[MUSIC PLAYING]

Even as revelations about Russia's possible meddling in the US presidential elections continue to unfold, privacy is being deregulated. Your browsing history is being sold. Who's buying it, what are they doing with it, and why should you care? Find out with Timothy Edgar, a cybersecurity expert, as we talk about the fate of online security and privacy.

[MUSIC PLAYING]

From Brown University's Watson Institute for International and Public Affairs, this is *Trending Globally.* I'm Sarah Baldwin. We recently caught up with Timothy Edgar, senior fellow at the Watson Institute and an expert on the policy challenges posed by global cyber conflict. Tim served as first director of privacy and civil liberties for the White House national security staff under President Obama, focusing on cybersecurity, open government, and data privacy initiatives. Prior to that, he served as the national security and immigration counsel for the American Civil Liberties Union, where he worked on safeguards for a number of post-9/11 counterterrorism initiatives, including the Patriot Act.

He is the author of the forthcoming book, *Beyond Snowden, Privacy Mass Surveillance and the Struggle to Reform the NSA.* Welcome to the podcast, Tim. Thanks for coming in today.

We've got a couple of burning questions for you. On April 2, President Trump signed a bill repealing internet privacy rules passed last year by the FCC that would have given internet users greater control over what service providers can do with their data. What does this mean for everyday users like me? What protections did we have before that we've lost and how will this change manifest itself? How will it feel different? Does this open us up to more marketing, or is it government surveillance?

Well, this really has to do with the difference between the way we regulate internet companies, like Google and Facebook, and telecommunications companies and cable companies, like Cox and Verizon. And what happened with what Congress did with these privacy rules is they repealed those rules that apply to cable companies and to telecommunications companies. And that's very bad for our privacy because we're sort of used to being tracked by Google and Facebook and these other services. We know that we give them our personal information in order to get services from them, but we don't really expect Cox and Verizon and the people who are carrying those data over the pipes that we use to be using our personal data.

And that seems to somehow violate a basic sense of the deal that we as a society have with them. We give them

pretty close to monopoly access, in many cases. There's some competition, but we really don't have a huge choice of providers. We pay them money to carry our data.

And what these rules were intended to do, that were adopted late in the Obama administration, was to set some limits on what kinds of personal information these companies can collect and how they can use it for marketing. And by repealing them, it's really open season on our personal data when it comes to these big cable and internet service providers. And that's a problem because we really don't expect those companies to be using our data in that way.

I don't think it has big implications for government surveillance because the government has its own rules about how they access our data, and we can talk about those a little later in the podcast. But it certainly has big rules in terms of commercial privacy. And it also is troubling because it shows the impact of big lobbying in Congress.

So this is really about business.

It really is about business, and it's about one set of businesses that hasn't had access to all of our personal data wanting to get that kind of access. Of course, they have the data, because they carry it across their wires, but they've been regulated in ways that Facebook and Google and other internet services aren't regulated. And that's basically designed to address the idea that, hey, they're carrying some pretty sensitive data. They've been regulated industries for many years. They have a good business model of selling us access to the internet. We pay them money, so why do they need all this data?

And we're used to the big debate over Google and Facebook, because for the most part, we're not paying them. So we have a big debate in our society. We pay them with our data. And some people think that's a valid model, and some people think it's troubling.

But we certainly don't pay Cox and Verizon with our data. We pay them with our money. And so the idea that, well, we'd also like to have your data too so we can make even more money just strikes a lot of Americans the wrong way.

So what kind of data are ISPs buying and what are they using them for?

Well, they have access to an enormous amount of personal data-- things like your browsing history, pretty much anything that you're sending to and from the internet, they would have access to. The question is, what are they doing with that data. And the purpose of these privacy rules was to regulate that and to say, they don't have the same carte blanche that companies like Google or Facebook or others have to use data based just on whatever their privacy policy says.

So one of the things that opponents of the repeal were worried about-- and I'm certainly worried about-- is the idea that an ISP could have access to your browsing history and sell that to someone. What would they sell it for? Most likely they would sell it to provide targeted ads.

But also blackmail?

Well, that would obviously be illegal, but it would be a danger if people who were buying that data posing as advertisers were then able to use it against you. And we've seen that in the past where data brokers-- companies whose business is to buy and sell personal data, usually for purposes like advertising but also for purposes like debt collection, can sometimes get spoofed. They can get approached by someone who appears to be a legitimate law firm or someone who may have a legitimate reason to buy this dossier that they've assembled from public sources and they get access to that information.

