ASHLEY DEEKS: Thank you so much. Thanks to the Federalist Society for convening this and to Chloe for inviting me to moderate. This is just the kind of event that I'm really excited to see from the National Security Law Center perspective here at UVA. National security today is deeply inflected with questions about new technologies. National security is no longer just about kinetic action on the battlefields. It's no longer just about human spies penetrating foreign ministries so much that we're worried about today is driven by new technologies.

And in that ecosystem, companies have a huge role to play. They are targets of attacks. They can act as proxies for states in these new kinds of warfare, where we see information really being prominent. They are defenders of the US' critical infrastructure. So cyber operations are often drawn out as the most prominent example of these changes.

We're also now seeing threats to the US national security, though, in things like supply chains, where our military is buying things that may have hidden back doors in them. We're seeing it in bulk collection of data by adversaries. And we're seeing it in election interference, in part the hack and dump operations, manipulation of social media.

So this brings us to today's topic, where we're going to be talking about TikTok as a threat to US national security. And we're really fortunate to have two experts with us today to help work through why the US government has determined that TikTok poses a national security threat, what the US government is doing about it, what the legal frameworks are through which the US is acting, and hopefully tell us a little bit about what they think lies ahead.

So let me introduce the two speakers. We have Charles Flint, who serves as chief of staff for US Senator Marsha Blackburn of Tennessee. He advises the senator on a range of issues, including foreign threats, data privacy, and content moderation on platforms.

Before he started working on the hill eight years ago, he was an assistant state's attorney in Florida, where he prosecuted misdemeanors, felonies, and crimes

against children. He also has a private practice background in insurance defense litigation. Mr. Flint graduated from Albany Law School in 2004 and is a member of the Federalist Society.

Sarah Harris is a partner in Williams and Connolly Supreme Court in appellate practice. She's going to be arguing Salinas versus US Railroad Retirement Board before the Supreme Court in coming weeks. From 2017 to 2019, she was a deputy assistant attorney general in the office of Legal Counsel at the Justice Department. As many of you know, that's the office charged with reviewing the legality of executive orders and with advising the executive branch on a variety of national security issues

Mrs. Harris graduated magna cum laude from Harvard Law School, holds an MPhil and a PhD from Cambridge in International Relations. She clerked for Justice Clarence Thomas and has also authored a book on the CIA's relationship with anti-communist intellectuals in the Cold War.

Chuck is going to start us off by discussing the national security risks posed by TikTok and say a little bit about its relationship with the Chinese government, and maybe also some of what the executive and Congress have done in the past few months to address those risks.

Sarah is then going to put those issues into a legal framework. She'll talk a little bit about IEEPA She'll talk about the CFIUS review process, the litigation that has ensued, and maybe some of the implications of the potential bans.

So before I turn it over to Chuck, Chuck, I'd like to just remind the audience to please submit questions via the Q&A function at the bottom. And I will ask questions to the speakers once they've each talked a little bit to lay the background. So please feel free to use the Q&A function. So with that, let me turn it over to Chuck to get us started.

CHARLES FLINT: Great. Professor, thank you so much. Appreciate that. And I'll start off talking about TikTok, just giving some background in general about it, and then moving on to what people who support TikTok say, and what some of the other arguments are on the other side and then the national security implications.

So just to start out, I assume a lot of people know what TikTok is. But if you haven't used TikTok or you're not sure, TikTok a video sharing app, and it makes music videos. You can shoot out a quick video. There's music in the background. It's this lighthearted fun. A lot of people like it. You see a lot of people in the music industry now, I believe, who are on it.

So it's become very popular. It's been downloaded over 175 million times in the United States and over one billion times globally. And for perspective the population of United States is over 330 million. So those downloads represent approximately 52% of our population. Assuming that it hasn't been downloaded more than once by an individual, that's a fairly significant number.

TikTok's parent company is ByteDance, which is headquartered in Beijing. It was founded in 2012. And ByteDance has a valuation of roughly $75 billion. TikTok's valuation, excuse me, valuation is right around $50 billion. So both very successful I believe TikTok might be China's most successful technology company.

Moving into the type of information that TikTok collects. So TikTok will collect your browsing history, search history. It'll collect your location data. It can collect financial data. You'll actually enter your credit card information in there to go ahead sometimes and buy gift emojis.

It can collect your phone number. It can collect your social contacts that you have. There are allegations in some class action litigation that it even collects biometric data. And I believe it's also alleged that the TikTok app will start collecting data before you've even created an account. And that's really important.

So once TikTok is downloaded, it starts collecting information on you. And that's fairly significant. That's part of the reason the federal government doesn't like it. If you think about the location data, the fact that you could track a federal government employee or a federal contractor is something that causes a lot of concern amongst national security experts.

Now, I want to move on to the storage aspect. So TikTok has two servers. Its main server is located in Virginia. They will tell you and swear up and down that all of the data stays in the United States. They don't transfer any of it over to China. The Chinese government never gets its hand on any of it. And they say that if the

Chinese government asked them that they would refuse. I also know they've got a backup server in Singapore.

Now, there are allegations, and these allegations also exist in some class action litigation, I believe, in California. It's part of the group of parents that are suing TikTok saying they collected the biometric data, which would be facial recognition and perhaps fingerprints of children and so forth, that that data does go to China via third parties. So I just want to-- I want to throw that out there. Those are some of the allegations that exist.

What's interesting is that TikTok itself says that, we don't share data with the Chinese, but they have been careful to say that they have not only the ability to do it, and I really want people to listen to this part, they say that would actually be legal for them to do so. And their attorneys have admitted that in litigation.

So they don't do it. But if they wanted to, it would be legal. So just think about that. As far as pro-TikTok , arguments I'll lump them in, pro-TikTok TikTok supporters. There have been a couple interesting articles recently. There was one in Forbes on July 11. It was written by Zak Doffman. And he quotes some national security experts in there. And the tone of the article, and I believe the actual title is, should I delete TikTok?

And he sort of comes down in the middle of it and says it's really an open question that there is no proven or credible concrete evidence that data is going to the Chinese government. There are some experts that are quoted in there that say, hey, this is a bunch of bluster. why would ByteDance, TikTok, want to risk a good thing here and trample on privacy rights?

CNN had another article, I believe it was written in July, from a-- and there was a national security expert who is also quoted in there. And he said, you have a right to be suspicious of the Chinese, but that TikTok wouldn't really be a useful intelligence tool for them.

