duties. I'm so grateful to all of you for helping us do that today. And the discussion and debate will continue. Thank you very much. We're going to close.