So for example, LexisNexis has a big data broking industry. Axiom, which I think is now called something else. These big data brokers can sell your information. Many of them have had to regulate themselves to try to prevent that kind of misuse.

How do you mean regulate themselves?

Adopt compliance rules to ensure that they don't sell data to thieves, people that are going to misuse it. And that's been the result, oftentimes, of a scandal, and it's been true for many years now.

So these kinds of regulations are actually beneficial to the industry if they look at it from the long term because being told that you can do whatever you like may get your company into big trouble. But certainly, something like a browsing history is very sensitive information, but it's big business for companies that are doing advertising. And like I said, we sort of have this deal with our telecommunications providers, our cable providers. Look, we pay you money, oftentimes a lot of money. You give us a service, that's it.

Whereas we understand the deal is different with Google and Facebook and services like that. OK, we give you information, and you give us a free service. And then you serve up targeted ads, and we understand how that works.

And for these companies that don't have experience in that area to be saying, hey, we want a little piece of that action, we want a little bit of a piece of the personal data part of it, we have all this data, why aren't we using it. That creates just an additional risk of abuse, an additional risk of more ads being delivered from a new person, a different person. And so that's really where the danger lies.

Well, President Trump, but also members of Congress who are in support of this, move away from privacy, are

also citizens, and they're also vulnerable. So what is in it for them?

Well, I just think this shows the power of the big telecommunications companies in Congress. They hated these rules when they were adopted by the FCC, Federal Communications Commission, in the late Obama years. They have been really itching to try to compete on personal data gathering with the big internet companies, and they're flexing their muscles in the new administration. Republican Congress, Republican White House that is not favor regulation in the way that Obama did. And this was their way of essentially getting some payback for those positions.

So what troubles me is that-- I mean, who was out there clamoring to deregulate Cox and Verizon's access to our personal data. Where was the grassroots support for what Congress was doing? There really wasn't any. I mean, clearly even on the right, the Tea Party groups or other conservative groups, they certainly weren't clamoring for letting big telecommunications companies out to get our data. If anything, they tend to be pretty libertarian and worried about privacy issues. So to me, this just shows really a way in which our political system is not reflecting what we're worried about as citizens, as internet users, and that's troubling.

Is there a way back? I mean, once privacy and protections are eroded, is there a way to get them back?

Well, I think they may have bitten off more than they can chew, these big telecommunications and cable companies. I don't think they expected the kind of backlash that they're receiving right now. Partly that's because these are relatively new privacy regulations that were adopted by the Obama administration. So maybe they could say, hey we're just rolling back some regulations from a few years-- from last year, so what's the big deal? This was the same rules we had before those regulations, for most of the Obama years.

But there's a difference between a situation in which you haven't been regulated yet, but there's an expectation that you probably will be, and a situation in which regulations were passed and then repealed. So my guess is that there's going to be continuing backlash against this repeal. It will be an issue, perhaps in the midterm elections.

Yeah. I was going to ask you about that.

It may be an issue at the state level. Whether state legislatures can do anything about this, given their control over cable companies or other companies that service their customers. So they may have a fight on their hands that they weren't expecting. And there's always a difference between when a industry or a powerful group is trying to stop regulation or slow down some kind of progress and when they're actually trying to go backwards. When they're going backwards, that often provokes the kind of backlash that they don't get just when they're having their voice heard in Congress to try to slow something down.

Well, it's definitely worrisome, and it's developing as we speak. So I'd love to have you back to talk about--

Sure. Absolutely. It's just one example of how it's very different to complain about a regulation that is being considered and actually repealing it and taking away protections that people feel like they already had.

Yeah. OK. Let's turn now to Russian hacking of the US elections.

Sure.

What's the latest? What are the consequences? Who has the authority to punish whom? And if it is true that Russia did interfere with the US election, does that compromise the legitimacy of the Trump presidency?

Well, I think that last point has actually been an obstacle to looking at what happened in 2016. In other words, Trump's best argument has been to try to make this a partisan issue, to try to make the Russian interference into an issue of Republicans versus Democrats. Oh, the Democrats just want to cast doubt on my legitimacy.

No. Actually, a lot of people, both Democrats and Republicans, are deeply troubled by the fact that the Russian intelligence services were engaged in a concerted effort to interfere with the US election process. That they're continuing to do so in European elections this year and that they're using cyber means in order to achieve their objectives.