There was a Wall Street Journal article on July 7 which actually has a quote from a guy named John Callas who is a senior technology fellow with the ACLU. And he takes a different approach. He says that the Chinese apps are among the most abusive and that people are right to be concerned about them. So I would just point

people in both directions, trying to be fair to the people that are pro, TikTok say this. It's not a big deal. Then, on the other side, there are people that are very concerned about it.

And so now I'm going to tell you why I think you should be concerned from my perspective, what I hear. Some of the contacts I've had-- and I'll start out by saying this. The United States military has banned it. Wells Fargo has banned it along with some other private companies. Amazon thought about doing it. And the country of India has banned it completely.

Last Friday, in preparation for this conversation, I had a talk, and I've talked with him a couple times, with general Robert Spalding, who wrote the book, *Stealth War.* And he's a former senior director at the Hudson Institute. Some of you ave maybe heard of him. And he's the author of the book, *Stealth War.*

And I was curious. A lot of times, what people say is, all this data, it's not harmful. Who cares about my browsing history, my search history, and this and that? And General Spalding, I think, summed it up really well. He said, the point is that China thinks-- or people think that China has no reason to do anything to them. But they have your information. And if it becomes necessary for them to do so, they will do it. They will act.

And what they're doing is they're learning an awful lot about your profile. They're developing a personality profile on you with this data that they are collecting. And in one you know separate snapshot, it's not much. But when you aggregate the data, as professor Deeks mentioned, data aggregation and collection, well then, there are algorithms, which are artificial intelligence. They can sift through all of this, and they can learn a lot about your personality. They can learn about your relationships. They can learn about your likes and your dislikes. Can learn an awful lot about you.

And so people will say, OK, well what does that look like? And I'll give you a couple of examples. Maybe somebody decides they want to file a fraudulent tax return on your behalf because they've got your financial data. Maybe all of a sudden, your credit rating gets dinged a little bit, and you can't obtain financing to purchase a home.

That's what this information is used for. It's used to blackmail. It's used to coerce. And I'm going to give you a very concrete example right now. In June of 2018, there was a Marriott employee working out of Omaha, Nebraska. And he used the official Marriott account, for whom he worked, to like a tweet from a Tibetan separatist group.

The Tibetan separatist group had simply tweeted thanking Marriott for listing Tibet as separate from China. And so because he liked that tweet from the account, that triggered an onslaught of calls to Marriott.

They actually got a call from a travel agency over in Shanghai. And in two days, that employee was fired. And I think that speaks to just how meticulous the Chinese are. That was a tweet. They don't even have Twitter in China, but they still watch. And they still follow.

I want to talk just a little bit about some of the cultural differences. Look, war in China and war the US are viewed very differently. War in the United States is viewed as applying force to achieve a political outcome. And I would expand that to not just the US, but the west. But in China, politics is war. That's they view it.

Their system is different. And the internet allows them to conduct this war on a global scale. Think about that. So you look at that, you look at the difference between the systems. I would point you to a couple of other things, too. China has passed a law on June 28, 2017, a national security law that says anybody who's a foreign intelligence officer there can designate a company or a person to collect intelligence for the Chinese government. Any person.

Now, you can be in China, or you could be abroad. You could be a business. You could be an individual. So that's one thing I would raise. The other thing that I would raise is that just a couple of weeks ago, President Xi Jinping said that every company in China in the private sector has to maintain a certain presence of Communist Party employees, every single one.

So TikTok he said, hey we have no influence. There's no communist party influence here. But now, we know that that can't be true because based on what Xi Jinping said, they're going to have to have that. And part of the reason that they have to have that is because in China, everything is one. Everything is uniform. That's what

they want they even want dissent to be harmonious.

And so in I'm going back to what Xi Jinping said here. Part of his reason for doing this is because they want to keep the companies' moral and ideological direction in line with the Communist Party. And that's something that would never happen in the United States. It would actually be impossible.

I mean, think about the government calling up Google or Apple and saying, hey, you're going to have to pick 50 government employees just so we can make sure that you guys are doing the right thing. And I think that's important to know.

I sometimes hear about the tech companies in the United States, don't they do the same thing as these companies? And just remember, the nexus between China and their companies is strong. I mean, you could almost say sometimes they're one in the same. And that's very concerning.

Who are you dealing with over here? Are you dealing with a private company, or are you dealing with somebody who's, perhaps, an agent of the Chinese government? And I don't want to be too accusatorial, but I'm just referring to facts in making that statement. And I think that's something that's fair to surmise.

It's been written that China is looking to create some type of a digital Silk Road. And I know we're not talking about 5G and so forth. But they have plans to get into every country. And whether that's through technology companies, whether it's through Huawei and Belt and Road.

If you understand parts of their history, you know the one thing that China thinks a lot about, and their strategists do, is strategic encirclement. They actually have a board game called Weiqi and it's kind of an advanced version of checkers. And one of the ways that you can win is just by surrounding your opponent. And sometimes, you can look at the board, and unless you're a real expert, you won't even know who won.

So the mindsets are completely different. And I would just-- going back to what Professor Deeks said, I want to bring it back around now, that's why it's so important to pay attention to this, that the art of subtlety is what they do best. And your data, in a snapshot, going on there one time and doing something might not mean a

whole lot. But if you're on TikTok routinely, believe me, they're building a profile on you.

And I'll tell you something. I was a victim of a hacking of OPM back in 2015. And the Chinese were alleged to have done that. And it was great. I mean, I got free credit monitoring for a year, and fortunately, nothing happened. But they said that they were trying to create a Facebook type of system for government employees.

So this isn't the first time. It's not our first rodeo with this. And I'll just go ahead and I will stop there. And now I'll let Sarah go ahead and give more of a legal breakdown. Thank you.

SARAH HARRIS: Well, thank you so much, Chuck, and thanks so much for having me, UVA. You know it's really great to appear even virtually. You you guys have an incredibly robust national security program, which is really terrific, and also a very robust Federalist Society, which was a huge part of my law school experience in terms of just informing myself about issues and having a fun exchange of ideas on some pretty pressing topics.

So what I'd like to do is pick up from where Chuck ended and start with the questions confronting any president, our president, but any other one, too. You're the president, and you are concerned with TikTok because you should take the concerns listed in recent orders, at least.

