THE BROOKINGS INSTITUTION
The *TechTank* Podcast

"'Signalgate' and the use of commercial apps in government"

Monday, April 7, 2025

Guests:

STEPHANIE PELL
Guest, The TechTank Podcast
Fellow, Governance Studies, Center for Technology Innovation
The Brookings Institution

SCOTT ANDERSON
Guest, The TechTank Podcast
Fellow, Governance Studies, The Section 230 Project,
The Brookings Institution;
General Counsel and Senior Editor,
Lawfare

Host:

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

[music]

HOST NICOL TURNER LEE [00:00:00] You're listening to TechTank, a bi-weekly podcast from the Brookings Institution, exploring the most consequential technology issues of our time. From racial bias and algorithms to the future of work, TechTank takes big ideas and makes them accessible. Welcome to the TechTank Podcast. I am co-host Nicol Turner-Lee, the director of the Center for Technology Innovation at the Brookings Institution. And I am particularly excited about this episode. I think I actually say this every episode that we have that I'm excited about all of them. But this one in particular is quite timely. On March 24th, The Atlantic published an article detailing how its editor-in-chief, Jeffrey Goldberg, was inadvertently invited to a group chat with high-ranking national security officials on the commercial messaging app Signal. Now, don't get me wrong, I've done this before. I've added people to a chat that weren't supposed to be there. But in this particular instance,

the members included U.S. Defense Secretary Pete Hegseth, Vice President J.D. Vance, National Security Advisor Mike Waltz, among so many other people who discuss plans including exact times and locations of the U.S.'s attack on Yemen that was carried out in prior weeks. Listen, this story's reach has been vast. Some are even calling it “Signalgate.” For those of you who are around, we remember Watergate? Well, now they've named this Signalgate because of the political blowback to mounting concerns about the security of sensitive information. being shared under this administration. Now, Signal, for those of you who don't know, is a tool that has end-to-end encryption. It's perhaps the safest messaging app available to the public, but it doesn't meet the requirements of protecting correspondence around national security, and it might also reveal a departure from prior concerns of privacy, cyber protections, and others that government officials and workers must comply by. This conversation today, yeah, we're gonna touch a little bit on what's happening in the news, but the bigger question is, how is this implicating how the government is using off-the-shelf apps to engage in highly classified exchanges? Think about that for a moment. What are we doing here, folks? And today I'm joined by Brookings colleagues, cyber national security experts, Stephanie Pell and Scott Anderson. Stephanie, she's a fellow at the Brookings Center for Technology Innovation, where her work encompasses topics like surveillance, cyber ethics, and cybersecurity law. I always want to shout her out for being a former West Point Academy professor. And Scott is a fellow at Brookings who also serves as general counsel and senior editor of Lawfare, our sister publication to our TechTank newsletter with expertise in foreign relations law, international law, and national security law policy. Stephanie and Scott, thanks so much for joining me.

STEPHANIE AND SCOTT [00:03:23] Thank you for having us.

HOST NICOL TURNER LEE [00:03:25] So I just laid out in my inquisitive national choir self what's happening with Signalgate, right? And I think obviously much of what I'm gleaning like all of you is what is in the news. But I wanna start with this story of what happened with the Atlantic because this was particularly unusual that a reporter would be added to this type of chat. And I there's been some back and forth on how we got into the contact list which we don't necessarily have to talk about. But given both of your expertise in this area of national security and cybersecurity, I'll start with you, Stephanie. What's your initial reaction to hearing that such plans were discussed on this commercial ad?