So what we know about what happened last year, in 2016, based on the assessment made public by the intelligence community back in January, is that Russian intelligence services used hackers to obtain access to the DNC, the Democratic Party's, emails to obtain access to John Podesta's emails to Hillary Clinton's campaign manager. They also attempted to access some of the other political parties, including the Republicans, but they didn't act on that. And the reason they didn't is because, again, the intelligence community assessment-- not me, but our 17 intelligence agencies-- have said that was because they preferred Donald Trump be the elected president.

This was a controversial finding within the intelligence community. But then, I think, when more evidence emerged, it became less controversial because some agencies last year, during the election, thought, yeah, they were definitely trying to favor President Trump over Hillary Clinton. Others were saying, no, they're just trying to cast doubt on the election process, so chaos. Undermine our confidence in the legitimacy of democracy.

But I think with additional information from intercepts and other sources the intelligence committee has became very clear that, no, they were favoring President Trump. And of course, the FBI director, Jim Comey, has confirmed that the FBI is looking into this as a counterintelligence investigation and that they have the lead on examining any coordination that may have occurred between the Trump campaign and Russian intelligence

officials. That if there was this kind of coordination or if there were any other crimes that were committed, then they would also engage in a criminal investigation.

Of the Trump campaign.

Correct. Of anyone who may have committed crimes in the course of this attempt by the Russians or successful attempt by the Russians to interfere in our election process. Now, just to be clear about this, what Director Comey said is essentially always the case when you're talking about intelligence investigations by the FBI. Ever since 9/11, there's been an effort to make sure that intelligence and law enforcement are working hand-in-hand. The FBI is both an intelligence agency and a law enforcement agency.

So in every intelligence investigation, whether it involves a foreign power, like Russia, whether it involves a terrorist group, whether it involves something else, they will also be considering whether there might be crimes. What are some of the crimes that might have been involved? Well, you could imagine someone like Paul Manafort, who received millions of dollars in payments from the Ukrainian political party associated with the Kremlin, did not disclose those payments, did not register as a foreign agent, which is required by law. He may be in big trouble for failing to register as a foreign agent at least.

Same problem with Michael Flynn, who also failed to register as a foreign agent for the Turkish government. He was paid huge amounts of money by a Turkish group that was not directly the government itself, but had ties to the Turkish government. Carter Page, who we learned yesterday was the subject of a Foreign Intelligence Surveillance Court wiretap, which means that a federal judge found probable cause that he was acting as an agent of a foreign power. He, again, could suffer serious consequences for being an unregistered foreign agent, for other possible criminal violations. And he was involved early on in the Trump campaign and later became unaffiliated with the Trump campaign.

So these are associates of the Trump campaign, including the campaign manager for several months, who are in big, big legal trouble. And so what essentially Director Comey was saying is, we're continuing a wide ranging intelligence investigation to understand what the Russians were doing, what kind of coordination might have been going on, if any, and what kind of crimes may or may not have been committed.

Can I just ask one question about-- those are all US citizens. How can-- I'm using air quotes-- Russians be held accountable?

So that's difficult because, of course, every nation engages in its intelligence activities, including the United States. The United States certainly has engaged in interference in other countries' internal affairs using its covert action authorities. So it's President Obama had expelled some Russian diplomats and others at the end of his

administration to send a signal that the US was displeased about this activity. Whether or not any of the Russians involved have potentially committed crimes under American law is not at all clear. It would depend on what they were doing, when they were doing it. And even if they had, we found with other examples of hacking that it can be difficult to get justice, even if we have indictments, because they're not in our jurisdiction.

So it's difficult to see exactly what we can do to the Russian government to send a signal. We are already, of course, put significant sanctions on them over Ukraine. We have a tense relationship over issues like Syria. So are there additional things that we could do? Probably. Will they have the effect of changing the behavior of the Russians? That's the big question, and I don't know the answer to it.

Well, that's a question I have too, I guess that there is no answer to. But is this open season? Hacking, by definition, is not regulated.

Correct. And also before we get too much on our high horse, we have to understand that part of this is our own responsibility for failing to set clear rules about what we think is OK in the cyber world, especially when it has to do with matters related to intelligence. The United States has for many years been involved in an effort to basically shame countries that are involved in industrial espionage. We had an informal agreement with the Chinese in the second half of the Obama administration, which seems to have been surprisingly effective. At least, we haven't heard much about Chinese hackers stealing trade secrets or doing other kinds of industrial espionage.