You think that the ability to sweep up a massive amount of personal identifying information opens US citizens to potential blackmail and also potential corporate espionage. It's just a huge amount of very manipulable data that allows any foreign power, and especially the Chinese, who as Chuck mentioned, are very sophisticated in this area, to leverage that data both to target individuals and also to attempt to influence public discourse in the United States writ large.

So you're pretty worried, even though at first glance it might just seem like it's really fun people doing karaoke or something. I'd like to go through the tools at your disposal if you're in that situation and you want to mitigate the threats that you see with respect to this data collection.

So there are two that Professor Deeks flagged, the CFIUS process and IEEPA And

there's some overlap between those powers in the TikTok case and in general. But in simple terms, CFIUS is something that focuses on transactions, and IEEPA is a power that focuses on foreign entities and just whatever property they have that is potentially subject to US jurisdiction.

So I'm going to first walk through what these powers entail and then talk about how the administration has deployed them vis a vis TikTok, and then the explosion of litigation that has ensued and what might happen next. So let me start with CFIUS, which is the Committee on Foreign Investment in the United States.

That is a nine-member intra-agency group. The Treasury department's at helm. And its job under a statute called the 1988 Exon-Florio Amendment is to review all mergers and acquisitions involving any foreign person whereby the transaction could create foreign control over a US business. CFIUS ultimately reports to the president, who makes final decisions and some of the reviews.

So as is the way of many agencies, CFIUS defines its jurisdiction very, very broadly. And Congress actually encouraged CFIUS to do so with recent amendments. So the particular focus now of the statutory scheme and of CFIUS itself is really on foreign access to personal identifying information.

That used to be a informal focus of the process, and recent legislative amendments have made it a very explicit focus of the process. So what usually happens in terms of CFIUS being able to exercise its review powers over mergers and acquisitions is you're a foreign company. You want to acquire a US business. And let's say it involves something remotely sensitive.

So obvious things would be computing technology, web communications, or even you want to buy a gold mine that just happens to be a mile away from a US military installation. The parties are very well advised at this point, because of how many CFIUS cases there have been, to proactively file for CFIUS review before they conclude this transaction.

That is really the usual rule of CFIUS practice. If your transaction involves a Chinese company and it's obtaining any kind of stake in a US business, even a minority stake that gives it, really, any kind of access or rights, it is much better to file.

And the reason is if you don't file, CFIUS has infinite and indefinite jurisdiction to look at your transaction retroactively. And that's something that most people don't like, at least if you're a private company and you want to move forward with your business, because you could all of a sudden be thrust into a national security review where a merger you concluded five years ago, 10 years ago, however many years ago is potentially unwound by the US government. And obviously, the US government is also probably less inclined to look at your transaction favorably, given that you didn't tell them about it.

So there have been instances where people roll the dice and CFIUS tried to review retroactively. One interesting example is the app Grindr, which is a dating app. And so you might think, OK, who cares? It's a dating app. But Grindr collects a massive amount of personal identifying information and is also incredibly useful if you are someone who wants to use information to pinpoint potential users and then, for instance, blackmail them based on other information you are able to obtain about their personal lives.

For instance, if they are federal contractors, that they're-- I think you can imagine the potential that dating apps might offer if you are someone interested in that angle. So CFIUS retroactively reviewed Chinese investments and ordered Chinese investors to divest from Grindr because of that concern.

The upshot is if you file in advance, CFIUS can clear the transaction, and you're safe after that. You have predictability of knowing that you will not be suddenly heeled before CFIUS and have your transaction under this review.

What does the review entail? There's three usual outcomes. One is that the-- that CFIUS can clear the transaction without adding any conditions to it. That's pretty unlikely for transactions involving Chinese companies that involve any sort of personal identifying information. But it could happen if it's just a really, really plain, vanilla deal and there's just no risk for whatever reason.

CFIUS can also negotiate something called a mitigation agreement with the parties. And so what happens there is the parties go back and forth with different government representatives from the different agencies comprising CFIUS. And it's almost like a game of Battleship, where you get different questions from different

governmental agencies. And if you're in private practice representing one of the parties, it can kind of give you a sense of what the government's concerns likely are.

Of course, all those concerns are based on classified information, so you're certainly not going to get your hands on that. But the process there involves talking through with the government what will the-- what will CFIUS be able to live with and what will the parties be able to live with.

And at the conclusion of that, the mitigation agreement often involves, for instance, no foreign nationals in particularly sensitive US facilities, no foreign nationals having access to personal identifying information, restrictions on how foreign nationals can exercise control over the company. Stuff like that.

The agreement lasts forever. And it often involves monitoring and inspections. And so if you violate the conditions, CFIUS can have the right to jump back in again. And finally, if there is no way to mitigate those risks in the judgment of the CFIUS agencies, CFIUS recommend to the president that the president block or unwind the merger or acquisition depending on if it's prospective or retrospective.

And the president can do so. He needs to make a determination that there is a threat to national security that requires that action. But after that, that's the end of the day for that particular deal.

And these are pretty significant powers because they combine the president's existing foreign affairs powers with a pretty substantial delegation of Congress's commerce authority. One drawback of them is, of course, they are very zeroed in on a transaction writ large. But with respect to the transaction, that is a pretty good amount of power.

For a long time, the main rule of CFIUS practice was that there is no judicial review of CFIUS. So it looks like a very black box process to a lot of people. That did change in 2013, when the DC circuit held in a case called Ralls involving a Chinese investor that was very unhappy to have an investment unwound by CFIUS that due process requires CFIUS to at least inform a party of unclassified information upon which CFIUS is relying in order to hint at CFIUS as concerns in a more tangible way. And there has to be an opportunity for the party to respond before the president

takes action.

But in practice, that's not really a big hurdle for the government to clear because, well, first of all, it's not too difficult to produce that kind of information. And second of all, the cost of doing so is low because, again, the government is not being forced to disclose the classified information, which is really the bulk of what the government is going to be relying on a lot these cases. So that's CFIUS.

The other tool that I talked about at the outset is IEEPA. IEEPA is a statute that delegates to the president very broad authority to regulate foreign entities' property that's subject to US jurisdiction. And that power is triggered by the president's declaration of a national emergency.

So the statutory language involves empowering the president to address a, quote, "unusual and extraordinary threat which has its source in whole or in part outside the United States," and the threat has to be to national security, foreign policy, or the US economy. And, again, the president has to then declare it a national emergency.