STEPHANIE PELL [00:04:07] I was extremely surprised. I thought it was a complete lapse in operational security. As you note, Nicol, high level government officials on this group chat were discussing the sequencing, timing, and the weapons used in advance of the March 15th attack, potentially jeopardizing the safety of American service members carrying out the attack. And in a brief after action summary that occurred on this group chat, National Security Advisor Walz identified that the military had a positive ID of a senior Houthi leader walking into his girlfriend's building. And in news reporting that occurred later, and reporters from the Washington Post indicated that this reporting came from Israeli collection capabilities and that the Israelis were understandably not thrilled that their capabilities were made public. So none of that sensitive information was appropriate to communicate over signal. And here, as you've noted, I think it's useful to understand what signal does well and what it doesn't do. Signal encrypts communications from end to end. So your communications are encrypted in transit from one end to the other. But when you access your decrypted communications on your endpoint device, they are no longer encrypted. And anyone who has physical or remote access to your device can access those chats. So think about who was involved in this chat. High level national security officials that are understandably going to be the targets of our foreign adversaries. And if you are a foreign adversary and you wanna get on somebody's phone and you use all of your talents, all of all of, all of services, It's very hard for an individual. to protect their

devices. That is why certain kinds of communications are not appropriate for commercial apps, even like Signal. And that is why our government has protocols for engaging in communications that must be secure at the highest level we are able to secure them.

HOST NICOL TURNER LEE [00:06:49] Well, I think that's such a great point. And let's come back to that. Scott, why don't you jump in and give, you know, what your perception is of the story and where you think it's landing.

SCOTT ANDERSON [00:06:57] Sure, it's an extraordinary story. I think it might be the most extraordinary story about leaked confidential information I've seen in my, you know, at this point, getting close to 20 years, rounds up to 20 year career in national security, law and policy of various stripes, for a lot of different reasons. But the story is more involved and complicated than I think most people fully realize because there are a lot of problematic decisions that went into the sequence of events. each of which reflects some pretty problematic decision making, in my view, or at least issues you would want to probe. The first is the use of private devices, as Stephanie noted, by several members of the cabinet. Signal is not an app that at least prior to the entree of the Trump administration was approved for the use on government devices. It still isn't for the most part. Maybe there is some special exception made for some of these people, but we haven't seen any evidence of that. So that's the same vulnerability, whether they were using Signal or not, that creates a vulnerability about access to those machines. Then there is the decision to use those machines on Signal, a network that is secure, probably the most secure of commercially available communications platforms like this, but not necessarily absolutely secure, not in the way that the government wants communications to be secure, not in a style, there's a reason why this is not a format or a channel that's usually used for these sorts of conversations. Then you have to have the decision of how on earth did Jeffrey Goldberg get into this conversation? That's closely related to two, because a lot of it has to do with how Signal works, but we have this added complication coming in where Mike Waltz has tried to blame his staffers at various points and suggested that somehow the name of Jeffrey Goldburg got added in because he had another person he was working with who had Goldberg in his phone. That all may be a kind of noise and an effort to divert from the fact that he had Jeffrey Goldburge's number in his cell, which appears to be a point of. controversy within the White House. But regardless, it adds this question of saying, how did this person get on this conversation? Then you have the decisions by Pete Hegseth and Mike Walt to share very sensitive information. Pete Heggseth in the form of a TikTok laying out the types of strikes that will be happening and the timing about two hours before they started, which is operationally sensitive to say the least, although we can talk a little bit more about the likely classification level and things like that. And then after action, we have this report that Stephanie noted by Mike Waltz, where he first says and then explains after prompting by the vice president that they have this asset who was able to confirm a number of individuals killed and including the individual being targeted after the fact on the ground, which is a different sort of information with great sensitivity and as Stephanie mentioned, has this nexus to a foreign ally. And then we have all the conversation that's happened after this, because of course what we know happened is that the Trump administration denied that any of this was classified and sensitive, and that was the reason why the Atlantic has now made it public. That decision itself deserves a really close look because some of this information was clearly sensitive, not least the fact that you had a foreign government's espionage asset involved in some of these activities, and they're giving real life information about their activities that could easily be used. to at least put that person at risk. So it's not just about the use of signal, it's about a whole nexus of decisions that went into this outcome that we're now seeing, which is this extraordinary conversation and the extraordinary events before and after it.