And part of the reason that we can do that is the US has a longstanding policy of not using its intelligence agencies for direct industrial espionage. And what I mean by that is, stealing trade secrets from foreign countries and then giving them to our companies for a competitive advantage.

Now, the US does engage in extensive intelligence activities, as I'm going to talk about in my forthcoming book, *Beyond Snowden.* And those include intelligence activities well beyond terrorism to include economic negotiations over things like trade agreements. So we draw very strict distinction between that kind of intelligence gathering and industrial espionage, but not every country in the world necessarily would agree with this on that.

And as I said earlier, the US also engages in covert action. So for us to basically be on the receiving end of interference and covert action is an unusual situation for us to be in.

Now the goal of US policy should be to get the Russians to stop. The question is, how do we achieve that goal. And I think that some aspect of deterrence may be helpful but we may need to also look at other ways of addressing the issue. One thing that I've suggested is that our efforts together with our European allies to reform surveillance, to reform our external surveillance, our NSA surveillance and other agencies that operate outside the US, can have a beneficial effect of allowing us to regain some of the moral high ground that we lost.

Do you think it's likely?

Well, we've already taken some steps in that direction. President Obama, after the Snowden revelations, came out in the summer of 2013, initially began with kind of a defense of our intelligence activities and saying, we had rules to protect against domestic spying and spying against Americans, and those were only partly persuasive. It turns out that we have a lot of important businesses, like Google and Facebook and Amazon, that have customers around the world who wanted more reassurance about the privacy of their foreign customers.

So in January of 2014, President Obama issued something called Presidential Policy Directive 28-- that's PPD 28. For the first time in American history, and probably the first time in the history of the world, a major power announced that it was going to have some rules to protect the privacy of foreign citizens in intelligence gathering. So now about foreign citizens outside the United States.

Now, these are not hugely protective rules. They still give the NSA plenty of room to gather intelligence, but they do adapt some of our oversight requirements to protect personal information regardless of whether you're a US person that is an American or a foreigner overseas.

Germany has taken some stronger steps last year. They passed a reform of their intelligence services a new oversight law, which provides a judicial commission that reviews what their external intelligence service, the BND, does when it engages in spying and gathering of intelligence. And they're a very important country when it comes to this because they sit on the internet hub between Europe and the Middle East.

What does that mean, they sit on the--

So the internet has a few big, big pipes, which we will call the backbone. Carries huge amounts of traffic, and those are carried over telecommunications lines. If you have access to those, then you are in a privileged position when it comes to gathering data.

The US government can use a new law passed shortly before Obama became president, called Section 702 of the Foreign Intelligence Surveillance Act, to get access to foreign data inside the US. And they can get it from these internet hubs. They can also get it directly from companies like Google and Facebook and other major companies in the US.

The Germans have a similar privileged position in Europe. The British, of course, have access to lots and lots of intelligence information because they also serve as kind of a conduit, a gateway between Europe and the Americas, not just the United States. So if you look at sort of a map of the world, it's surprising how little it changes over the course of more than a century since we've been laying undersea cables for telephone traffic.

Now those undersea cables are fiber optic cables. They're carrying huge amounts of internet traffic. And in fact, most of the internet traffic in the world is carried through those fiber optic cables instead of being carried on satellites, which is one of the big shifts that we've seen over the past couple of decades when it comes to intelligence.

And this has given the US government access to a huge amount of data because we're, in many ways, the hub of the global internet. It's given other countries access to data that travels through their countries. And one thing we're engaged in is a global dialogue about what rules should apply to countries that access those data. Because essentially, there haven't been very many rules.

Yeah. It's almost like cyber is way out ahead of any sort of thinking about it.

That's absolutely right.

It's developing faster than we can--

That's absolutely right. And our focus before the Snowden revelations came along, before the controversy about Russian hacking and Russian interference came along, our focus was mostly on the idea of possible cyber warfare. The idea that countries would actually attack each other's power grids or their critical infrastructure, dams and so forth, using hacking techniques, using malicious software. And we saw something very much like that in the Stuxnet attack against Iran, against a nuclear plant in Iran probably the first example of a real cyber attack of that kind.