And then, if the president does so, the president is empowered to regulate, directly compel, nullify, void, et cetera, et cetera, many other verbs pertaining to any transfer of or dealing in or exercise any right to power or privilege with respect to any property in which any foreign country or any national of a foreign country has any interest with respect to the property that's subject to US jurisdiction.

So that's a lot of verbs, a lot of very broad verbs, a lot of very comprehensive verbs. And what all those verbs do, again, is allow the president to regulate whatever property belongs to a foreign national or a foreign country that the US can exercise power over. Congress can, of course, exercise some supervision over this power. Congress, for instance, can terminate emergency declarations through fast track procedures. But that does not happen super often.

And then, I'll flag just two relevant exceptions to IEEPA because this is a preview of a discussion to come. One exception is for personal communications. So one thing the president cannot do under IEEPA is to regulate or prohibit directly or indirectly any personal communication, be it over the postal service, telephone call, or anything else.

And a personal communication means something that doesn't involve a transfer of something of value. And then, the second exception that's relevant to our later discussion of TikTok is the informational materials exception, which is the president can't regulate or prohibit importing or exporting any information or informational materials, like books, or a poster, films stuff like that. And it doesn't matter if those are commercial or not. You just can't-- the president can't use IEEPA to target that type of property.

So those are the tools writ large. Applied to TikTok, the administration has pursued a belt and suspenders approach that combines incentives to try to leave TikTok with a US owner at the end of the day while mitigating the risks that poses in the meantime. So it's a tricky situation.

I think the belt and suspenders approach, if you look at it writ large, might seem like something that reduces the legal risks. But it also has given, I think, some of the challengers some opportunities to knock out particular pieces of the strategy one by one. And we'll see how that turns out.

CFIUS is the lights-out option. It's a complicated tool for the administration at this point because the whole issue is that ByteDance acquired what became TikTok, a company called Musical.ly, in 2017. And then, a year after that, Musical.ly merged with TikTok and took all of the US users' personal identifying information over to the TikTok platform.

And there was no CFIUS review of that transaction back in 2017. The companies didn't file. CFIUS didn't do anything at that point. And frankly, I'm not sure why. I'm sure there are lots of good reasons why. They are almost certainly classified. But suffice it to say, members of Congress started raising questions about this in 2019. And shortly afterwards, CFIUS announced that it was going to retroactively start review.

So that process involved the back and forth that I talked about earlier, in which ByteDance and the government talking about are there mitigation strategies, yes or no. And I know this from reading the pleadings and the ensuing litigation that this apparently happened.

But the upshot of it was CFIUS was not satisfied. And the president in August 2020 made a determination that national security requires ByteDance to divest itself of all property or assets used to enable TikTok's operation in the US and specifically has to give up all data obtained from the US users. And that has to happen within 90 days. CFIUS can impose a 30-day extension on top of that if it wants.

And to remedy the situation, CFIUS says that the TikTok operations have to be transferred to US companies. So a lot of [? suitors ?] have lined up. And the best case endgame, I think, is a US-- from the US government's vantage is a US company steps up and solves this issue.

Then, there's the IEEPA piece of this, which offers the administration some more tailored options. If you recall the description of all those verbs, IEEPA gives the president lots of leeway in taking regulatory actions regarding the foreign entity's property. The president has made the requisite national security determination and then had the Commerce Department come up with a list of specific transactions that were going to be subject to IEEPA orders.

So here, TikTok is the property that's being regulated. And the various transactions that the Commerce Department wanted to use IEEPA to effect included blocking any future downloads of the TikTok app. And that was supposed to start on September 27. And then, there were a lot of steps that are supposed to happen in November with respect to disabling the functionality of the TikTok app within the United States.

So unsurprisingly, TikTok was not pleased by this turn of events. And both TikTok the company and groups of TikTok users have filed many, many lawsuits. There is litigation in the Central District of California. There is litigation in the Eastern District of Pennsylvania. There is litigation in the district court for the District of Columbia. And there are lots of other lawsuits out there that-- it's honestly like a viral video at this point, one could say.

But I'll focus for now on the DDC suit because the District of-- District of Columbia suit because that's where the most immediate action has been happening. And I think it's the most interesting from a what's going on for a legal standpoint.

So on Sunday night, Judge Nichols, who's a recent GDC appointee, issued a

preliminary injunction enjoining the administration from implementing the IEEPA the order that would have banned TikTok downloads. So in plain English, you can still download TikTok for now.

That ruling was very bad news for the government, possibly pretty unexpected news for the government, because the premise of the preliminary injunction ruling is a pretty sweeping holding suggesting that the president cannot actually regulate TikTok under IEEPA.

How did Judge Nichols get to that conclusion? So if you remember the two IEEPA exceptions I mentioned for personal communications and informational materials, his reasoning is both of those exceptions describe TikTok. TikTok, in his view, facilitates personal communications between users, and no one's getting money out of them, necessarily. So he sees TikTok communications and the platform itself as therefore an attempt to restrict personal communications.

And similarly for informational materials, he views TikTok as facilitating the import or export of messages, which are similar to telegraphs or mail, which are the other things listed under this exception. And so a platform that facilitates that, he says, would be under that exception, too.

I don't have firm views on the scope of IEEPA that I would commit to forever. But my initial reaction reading the opinion is I'm not so sure that this is going to hold up to scrutiny for two reasons. I mean, first of all, I think you can ask a lot of questions about the level of generality of the debate that's going on with respect to do you view TikTok in terms of its individual communications, or do you view it as a platform.

And I'm not so sure that if you prohibit the use of a platform for communication, you are really targeting the communications themselves. There seems like a disconnect between the text of IEEPA talking about specific, personal, or informational material or communications versus the whole range of things you can do on TikTok and the fact that it's a platform.

The government's brief, I thought, used a pretty effective example of a postal service. So if China, for instance, established a postal service competitor in the

United States and read all the mail, you wouldn't necessarily think that IEEPA would prohibits the government from banning that sort of platform for communicating, even if the ancillary effect was particular people can't send stuff in the mail.

Or other examples. I mean, you could take email services, or something like Google. Or you could take it even further and say an open access TV station wouldn't be subject to IEEPA, no matter how nefarious the usage of it, or even internet service providers, since you need the internet to send communications.

So you can see with a lot of hypotheticals pretty fast a lot of questions about how broad is this exception, really, and is there a disconnect between personal communications as something that you can't prohibit versus things that in any way facilitate personal communications or informational [INAUDIBLE].