HOST NICOL TURNER LEE [00:10:33] You know, those points that both of you make are really interesting, right? Because it drills into not just the use of the platform itself, but just the depth of the information that was shared that just had so much vulnerability wrapped around it for the individuals that are out there in the military. I mean, so that conversation in and of itself is really one in which should have heightened the interest and awareness of this. you know, pushing it outside of the, you know he say, she say debate that we've been seeing play out publicly. But what's so interesting also about this conversation let's just stay with the app for a moment, right? There is this position that Signal is probably one of the better encrypted apps when it comes to conversations. And outside of what happened with the military intelligence that was shared over the platform. We've also seen an increase of its use among federal workers who are experiencing layoffs or in the age of finger pointing, people who are just seeking the types of protections that they need so that they don't experience some of the public wrath that is actually happening in this administration. What's so interesting to me is high ranking officials are also using this, right? That work for the government. So it's almost like this app has like gotten the attention of both consumers as well as officials. For both of you, is it just another way that high ranking officials should be communicating with one another, right? Do they have to take to an app that, you know, most people are finding a trust and reliance in, but at the same token, we're not gonna say talking about military operations, you know what I mean? And highly sensitive classified information.

SCOTT ANDERSON [00:12:13] So I think that point you make about the type of information and the way this network is being used is really the key one here. Obviously, private citizens use all sorts of messaging apps and signals become increasingly popular recently because of its highly secure nature. Is that super important? I think a lot of people, like you mentioned, federal employees who are facing scrutiny for uh facing termination and organizing and communicating about things happening have turned to this as part of the reason people are saying it's gotten more popular recently which may be right um you know they're communicating because i think they feel more secure having conversations they're worried about the government i suppose monitoring communications i don't think it's actually very likely that that makes that big of a difference i don' think the government is likely to use the authorities it has to monitor uh communications on other platforms perhaps more easily than signal to monitor people organizing about labor rights and trying to share information about their jobs for federal employees. If they're using their private phones and on private networks, whether it was WhatsApp or just texting or Slack or something else. But it makes people feel better. It makes people feel more secure. In these kind of worst case, you know, black swan scenarios where somebody really does something extraordinary like that, which would almost certainly be illegal, by the way, to monitor communications like these sorts of people, they feel more secure about it. So they've turned to it. Similarly here, we see it looks like a number of government employees, high level officials turn to this network initially for a set of communications that actually isn't necessarily inappropriate, although it is a little odd to do it by this form. Initially what they do is Mike Waltz starts this group and says, hey, everybody, we're gonna use this for coordinating, you know, X, Y, Z, give me a point of contact. That sort of action. uh setting aside you know how you how exactly you identify what the purpose of the conversation how much you give away the idea that you might use private communications to coordinate you know activities with people particularly that where they're traveling around the world might not have easy access to computers i don't think is fundamentally unusual or necessarily itself inappropriate federal employees are people like anybody else if they need to reach out to each other if they needed to contact each other they want to coordinate the innocuous and the unconfidential parts of it, that's. usually okay with one possible hook here, which is that federal records and communications are supposed to be preserved under federal law. And that doesn't happen with signal. They get deleted after a period of time, depending on what the user sets the time at. In this

case, it was originally one week, then it got adjusted to four weeks. Setting that legal question aside, which is a serious one, it's not necessarily weird for these officials be coordinating something innocuous amongst themselves or even the innocuous parts of something that might have confidential parts. I've seen that in government myself, like it does happen because you're just practicalities of having to communicate with people traveling in different parts of the world with different access to information and classified systems that you do use to communicate stuff like this in the government aren't particularly portable. They're not always readily accessible, particularly in a timely fashion. So it's not that weird. What then happens though, is this choice to first by Secretary Hegseth and then later by National Security Advisor Mike Waltz. to then use this network, which is not secure, to go ahead and communicate this sort of sensitive information about first the nature of the strikes and then the nature the information received after the strikes from on the ground. And the fact that everybody else in the conversation seems on board and be engaging with us. A lot of people were relatively silent, but Vice President Vance was actively engaged. A few other people were actively engaged in the conversations, and nobody raised any concerns about it. And that's really where I think you saw the use go off the rails in terms of what might be justifiable or appropriate in a pretty inappropriate direction.