But what we hadn't seen as a broader conversation about privacy, surveillance, and intelligence gathering. Because even the United States, which was kind of raising the alarm and saying, we want to make sure that we have rules to govern cyber conflict, they were always saying, well, of course, surveillance and intelligence is not going to be part of this discussion. And part of that was because the US just has such extraordinary intelligence capabilities.

So we've been on the receiving end of these attacks from the Russians. One thing that I think it is an interesting question is, where does surveillance reform go in the Trump administration.

Yeah.

I think we saw in last year's election campaign some very alarming signs from then candidate Trump about his views about the Constitution, civil liberties, freedom of expression, the rights of minorities. This was something pretty new. We saw a right wing populist campaign that took direct aim at basic constitutional rights and freedoms. And it drove a wedge between candidate Trump and the foreign policy establishment and the national security

establishment of his own Republican Party.

People may not remember, but a huge number of foreign policy types, including many Republicans, came out against Trump in the summer and or late spring and early summer of 2016, long before this controversy about Russia's interference came along. And they did so mainly because they were alarmed at his rhetoric. They thought it was a bad signal to send to our allies around the world. Very bad in terms of cooperation with Muslim communities inside the United States.

And so it seemed for a time-- still does, there's still a risk-- that Trump would essentially shift the balance dramatically away from a focus on protecting privacy and civil liberties, which has been essentially a bipartisan view, really since the middle of the Bush-- of the late Bush administration.

Yeah. Well, it didn't the Department of Homeland Security just try to get Twitter to release personal information on accounts that were critical of the Trump administration?

So, I'm not familiar with that story. All I can say is that I think there's concerns about Homeland Security, there's concerns about the FBI, other intelligence agencies. And here's where I think the big danger is. If you look back at the surveillance abuses that have happened in America in the past, they've generally-- there's they're sort of two key factors that you see there.

The first factor is a lack of rules, a lack of regulation. So trust us, we're the government. We're doing the good thing. We're doing the right thing without a lot of rules.

And that's actually changed pretty dramatically since those times. We have a Foreign Intelligence Surveillance Court, we have the Foreign Intelligence Surveillance Act. We have protections for the privacy of Americans. We have a whole system of oversight for the intelligence community that applies to domestic spying. I'm going to get back to that, because I still think there's an issue with the rules that we have.

The second has been a desire on the part of the intelligence community to please those in power. To give them information that they want to hear that may not really be true. And what I mean by that is if you look at President Johnson, if you look at President Nixon, Johnson and Nixon were both convinced that the upheavals of the 1960s and early '70s were being funded by Moscow. That there was real money that was going into the new left, the more militant-- or what they saw at least-- as the more militant parts of the civil rights movement.

And this just which was not true. This was fake news, if you want to call it that. But they were convinced it was true. And so they go to the intelligence community and they say, show us the information showing all the links with the Soviet Union. And they come back and say, well Mr. President, we don't have this information. Well, you need

to go back and look harder.

And that's what really unleashed some of the worst domestic spying abuses was a desire on the part of the FBI, the military, the NSA, the CIA to produce information for Johnson and then Nixon to prove something that just wasn't there. And so what I fear with Trump is if you look at Steve Bannon, if you look at Sebastian Gorka, who is a pretty controversial counterterrorism advisor, they have painted Muslim organizations, and especially those that are politically active, with a very broad brush.

Most counterterrorism analysts are very careful to distinguish between a very tiny group of extremists who commit seriously violent acts and a much broader group of Muslims who may be more conservative, may be more active politically, and may have a vision of a society with a strong dose of Sharia Law that people in the United States may not agree with. In fact, most American Muslims probably don't agree with, but which are not the same thing as terrorists.

And Sebastian Gorka, Steve Bannon, and others are very much swimming against the tide of that, and are saying, no, no. We're at war with this large group, this ideology, and have promoted a kind of Islam versus the West sort of ideology. Any incompetent intelligence analyst will tell you that's just not true. That there aren't these links between basic Muslim organizations in the United States and some sinister group involving the Muslim Brotherhood and terrorists around the world.

But if you've got a directive from the White House saying, we need to see a report that shows these links, we need you to go back and look harder. We need you to loosen some of our privacy guidelines to give you the ability to do that, then you could see pretty widespread abuses of our surveillance powers.