And the related-- the concern I have is, I guess, I worry that judge Nichols' reading blends together the personal communications and informational materials exceptions in a way that I don't know is actually consistent with IEEPA. They do seem separate. I mean, it seems like things that fall within the first exception would probably not necessarily fall within the second exception.

But by looking at TikTok at the platform level and saying some of the communications on TikTok will fall into one and some will fall in the other so the whole platform falls under both, I think that just exacerbates the level of generality problem that I just talked about.

So that's the biggest and hardest IEEPA challenge going on right now. But there are more. The other questions that are lurking in the background of this litigation include, is there a First Amendment problem with prohibiting US users from communicating on their preferred platform? That's one of the lurking questions of the case that's getting litigated pretty heavily.

There are also due process challenges to IEEPA involving the purported lack of information that the United States may or may not have disclosed regarding the basis for the president's determination and whether due process requires the president to do more on those [INAUDIBLE]. There's also a very hot nondelegation challenge, which is a renewed subject of scholarly and litigants' interest ever since the Supreme Court's [? Bendy ?] decision, suggests that the Supreme Court might

fight on this.

So the theory there is that IEEPA involves an overbroad delegation of power to the president with absolutely no limiting principle. And so I'm not sure that one has legs, but it's in the air. And then, the final thing about challenges is we may see, we haven't seen yet, a challenge to the CFIUS divestment order itself. Now, I think that would be particularly hard given that CFIUS challenges are particularly difficult to litigate in light of the-- even in light of the Ralls decision. But we'll see. That, too, may be on the horizon.

My final thought before opening it up to questions is if you take a step backward, I mean, what's the point of this litigation? I think for TikTok, it's really just to slow the process down. That's the main goal. The longer TikTok is able to be in business, the more the odds are that either the political dynamics will change and help TikTok out or that it will be too difficult to find a US suitor to take over the company.

And so there's just opportunities for maintaining the business in more like its present form, and that there's also more opportunities for China, which is the other actor involved, of course, to say, yeah you're not divesting [INAUDIBLE] to take-- take actions on the Chinese end.

Another ending, which is what I think the United States government is ideally hoping for, is that US companies end up acquiring TikTok before the various deadlines and the litigation moves out. And so everyone continues on their happy way, but TikTok is under a more secure owner where the US is controlling the [INAUDIBLE].

But I think the bigger picture in terms of litigation for me as a separation of powers nerd is there's also another dimension of risk that is now, I think, really highlighted by Judge Nichols' opinion, which is there might be a happy ending at the end of the day. But the risk now is also that US courts are going to cut back on the president's authority under IEEPA and CFIUS in ways that could have pretty negative effects for presidential power in future cases. So that is yet another dimension of risk, and it's interesting in this set of cases to me.

All right. So with that, I would love to hear questions from everyone else. And, again, thanks for having me.

ASHLEY DEEKS: Chuck and Sarah, thank you so much. You've given us a lot of information on this. I like how you ended your comment about presidential power, Sarah. Spoken like a true OLC former attorney. There are a couple of questions in the chat, and I also had a question about the Oracle deal.

So Sarah, you mentioned in passing where it looks like this is headed. I wonder if you and/or Chuck have views about what kind of TikTok deal should satisfy the administration, on the one hand, and should satisfy Congress on the other if we think that Congress has a role to play here.

So there's been some reporting that the Oracle-Walmart deal may not actually solve the security issues that Chuck identified. So I wonder if you could share your views about whether you're optimistic the deal will happen, what a satisfying deal would look like from a national security perspective, and maybe also if you could say a little bit, if you know, China's role here, and whether China will be the spoiler on this by blocking the transfer of any TikTok algorithms? Chuck, can we start with you?

CHARLES FLINT: Sure. I'll leave that 100% divestment is the only acceptable solution to this. Sarah made a really good point when she was talking about TikTok potentially dragging this on. That's a very common Chinese strategy that they've used over the years. They will wait, if conditions are not favorable, until they can get an upper hand, or just a better hand to play themselves.

And maybe that would come if there were a different administration. Maybe it would come with different members of Congress. But they know that we've got an election coming up. The president is up for re-election, members of the Senate, members of the House.

And so maybe there is a way for them to kind of shift some of the thinking on this. But given the security risks, I don't believe that anything less than pure, 100% divestment and decoupling would solve the problem. And I'd be happy to turn it over to Sarah.

SARAH HARRIS: Sure. So I guess my-- this will also be a typical, perhaps, government lawyer response, which is-- or former government lawyer, at least, which is I don't know whether or not the Oracle or Microsoft options would, in fact, mitigate these specific

national security risks for a couple of reasons. One, I have not seen the classified information with respect to the nature of a threat. And two, I think when we talk about the shorthand of minority ownership or we're talking about what the structure of the deal would look like and partial divestment would look like, that may also be the tip of the iceberg in terms of what an actual agreement would look like.

That's the shorthand that you might see in the press, but I would suspect that it would not just be partial divestment. It would almost certainly involve partial divestment plus a bunch of other conditions that are much more tailored to personal identifier information that are just not super-interesting soundbites for a headline in the newspaper.

And so I don't know. I do think that Chuck's response is a sentiment that I sense a lot of members of Congress feel. And so the political angle is also pretty important, which is there are a lot of case studies in CFIUS history in which CFIUS itself may not have paid attention to a deal or may have agreed to something, and then Congress afterwards raises very serious concerns.

And that kind of public pressure can effectively cause the actors in public deal to walk away at the end regardless. And so that's actually what happened with the famous Dubai ports situation in 2006, where a Dubai-owned entity was going to take over a lot of United States ports, as the name perhaps suggests. CFIUS didn't do anything, but members of Congress were extremely upset about it, and the deal ultimately got scuttled.

So I wouldn't underestimate the role that politics and public pressure are going to play, I guess it's what I would say, to wrap it up. And what will China do? I mean, I again, I think all options are on the table. I mean, this is-- the TikTok case is an interesting microcosm for what's going on more broadly in US-China relations right now. There is a lot of power plays, I think. Both sides are testing each other to see how far they're going to go. And I think from the US side, there's an effort to convey that the US is much less willing to tolerate Chinese companies exploiting personally identifying information.

And I think this coincides with a lot more aggressive and public prosecutions of instances of Chinese corporate espionage, too. So on the US side, I think there is a

real effort to crack down. And on the Chinese side, there's also a corresponding reaction of not wanting to-- not wanting to capitulate. So yeah, I mean, I think the Chinese government is incredibly interested in using all levers at its disposal to try to undermine the US approach.