STEPHANIE PELL [00:16:11] Yeah, to pick up on the last part of Scott's discussion, when things, as Scott put it, start to go off the rails, I start to worry then whether rules and protocols for communicating sensitive information are even being thought about. And if they're not being thought about, then they start to erode. And if they start to erode at the top. You know that has the potential of really changing the way the culture of the national security community and the way that it protects information. If you don't have those rules and protocols enforced from the top, then again, you risk a real diminishing of the kinds of security practices that we know how to do and that we need our national security apparatus to follow.

HOST NICOL TURNER LEE [00:17:13] Well, and that to me is like the conversation that originally spurred the concern. And I think to Scott's point and Stephanie, what you're bringing up, it shifted the conversation, I think, to this other realm, which is the ability of these individuals to sort of share this information in a way that wasn't preserved in any type of national record book, and two, to share it in a way where. to a certain extent we got to see the way that they interact as well as the extent to which they don't quite understand how these types of conversations should have some relative privacy outside of the consumer space. Does that make sense to you? I was reading the transcripts and I'm thinking they're talking to each other like I talk to colleagues you know, or I talk to my family versus like thinking about where this fits. in the larger scheme of private and security of government information, which to me also triggers, we just had these conversations in the band of TikTok, right? In terms of government use, not to say that Signal is like TikTok, but I still think that there is this conversation around this shift in concern over privacy that we need to sort of tease out for our listeners. I mean, Scott, privacy, I mean where does this fit as well? I mean, not only are we looking at. this casual exchange of information and probably in a more inappropriate place. But what about privacy, you know, and how these conversations were so easily leaked? What does that also suggest about privacy and, one, how we as individuals assume levels of expectation of privacy, but more so how, you know, certain conversations are just not private anymore?

SCOTT ANDERSON [00:19:07] Yeah, it's a fair question and one that has ramifications obviously a lot more broadly and unrelated to this conversation. I mean, to be clear in this conversation, there should have been no expectation of privacy because conversations like this are supposed to be preserved as federal records precisely so that they're made

available to the public. Now not usually for like five or for classified information, sometimes 20, 30 years. But the idea is that you're supposed to kind of preserving these things because you are going to share them with third parties one day. So, when you are a public official talking about things in the scope of your public duty, particularly in a written, recordable format, there isn't supposed to be an expectation of privacy. And that's something that I think it's easy to lose track of when you're in government. I certainly had plenty of friends and I'm sure was guilty myself about sending personal emails and personal messages on messaging apps on government phones or on government networks. I think very few people in government probably aren't guilty of that at one point or another. but that information is all accessible to the government. On the flip side, on the consumer side, you know, it does show how, I think as consumers, and we have to remember all of these officials are just private people as well, who are consumers and users of Signal on their personal devices, it seems. You know, we do have this feeling of it, a very secure network, in part because technologically, Signal is quite secure in terms of the message exiting your phone and entering somebody else's phone. but that understanding of privacy is just actually not that sophisticated. It's not, especially when you're talking about a context that you might have highly sophisticated third parties interested in getting access to, like foreign intelligence services. Because the vulnerabilities aren't really primarily the signal network, it's the devices on either side or that involved in the conversation that can access this. Those are big vulnerabilities, and we know foreign intelligence services have targeted them, including Vice President Vance's phone that we know that Chinese intelligence has gained access to in the past. And so, we are aware of these sorts of vulnerabilities on the device side, separate and apart from whether using Signal or any other app. And then you have the added networking consideration, which is really what triggered Jeffrey Goldberg being involved in these conversations, which is that these networks are only as secure as you make them. and you can still have human error components that enter into how you are setting them up, that people who aren't diligent and aren't checking each other's work and monitoring this can easily expose information to a third party. So the idea of this being secure does appear to be very secure at a technological level, but that security only applies when applied properly and to a narrow part of the overall communication, not the entire thing. It's easy to lose track of that. when we are approaching, if you're an individual who, as an official, is approaching your job and your official duties through the lens of how you approach something in your personal life. But that's why you're not supposed to do that. That's why officials are supposed to have training, have advice, and frankly be the sorts of professionals that understand you can't just treat planning a set of airstrikes as if you were planning a Saturday night out. It's just a different set of expectations.

