Speaker 1:

... Editor Jessie Bur.

Jessie Bur:

All right. Hello. Hello, everyone. How are we doing? Getting past the after lunch slump? Okay, good because I'm very excited about the topic of this panel. Lawmakers on both sides of the aisle over the past several months have raised concerns about the security implications of the social media app TikTok. Recently TikTok CEO, Shou Zi Chew testified before Congress, and the testimony in the hearing often ended up causing more questions than answers. Just yesterday, Montana became the first state to completely ban TikTok in the state.

Jessie Bur:

Today I have a great set of panelists to discuss the future of TikTok and the impact that this social media app has on security more broadly, but before I introduce the panelists, it's going to be time for our polling question. Our poll for this session is, does TikTok pose a greater threat to the nation cybersecurity than other social media platforms? Yes or no? All right. While you guys are deciding, I'm going to introduce our panelists. Today we have Patrick Toomey, Deputy Director of the National Security Project at the ACLU, and Alan Butler, Executive Director and President of EPIC. Patrick and Adam, why don't you give me a little bit of background on what you do and your relationship with social media and security.

Patrick Toomey:

Sure. I work at the ACLU'S National Security Project. The ACLU is an organization devoted to defending the civil rights and civil liberties of Americans. We, in the National Security Project, work on a range of issues and policies where national security is invoked as the justification to infringe on the rights of people in this country. We work across issues, including surveillance, profiling, discrimination against groups on the basis of race, ethnicity, national origin, and we have worked on a host of issues over the years since 9/11, raising civil liberties issues in the national security arena.

Alan Butler:

I'm Alan Butler, the Executive Director of the Electronic Privacy Information Center, EPIC. EPIC Is a nonpartisan research and advocacy center based here in Washington DC founded in 1994 to focus public attention on privacy and civil liberties issues. We work on a number of the similar issues to what Patrick and folks at the ACLU work on. More recently we really have focused our work a lot on consumer protection and data privacy, data protection issues, but we also work on surveillance issues and other civil liberties issues online.

Jessie Bur:

Excellent. I'm sure we'll be monitoring the poll as the session progresses, but just taking a look now, it looks like people pretty by and large are saying that yes, TikTok does pose a greater threat. Do you guys agree with our audience?

Alan Butler:

Sure, I'll start. I think that several years ago during the Trump administration, when they first were working up taking some executive action against TikTok and this proposal was first floated for TikTok to

essentially enter into this relationship with Oracle, we wrote a letter really flagging the fact that transferring operational control of TikTok users data over to Oracle, which is in another [inaudible 00:03:29], one of the largest data brokers in the United States, isn't really a solution for the privacy of TikTok users.

Alan Butler:

We recognize that there are some, let's say, there's a unique threat model associated with concerns around access by the Chinese government to personal information, but even there, I don't think TikTok is in any way unique among social media apps or other online services. There are significant concerns about foreign intelligence collection of personal data through existing apps and services, even ones based in the United States, especially given the nature of the ecosystem around targeted advertising and how much data is created and generated there. I don't think that TikTok truly poses unique risks. I think maybe those risks are in some cases exacerbated because of physical co-location of data, but I think it's the same risks across the industry.

Patrick Toomey:

Yeah, I'd agree. I think that there are legitimate concerns about TikTok, but they're not unique. The public evidence isn't there today to support the kinds of bans that Montana and legislators around the country are calling for. The threats that people discussed when they are calling for banning TikTok are not unique to that platform. Privacy concerns are far broader. The kinds of data that people say the Chinese government could get access to can be acquired through many different means. US-based social media platforms raise many, many of the same concerns. The solutions I think for us are not to ban an app that is the home to an immense amount of first amendment protected speech and expression in this country, but to adopt rules that protect user data across the board.

Jessie Bur:

Let's get into the Montana ban for a bit. The ban itself would go into effect at the beginning of 2024, and it would impact the app stores and then also TikTok itself for basically making it available to people in Montana. From your guys' perspective, we can pretty much expect that there's going to be a legal challenge to this. Do you think this ban is going to hold up or even affect the kind of protections that it purports to do?

Patrick Toomey:

Like you said, I think it's virtually certain that there will be a challenge to the law just as there was in 2020 to the Trump administration's bans. Those challenges we think are very, very likely to succeed because the First Amendment doesn't permit the government to ban an entire communications platform, except where there is overwhelming and widespread evidence of a threat to national security. The threat has not been borne out in this instance by the public evidence.