ASHLEY DEEKS: Great, thanks.

CHARLES FLINT: Professor Deeks, can I add just one more thing to that? I think just something historically that would be important to point out the people, look, China became a member of the World Trade Organization back in 2001. They were granted permanent status.

And when you do that, you say you're going to be a reliable, good faith trading partner. And since then, it has not stopped them from devaluing their currency or committing IP theft on a massive scale. And that, arguably, was one of the most important things has helped their economy in the last 70 to 80 years. I mean, maybe the single most.

So I think it's hard for people to look at something like that and say, that was really important to China, and then they still cheat on the rules and then say, OK, well, we're going to go ahead. And if we get into this deal we divest a little bit, and I know TikTok and ByteDance technically not the Chinese government. But I think that that's the fear, is that if you leave them a little bit of a foothold, at least for members of Congress, perhaps, that they would exploit that. So I just wanted to add that. But thank you.

ASHLEY DEEKS: Sure. So a question from Ben Gellman, I think, maybe pushes back a little bit on this. He asks, "Would banning TikTok play into China's hands by advancing their goal of having a decoupled internet that they can have complete control of on their side?"

CHARLES FLINT: Who's that to?

ASHLEY DEEKS: How about to you, Chuck?

CHARLES OK. I don't think it plays into their hands because what they want is our data. And

FLINT: that's a lot of eyeballs. Look what they lost over in India. They don't want to be out of that market. And I think that's part of the reason that they're working hard on this deal, whether it's going to be with Oracle or somebody else.

They don't want to lose the US market. So I don't think that it works to their advantage at all. And I also don't think that that would happen, where they effectively have control of one part of the internet. I think that it's-- I think that it's to their advantage to be over here, and they want that.

ASHLEY DEEKS: OK. Josh [? Goland ?] asks, "China is becoming a global leader in the tech industry, and it's likely that much of the technology coming from China will have many of the same privacy issues that TikTok does. Are we headed towards a future in which not just TikTok, but many of the most popular apps and technologies we use come from China? If so, what do you believe a solution to this will look like, tighter privacy regulations? A blanket ban on apps with ties to the Chinese government?" How about Sarah?

SARAH HARRIS: I think that's a great question going forward because it really raises a lot of questions about whether the tools the president currently has are well tailored to the coming challenges. I mean, CFIUS is not going to be super-helpful for a lot of what you just mentioned insofar as if there's no acquisition of a US company, in order to get a foothold in the US market, it's just a Chinese app that you can download on an app store.

Now, you can still use IEEPA, potentially. But I do think Judge Nichols' order raises a big question mark over whether [INAUDIBLE] is going to be available for things like TikTok or other personal communications platforms, if they were so characterized that way. And even if those tools are available, I think there's a lot of questions about how tailored at the end of the day you can make an IEEPA order with respect to a going forward basis. How do you use it? Can you really use it to essentially create ongoing privacy regulations or protections?

So I don't know. I mean, I think it's a terrific question. And I think it's a really hard one because the challenge is simply the aggregation of personal identifier information. And I think a lot of it may also be, does it take agreement from private companies in the US that are offering these Chinese apps for download or sale? Are

there ways of controlling it that way? I don't know.

But it's really as much of a technical challenge as it is a legal one, and it is uncharted territory.

ASHLEY DEEKS: Chuck, did you have anything to add to that one?

CHARLES FLINT: No. I would just say that I think greater transparency, if that could ever be achieved, I don't expect that, dealing with a lot of companies from China. But if that were possible, that would make it easier.

ASHLEY DEEKS: We have a question from Andrew [? Neil. ?] "Did the way the process played out with the president weighing in on which US company he favored acquiring TikTok and suggesting the treasury get a kickback off any potential sale undermine the CFIUS process? And couldn't it open up any sale to legal challenges?" Sarah?

SARAH HARRIS: So, I mean, I think from the legal standpoint, obviously, TikTok will, and any challenger in TikTok's shoes, will try to leverage whatever public statements they can to make their legal challenge better. At the end of the day, though, I think most courts are going to look at the actual determinations that the president made in the form of executive orders and the Commerce Department's findings.

And so in that sense, I'm not sure that the president's statements are quite as important. But I do think that there's also an aspect of this that is a little, perhaps, misportrayed in the media, at least is my sense, which is in most divestment situations, it's not unusual for CFIUS to have as an option that a US company needs to take over what remains of a company that's impermissible.

I mean, that is an obvious cure for the problem that you don't want a foreign actor owning or controlling something that is a sensitive US company or has sensitive components. And in the ordinary course, I think that of course the government is going to have views as to which particular actors in the United States are best positioned to assume the mantle of protecting that information and helping to effectuate the divestment because in any administration, you're going to be looking at like who is going to actually protect the information and carry out the mitigation agreements that are probably underlying all this.

So that's the reality. I mean, again, though, then you see a lot of public statements that make it sound much more like the process here is simply picking companies that someone likes or doesn't like. And so I just think there's a disconnect between, perhaps, the way that this gets portrayed in the media and the way that the process would ordinarily work.

ASHLEY DEEKS: There's a question from Caleb Stephens. "It's become quite clear that China will not hesitate to crack down on American companies when any of their employees say anything critical about the PRC government." I might also add the NBA in that question. "In light of this, what could be done to prevent incidents like the Marriott hotel employee's situation in the future?"

Chuck, you told that story. Do you have any thoughts about whether there is legislation or , I guess, some other tool that could help avert that kind of problem?

CHARLES FLINT: That's a really good question. And I think that the only way to avert that problem is through public opinion and public pressure, frankly, to let people know that that's just something that's not acceptable. And I don't think you legislate that. I'm not sure how you would do it, and even if there were a way to do it, that it would be an appropriate function of the United States Congress.

This is part of the problem in doing business over in China. And this is how they leverage people, companies, et cetera. And the NBA is a great example. And Senator Blackburn has written a couple of letters to the NBA with concerns about their relationship with China, and in particular their business relationship and how it could affect actions that they take and so forth.

And of course, we saw the tweet from October of 2019, the Daryl Morey Houston Rockets pro-Hong Kong backing there, and it had significant backlash. That market for the NBA in China is a $4 billion market. So I just think that we have to support American companies and support them, but also let them know that they can't back down.