HOST NICOL TURNER LEE [00:22:22] Yeah, and I mean, Stephanie, we're going up your aisle here now on cyber security. And Scott starts mentioning the security of devices. It's not just the app itself, but it's also the device. I mean as a cyber security professional, somebody who also watches this, I mean what's going through your mind on that? Because I don't think we've seen that really discussed too much on this or any other type of breach when it comes to commercial messaging apps.

STEPHANIE PELL [00:22:48] Well, again, to reflect on what Scott says, it is important to understand what is secure and what isn't. And with the caveat that nothing is 100% secure. As I sort of started out the discussion and Scott reiterated, while signal may transmit your communications in a very secure way. when they are accessed at the endpoint on your device, that device may not be as secure. And if you are a high-level national security official, there are going to be foreign adversaries that are trying to get on your advice, and that can be accomplished in a number of ways. And so, you know, while I appreciate to Scott's point that. government officials are people and that they may communicate in less secure ways in their private lives, it's important to understand. a

government function, especially when you are communicating highly sensitive information, and why it is important that that be done through established protocols. I, you know, I don't give these folks a lot of slack. This is something they should have known going in, and they should, as high-level government, national security officials, follow the protocols. so that people below them know how important it is.

HOST NICOL TURNER LEE [00:24:33] Well, let's dig into that, Stephanie, for just a moment. What protocols are we speaking about? I would suggest that President Trump sort of started this in the first administration, if you recall. I wrote a paper about this very early on when we were thinking about social media use. President Obama's tweets were archived, placed in the Library of Congress for future research, future recollection for whatever means by the general public. There was a lot of challenges when it came to the first administration of the Trump presidency to sort of think about ways in which they were going to archive some of those tweets. And we've seen the president and now, you know, platforms like X sort of become the town hall for government information. I mean, what are we supposed to do with these situations where we have some explicit expectation, at least on the federal government side, at the highest levels of executive you know, uh, cadence that they will be some pro. I mean, what, what is it? Tell us what should we be expecting? And maybe it's what we should be expecting is written down somewhere. Just nobody's following it. Right. But what is the expectation?

STEPHANIE PELL [00:25:40] So I would say when we are talking about highly sensitive information, the expectation is that appropriate communication channels are used. This is the kind of communication that we saw play out that would normally occur in the situation room or in some secure compartmentalized information facility. That's called, the shorthand for that is a skip. And it is a particular environment that is set up to make sure that communications, when they are transmitted and when they are received, are secure. Back when I used to work in the National Security Division at the Department of Justice, and I needed to have a conversation that needed to be secure because I was communicating sensitive information. I had to do it over a special phone that was inside my office, that was inside a larger skiff. Now, high-level government security officials often have skiffs in their homes, or there are other ways in which aides help them use secure communication facilities and protocols. That's just a given. Now, the second part of your. question really went to how are we retaining, how are how are we setting up rules and an environment where government communications, which are perhaps not particularly sensitive, but but relevant to how the government conducts business and and engages with the American public, you know, how what are the rules for maintaining those and Look, a lot of the newer modes of communication, officials have had to think about how to retain those consistent with public record laws. That is all possible, but what I wanna be careful about is that we sort of don't lump what has happened with this particular signal gate incident in with other. general records keeping requirements that relate to things that are not highly sensitive.

HOST NICOL TURNER LEE [00:28:09] given what Stephanie talked about, right, that there are these two levels of communications and, you know, perhaps one is really a record-keeping conversation, which we should do later as another podcast episode. I mean, what should we have seen? What is on the books of what we should have seen followed when it came to protocols on not just this conversation, but I'm probably certain other conversations going forward when it's actually addressing very sensitive classified information.