And that brings me back to the question of, wouldn't we be saved by these the FISA court and the protections for privacy? Well, up to a point. Certainly, we have a rule in this country now that we didn't have at the time of Johnson or Nixon or the earlier abuses, which is, if I want to target you, I want to target your communications, I want to collect-- I want to wiretap you, I have to go get an order from a court that is based on probable cause, based on a recognized legal standard.

What we don't have is good rules for is some of the broader kinds of surveillance that we've seen, especially since 9/11. Surveillance involving metadata as the communications that say when I'd communicate with somebody, but not the content. Incidentally collected communications. So lots of communications get swept up in our surveillance of foreigners, including Americans. Those also have rules, but they're not as strict. So and information sharing-- sharing between intelligence and law enforcement agencies.

All of these reforms were adopted after 9/11 to make our counterterrorism efforts more effective. But they pose

dangers for civil liberties. And in the wrong hands, if you had a determined White House that was looking to prove a fact that just wasn't true, it could pose real risks for civil liberties and privacy.

So I think we need to do more to make reforms on those broader issues of surveillance. And here, we have a lot of irony, actually. Because what we have is President Trump who now claims to be the victim of this kind of surveillance abuse. He, of course, tweeted back in early March that he had just found out that Trump Tower had been wiretapped by President Obama. And that this was terrible and this was a huge abuse.

That claim has been thoroughly debunked, rejected by the FBI director, rejected by the Director of National Intelligence and others. But then he kind of shifted his argument and said, well, I was using surveillance in air quotes. Quote, surveillance, unquote. And that covers a lot of things. He said, Trump said, that covers a lot of things. Well, actually, he has a point. It does cover a lot of things. Obtaining metadata, surveillance of campaign operatives, incidental collection on the Trump transition as they were talking to foreign targets.

So none of this shows that he was right about his original tweet. Obviously, he wasn't. But it does highlight the ways in which-- the many ways in which the society we live in today with our large intelligence apparatus, with our global society can pose risks to civil liberties and privacy. And we still haven't actually-- I don't think we've heard the last of this issue. There have been allegations by people in the Trump White House and then by the house intelligence committee chair, Devin Nunes, that Obama administration officials had abused the civil liberties and privacy of Trump campaign and transition officials.

So far, those allegations haven't been substantiated, but it is still rather remarkable to see a sitting president and his White House spokesman, Sean Spicer, sounding a lot like the ACLU. And saying, oh my gosh, look at all this wiretapping, and they were looking at my name and did they have the right to do that, and I want an investigation. So we may all dismiss this as some kind of giant distraction from the Russia investigation, and a lot of Trump's political opponents are quick to do that. But I personally think that you can care about both.

It's certainly possible that there is, in fact, a problem with-- I mean, we know that there was Russian interference. We know that the FBI is investigating Trump campaign officials for possible coordination. It's also possible that some people in the Obama White House, possibly Susan Rice, may have crossed the line in terms of documenting what campaign officials were doing. And certainly, we know that somebody-- we don't know whether it was Susan Rice or somebody else-- we certainly know that somebody was leaking a lot of information about some very classified intelligence intercepts to the press in order to get that information out there about the Trump campaign.

And one of the ironies there is that that's probably the first and most consequential political use of intelligence that we've seen since 9/11. And it wasn't done by the Trump administration, which is what I think a lot of people were

thinking would happen, it was done to, at least, Michael Flynn and others in the Trump administration.

So one thing that I caution people who kind of call themselves part of the hashtag resistance is to be careful. To understand that the Constitution and our civil liberties are there to protect all of us, and they protect people that we don't necessarily like or that don't share our values or that we feel are our political opponents. And so it's important to get to the bottom of what happened, both in terms of the election and in terms of the leaking that happened earlier this year.

Well, speaking of getting to the bottom of it, I hope you'll come back very soon as this continues to unfold.

Well, we're certainly looking at continuing revelations day after day. I don't think this story is going away anytime soon. The FBI director teased us all with a pretty unusual statement confirming an investigation, and it's going to raise the question of, OK, so what did you find. And also the Senate Intelligence Committee has not been nearly as politicized as the House is continuing to conduct a pretty comprehensive review of this issue. So we've got a lot more, I think, to find out about.

Well, I look forward to having you back and having you help us make sense of it all.

Thank you. Appreciate it.

Thank you, Tim. This has been *Trending Globally, Politics and Policy.* You can subscribe to the podcast on iTunes, SoundCloud, and Stitcher. For more information, go to Watson.Brown.edu.

[MUSIC PLAYING]