And I know it's difficult sometimes, but they just have to hold tight and, they have to stand strong. And the right thing to do is not-- they should not have fired that employee. So I'll just say that.

ASHLEY DEEKS: I want to go back to one of the first questions, which is from [? Xixiang ?] [? Qidi. ?] "How does TikTok's data collection compare to other similar apps like Snapchat, Instagram, et cetera?" So these are, of course, US companies that are collecting the data.

I think the question, while a factual one, invites, in my mind, a question about legislation surrounding privacy and data security. So you could imagine that even if we are not as concerned about Snapchat and Instagram having lots of our personal information, we might be worried, A, about them selling it to people, and B, about having it get hacked, having it get stolen. You and I, I think, both suffered from that OPM hack.

So should we-- let's say that the data collection is similar. Does that suggest that we need some additional protections about data on these US companies? Chuck, can I start with you on that?

CHARLES FLINT: Sure. I would think that it does. And Senator Blackburn has introduced legislation in the past. She actually has been doing this for several years, and it requires an opt-in type of framework and so forth to add more transparency. I think that there's probably quite a parallel between the data that is collected by US companies such as Snapchat, Instagram, and Facebook and whatever is collected by TikTok.

The big difference that I was trying to drive home is, who's really in control of the company? And I think that's the question when you're dealing with any type of Chinese entity. Is it more of a state-owned enterprise, or are they on their own?

But to answer the question, Professor Deeks, yes, I think that that's something that a lot of people in the United States have concern about, is their privacy. What is done with this data? The privacy agreements that they opt into, I mean, heck, you need a team of attorneys to go ahead and read that.

They ought to have it be a little bit shorter and more comprehensible, I think, for people. And that would make things a little bit easier and also calm the minds of people who have suspicions about what's being done with their information.

ASHLEY DEEKS: Sarah, do you have any thoughts on that?

SARAH HARRIS: Yeah. So I think that's a really-- the privacy act implications for US companies are like a whole-- really, a can of worms that is really interesting right now. But a couple of thoughts on that. I mean, I do think the mere fact that companies in the US are collecting your data raises questions, as Chuck mentioned, about the nature of the agreements. Are those permissible contracts? Are people doing it voluntarily?

That's a different kettle of fish than what we've been talking about in terms of a foreign power simply getting access to the information, whether it is voluntarily relinquisheed or not. But I do think the interesting thing for US privacy law is something you touched on, which is the possibility that US companies are going to get hacked because I think it's a really interesting cutting-edge legal question of how can the federal government, if at all, compel companies to take actions to protect themselves against hacking? Can companies get sued for not protecting themselves enough? What kinds of federal legislation would be permissible to implement with respect to putting in place various protections? Especially since that's both a legal and practical concern.

The second you set up a framework that is fairly detailed with respect to, here is a good blueprint for not getting hacked, then it's completely obsolete. So it's just a whack-a-mole game, I think. And the other interesting question is a jurisdictional one for federal agencies. There's been a debate going on about whether the FTC should be doing this, whether a different agencie should be doing this.

Who is actually in charge within the federal government of ensuring that US companies are as robust as they need to be in preventing themselves from getting hacked? Because I think everyone has seen a lot of very, very serious hacks involving hacks of very, very useful information that foreign actors would love to get their hands on. But this is a hard area for better regulation. And so I'm not super-optimistic that we have a great interest here, unfortunately.

ASHLEY DEEKS: This actually feeds into a question from Richard [? Zeer. ?] Apologies if I pronounced your last name wrong. "Why is it the government's place to regulate any of this? Why aren't people responsible for knowing the terms and conditions of the social media they use?"

SARAH So I think, as my answer, perhaps, just suggested, I do think it's a different answer

HARRIS: potentially with respect to are you simply talking about people within the United States voluntarily giving their information up to a company operating in the United States? In which case you can ask questions about the scope of Congress's commerce clause power, stuff like that. And how far can you go in imposing liability under new theories of [? tort, ?] for instance, for data breaches and the injury to you, if there's no monetary injury, stuff like that.

I do think it's different when we're talking about the government trying to prevent a foreign actor from seizing information that, while you might have voluntarily relinquished it to a platform, you almost certainly haven't been like, yes, I would love it if Russian hackers, or the Chinese government, or other state actors you probably don't want to be aiding have all of your personal details.

And so I think there's questions about whether you can do that. And even if you consented to that, I think it is a different question of when the United States is saying, OK, there is an aggregated threat from aggregating all that data that foreign actors are, in fact, trying to use some of these platforms as a bit of a Trojan horse to use it for something very different than what it purports to be doing.

So it's not just fun and games and dancing. It is, in fact, a way of building up a picture for pinpointing both particular people and exercising influence over them and also potentially influencing just public discourse in the United States or misinformation campaigns.

ASHLEY DEEKS: This is a question about-- it reminds me of the Huawei situation, although it's not about Huawei. The question is, "Can China still threaten US national security if allies and other free countries, particularly NATO members, decide to continue using tech like TikTok? What tools does the US have to counter Chinese tech influence abroad? "

So as I'm sure you know, this has come up in the Huawei 5G setting where the US has tried to aggressively, I don't mean that pejoratively, aggressively tried to persuade other countries that they, too, should be nervous about Huawei for many of the same reasons that we've been talking about here tonight. Is TikTok like Huawei and that we should be worried that the UK, and the Netherlands, and Germany continue to let their citizens and maybe even their military use it? Chuck?

CHARLES FLINT: Well, first off, I just know that there are some differences. Huawei's a telecommunications company, and TikTok's a technology company. So right there, there is a difference. But this is what I was getting at when I was talking about Chinese theory of encirclement and strategic encirclement. So I would argue that there is a danger to our national security.

China has something called the Belt and Road Initiative, which is sort of like a digital Silk Road of the 21st century. That's not my term, somebody else's. I'm not going to take credit for that. But it's a $1.3 trillion initiative. And what they're doing is they're simply going round to countries and saying, hey, we'll build your 5G network, and we'll do it, maybe, for X amount of dollars, or we'll give you some financing to go ahead and complete this infrastructure project.

I want to just touch on two things quick. 5G is really important. For those of you who may or may not know about, it don't know how much everybody realizes or understands about 5G, 5G is different from 4G because it's about machines. 4G is about devices. But if somebody can overtake a 5G network, and this is something I talked to General Spalding about, I mean, imagine somebody overtaking an airplane, or a pack of drones, or a vehicle, maybe. So many things are connected these days.