SCOTT ANDERSON [00:28:40] Yeah, you know, there is a pretty well established infrastructure for doing this. You have at least two, actually like kind of several different depending on agencies, but generally can be grouped as kind of two classified types types

of classified systems. You have a system that handles primarily lower levels of classified information like secret and confidential information that a lot of employees at federal agencies have available to at their desks, but don't have easy access to. away from their desks. I think that might have improved a little bit since I was last in government. So maybe there's a little more mobile access to those sorts of things, but nonetheless are usually still quite secure. But they're only available to hold the two lower categories of classified information. That's confidential information and secret information. All of which tends to be at a fairly high level of meaning a level of generality. or limited sensitivity. So like a lot of foreign governmental information is presumptively assumed to be classified if there's an expectation that would be held confidential. So even if it doesn't relate to a supersensitive topic but there's a expectation it'll be held confidentially, it often will be classified as I think secret presumptive if I recall correctly. That's called foreign government information or FGI. Then you have another level above that or and again in reality like several kind of interlinking systems above that. that handle the much more classified things. These are the top secret or TS slash SCI, which stands for Specially Compartmentalized Information Systems, where you can access information with a much clearer level of granularity and detail about what the US government is looking at, thinking about, talking about what sources are providing. Usually that system generally doesn't have like specific sources of methods information to have access to that. You have to have the SCI part of that, the special compartmentalized access. So you need to have what's sometimes called codeword access. You have a specific program where you are cleared in as part of small group people specifically working on something because you have a clear need to know that stuff. That's the general classification system. In this case, what was the information being discussed? Where should it have happened? Generally, I think there's a good reason to believe leave the information. discussed here was at least classified or should have been classified at the secret level. There is a little point of contention here because we've seen the Trump administration repeatedly say, well, this wasn't highly classified information. Or at various points say that parts of this wasn't classified, but the talking points kind of switched out to highly classified. So it's not clear what that means. That's a little bit of a dodge in my mind or a way to kind of shift the debate on a more favorable terrain. They may be right that this wasn't TSSEI information, meaning like the highest level of classification, but even secret information is supposed to be protected and handled on these specialized systems that people really, you know, communications are supposed to happen through, again, the particular computer network. And then there are different types of phones and teleconference systems that are cleared for use with us that are usually in spaces that are routinely swept for bugs. have various counter missionaries in place to prevent surveillance and happen on secure actual networks and systems. The conversation where Pete Secretary Hegseth lays out the TikTok for the attacks, I would guess is probably at least the secret level. I think it probably is at the secret. There was not a ton of detail in that other than the time. There's some information about timing and type of weapon that is a level of detail that might rise to a higher low classification level. But I would guess that's probably at least secret. That's where if I had put money on it, that's where I would get the guess for those that lives. Part of that also is because that information or information like that sometimes gets declassified or you get special permission to share it shortly before a military action like this takes place because you wanna share it with either allies who you wanna sharing information with. Sometimes you wanna to share with the press in advance. So you actually declassify it so you can share it. Although again, I think this is a level of detail beyond that. Um, so there might be an argument that some of the stuff was declassified before the strikes happen would have been declassify to this detail level two hours before the strike started, particularly because they're actually having an active debate had just been having an active debate as to what the delay them. I'm less clear on that. I think that's a little more dubious. The other information, the information again about this reports from on the ground assets regarding the effects of the airstrikes. That's highly concerning. It was a

high level of granularity, but it's happening in real time. I doubt it had gone through a formal classification process yet, but it's the type of information that officials with classification authority and everyone on this call, I believe would have had classification authority, should know this is stuff that usually gets a high level of classification because it relates directly to sources of methods and it could really endanger those sources of method. And the fact that it's a foreign government source of methods really just doubles down on that. So that's kind of what I would have expected to see, is to see this conversation. Well, not happening on the system at all in the first place, because you're not supposed to talk about government information on private systems anyway. But particularly where you have these classified parts of this conversation, they should have been on the much more controlled systems, and perhaps even on the most controlled systems. Not happening on private devices on a private network.