5G is extremely important. There is actually an example. They call it debt trap diplomacy. And the government of Sri Lanka was having a port bill, and they couldn't obtain financing for it. And this was back in, I think, in the early mid-2000s. China came in and said, we'll offer you a loan. They offered to finance 70% of it, and they gave them a 6.3% percent interest rate.

Well, pretty soon, the Sri Lankan government was paying about 95% percent of their revenues going towards debt. And so the Chinese came to own the port. And they now have it with a 99-year lease and about 15,000 acres of land. And so that's not unusual in these instances in there.

I think Italy has actually accepted Huawei to go ahead and build 5G technology. A quick interesting story. I was in Portugal last summer, and I saw all these Huawei pictures everywhere, and I had my Uber driver had, I think, a Huawei phone. And I was just joking with him a little bit. And I said, hey, that phone's probably listening to

you and doing this.

And he said, he told me, he said, well, Google's probably doing the same thing, and I just laughed. I didn't say anything back. But anyway, I do think it's a problem. And I keep going back a little bit to war. China have used it differently. I'd encourage people to read a book by a PLA general that was-- Lieutenant Colonel, actually, that was written in 2009. It's called *The China Dream.*

And it essentially talks about how the Chinese want to fight this this marathon war, 100-year marathon, which is also the title of the book by Michael Pillsbury. And they'll win without even firing a shot. And that's the goal, but they're studying our weaknesses. And if they have to, they'll be able to go ahead and fight us asymmetrically on a military level. But the fear is the strategic encirclement. And that's why I mentioned that game, Weiqi that they play. It's a very famous game in China, and it gives you insight into how they think, which is much different than how we think.

ASHLEY DEEKS: I have a question that I think is for Sarah. It's from Ben [? Elron. ?] "Is there any in-camera review of the existence or extent of the national security threat, or is the presidential determination dispositive?"

SARAH HARRIS: So the presidential determination is dispositive, at least as you pose the question in the sense that no, there's no in-camera review of the underlying findings. But I do think this does go back to something I applied at the outset with respect to the CFIUS process and changes to it, which is it used to be the case that it really was-- the determination is there the president has said there's a national security threat, and that's all you're going to get out of the government.

And the Ralls decision from the DC circuit requiring at a minimum-- and this is similar to the designation of particular nationals on various other-- for various other sanctions programs, that you need to at least provide unclassified hints using public information that the government is relying on and an opportunity to respond.

So I think, maybe, that's not quite a middle ground between the two parts of your question. But it is a proxy for a very small level of review, of, can there be more engagement with respect to what the threat actually is? It's just hard because a lot of this is incredibly classified. And the whole premise of the process is there's a

[INAUDIBLE] give them the classified information.

And even the in-camera review is going to be a hard proxy for the way that discussions are going to be happening between the agencies who are a part of CFIUS or the rest of the intelligence community underlying IEEPA decisions.

ASHLEY DEEKS: I'm just going to take a moderator's prerogative here to follow up on that. While I do, of course, appreciate that some aspects of the underlying information driving the executives decisions are classified, might be sources and methods issues, we don't want to tell China how we know everything we know, but I do wonder whether the US government could share a little bit more, they sometimes can share more when they're really pushed to, in a way that would help clarify for the American public what some of the actual concerns are.

Maybe share more with allies. Maybe share more with Congress. Whether you think that's helpful, necessary, or impossible, whether there would be any advantage to sharing a little bit more about what, precisely, we know.

SARAH HARRIS: So I guess I see this as a two-part question of one is what's the legal answer in terms of what the law should require or not require, and two is what's the policy answer, or maybe the political science-y answer of, is there a benefit to disclosing more information so people buy into the process more.

And I think those are two different calculations because I think with respect to the legal answer, presidents, traditionally of both parties, very jealously guard their prerogatives over protecting classified information. And that's usually for pretty good reasons, which is the more you start opening up the process to other actors having some sort of legal entitlement to look behind the scenes, it's something-- it's a Pandora's box type situation where it can be very hard to keep that information secure after that.

And so that's the way presidents have treated it for a long time. And as a legal matter, presidents have enjoyed a lot of success in the Supreme Court with those types of arguments with respect to the president's powers. Should that be the answer in terms of should presidents voluntarily relinquish some of that power? Or is there a public transparency benefit to doing it?

I could see individual cases where the answer is yes because I think we all like to think that if people had a-- if people could only understand the United States government's perspective, people would be more sympathetic to the way that decisions are made. And that's an appealing thesis.

I think the downside is there's also a big risk that a little bit of information can also be misleading in some ways, where you get an incomplete picture of the depth of information that the government's gathered or particular ways in which the information has been validated.

And so I think it's a real pickle. I mean, I think the traditional view from a lot of people from a policy perspective is more transparency would make people more comfortable with the process. But I also think there are costs to that kind of [INAUDIBLE].

ASHLEY DEEKS: We are getting short on time. I'll give both Chuck and Sarah just a final sentence or two if you have any concluding thoughts as we go off and try to remove TikTok from our telephones. Sarah, do you have any parting words?

SARAH HARRIS: I think it's just, stay tuned. It's one of the most interesting, again, like microcosms for this whole area of law, both in law and policy for national security nerds that I've seen in a long time. And so if you're interested in it, the briefing that the government and TikTok do is actually pretty accessible and has really good summaries of the current state of play with respect to what the government is going to disclose on in plain English, how it's portraying the Commerce Department findings and stuff. So I would encourage you to look that up online. It's pretty easy to find.

ASHLEY DEEKS: Great. Chuck? Parting comments?

CHARLES FLINT: Sure. Just first off, thank you, UVA, UVA FedSoc, Professor Deeks for doing all this. I think it's been great, and I really enjoyed it. And I've enjoyed listening to Sarah. I would say one thing. Just take with you. Today, TikTok announced that they were going to be issuing election guidance for their users. And so they're going to direct you to what they consider to be verified sources of information that are reliable in the US election.

And I just thought that that was an interesting development. Maybe just something else to put in the back in your mind as you think about everything that we said.

ASHLEY DEEKS: Great. Well, thank you both very much. This was incredibly interesting and educational. I'm sorry we weren't able to get to all of the questions, but there were excellent questions asked, and some remain unanswered. But we appreciate everybody attending this as well. So thank you very much.

CHARLES FLINT: Thank you.

SARAH HARRIS: Thanks, everyone. Thanks so much for having me.