HOST NICOL TURNER LEE [00:34:03] You know, as we wrap up here, I mean, Stephanie, for you, I think that, you know, should we gain some lessons about this going forward? Obviously, these conversations that continue to happen, these platforms are gonna be readily available. You know just some closing thoughts, like where we should be taking the lessons of this and applying it across other federal agencies that may find the need to, you now, find a platform where they can actually aggregate them and congregate in ways like this.

STEPHANIE PELL [00:34:34] I think it's pretty simple for me. I think national security officials need to follow established protocols for sensitive communications. To the extent that they need more assistance in doing so, they should ask for it. but we need to be really deliberate about understanding what communications are sensitive. and what aren't. And we need to take the steps that are in place to protect those communications. Threats from foreign adversaries are only growing. These folks are understandably targets. They have within their capacity to use secure communications protocols and why they, in this case, refused to do so. just makes absolutely no sense and potentially could have harmed an ongoing operation.

SCOTT ANDERSON [00:35:38] And I'll just say, to add to that, that there is kind of actually a broader policy question about this, because this isn't the first time we've seen the Trump administration, either this one or the prior Trump administration do things like this that are a little reckless about sharing these types of information. Of course we have, if nothing else, the huge Mar-a-Lago scandal in subsequent criminal prosecution related to the fact that President Trump took lots of sensitive records with him. out of the White House and then later claimed that he had in fact declassified them and started sharing them with biographers, with third parties and other people while he was at Mar-a-Lago at Bedminster, one of his other clubs. That's really problematic behavior, but it's worth noting that the president and people who work for the president can get away with it because the authority to classify or declassify things rests with the president. In fact, outside of very narrow channels that Congress has legislated around, like The vast majority of classified information is only classified as a result of executive branch action. Meaning, if you have a president who doesn't care that much about it and is willing to install exceptions for him and for people he likes and people he works with, or when he wants to use information that's convenient to him, even if it may compromise other equities, he can do that. It doesn't have to actually be that way. Congress occasionally has, like I said, in the nuclear context and a few other very narrow contexts. And Congress could install mechanisms that both require the draw lines about what sort of information needs to be treated certain ways and installs real enforcement mechanisms to say, hey, if we have a breach on this, we need to have an investigation, we're directing you to have investigation or we are going to initiate a congressional inquiry and that there could be a range of penalties in place beyond just professional consequences or criminal prosecution. both which lie with the

executive branch and probably will never be brought to bear in this case or may not be. That's a bigger policy question for Congress moving forward. But if we're really in an era where the executive isn't treating sensitive information as carefully as it has traditionally, and that presents real policy problems, then it may fall on Congress to start saying, well, maybe this is something we need to start regulating instead of leaving it to the executive branch to take care of.

HOST NICOL TURNER LEE [00:37:55] Well, I think that is where we close, right? We need Congress potentially to step in and to help us with some standards on what's appropriate. Stephanie, I'm thinking about your work, what's compliant in terms of the tools that we actually use and really match those against the existing protocols if we're gonna make sure that we have consistent communications, particularly in the highly classified spaces. Thank you, Stephanie and Scott, for joining me. This has been really interesting. I've also learned so much on this, so thank you, Bo. Thank you. Thanks, Nicol. Your insights have been valuable. We look forward to looking at more of your research. Friends, if you have listened to my colleagues, you can find them at the Brookings Institution through the Center for Technology Innovation or on the Lawfare website. Please explore more in-depth content on tech policy issues at TechTank, the newsletter, and keep listening to us on TechTank the podcast. Listen, your feedback is so substantive to us and we are excited. and we're coming soon. with some tech bites with Mark McCarthy, our non-resident scholar soon, that will show up in the next episode. This concludes another insightful episode of the TechTank Podcast. We make bits into palatable bites. Until next time, thank you for listening. Thank you for listening to TechTank, a series of roundtable discussions and interviews with technology experts and policymakers. For more conversations like this, subscribe to the podcast and sign up to receive the TechTank newsletter for more research and analysis from the Center for Technology Innovation at Brookings.