Jessie Bur:

Alan, do you have any thoughts on...

Alan Butler:

Yeah. I generally agree with what Patrick is saying. I think that the practicalities around how this law would actually go into effect also probably play out in the course of any challenge where there's going to

be harms analysis and an injunction type of challenge and the question of whether it's even possible to apply this ban in a way that doesn't further exacerbate harms to the users, even if those harms are privacy based. There's concerns about do you geofence Montana? Do you have to collect more personal information as TikTok from all other users so they don't have to prove that they're not in Montana? I think that there's fundamental questions about how this will work that I think will play out in the challenge as well.

Jessie Bur:

I think one of the biggest concerns brought up about TikTok is China's access to the data of users, whether that's just the average American or significant people whose data might be especially valuable. Do you guys think that TikTok being owned by ByteDance and that kind of thing gives it an extra vulnerability of data, or is China able to just purchase this data legally already from all the other social media apps that aren't getting scrutinized this way?

Patrick Toomey:

Like Alan said before, there may be differences in terms of TikTok's relationship with the Chinese government that heighten concerns, but those concerns apply broadly. Other apps collect this data, sell it on the open market where it can be bought by all types of entities, foreign governments and other commercial entities to track people, to learn incredibly intimate things about where people go, who they are, their political preferences, and an immense amount of other private information. The fact that TikTok is connected to ByteDance is one consideration among those, but it's not a controlling or determinative one here.

Alan Butler:

I think TikTok has a US presence and is subject to US law. In earlier sort of different version of this fight a number of years ago before the Supreme Court took up the Microsoft case, there was a question about whether companies like Microsoft and others could comply with legal orders in Brazil and other countries that were requiring them to disclose user data in ways that conflicted with the electronic Communications Privacy Act here in the US. Those fights, I think, really showed that US law and legal protections do have a substantial effect in the sense of actually limiting the circumstances where entities can either collect or disclose or use data. That is a real protection against the type of threat that lawmakers seem to be flagging in the TikTok circumstance. That, to me is the obvious solution to this problem as opposed to, as Patrick said, banning a single app.

Alan Butler:

I'll also point out that evidence is shown in past examples that when foreign intelligence collection and activity is going on, they're usually not knocking on the front door. In many cases, they're using other surreptitious means as the Chinese government is or has done in the past with or as other governments have done in the past with Twitter, for example, or buying it on the open market. There was a horrifying story in the Wall Street Journal today about US based entities that were targeting advertisements to individuals who were visiting abortion clinics based on geofence data. That in and of itself involves collection of that information about where these people are going with an inference of what they're doing and that's all happening, again, just on the open market, on the current environment. If we really want to get serious about these risks, it's not unique to TikTok and it requires real application and heft of privacy rules in the United States actually setting comprehensive standards that are enforceable against all entities.

Jessie Bur:

If by and large the security threats posed by TikTok are evident in several different social media apps, why do you think there's such bipartisan push to target TikTok specifically versus passing a comprehensive data privacy law?

Patrick Toomey:

I think there...

PART 1 OF 4 ENDS [00:11:04]

Jessie Bur:

... comprehensive data privacy law.

Patrick Toomey:

I think there are multiple reasons, but one of them is surely that with rising geopolitical tension with China, it has become politically expedient to go after Chinese companies and that it's easier to score those political points than to solve the very hard problem of adequate privacy protection that applies across all the companies, whether they're based here in the US or abroad. But that's what needs to happen. Lawmakers need to take up that challenge and really limit the amount of data that companies are holding in the first place so that it can't be sold on.

Alan Butler:

I think that, I'll say to their credit, lawmakers have been taking the task of identifying and getting real privacy rules underway over the last year. We've seen significant bipartisan work done in Congress on the American Data Protection Privacy Act, the ADPPA, last session, likely to be reintroduced again in this session. And even at the TikTok hearing that you mentioned in the House, the theme coming out of that hearing actually was many lawmakers saying essentially seems like there's a lot of problems here that TikTok is raising, but that require a broader solution that requires stronger comprehensive rules.

Alan Butler:

I do think that part of the reason why there's an animating principle maybe around and behind TikTok and animating the Montana ban and others, is that in addition to specific data access and privacy concerns and foreign intelligence access, there's also this additional layer of harmful content and content moderation that was certainly the focus of certain parts of the House hearing that TikTok, I think with its growing user base and algorithmically derived feed has brought into focus and the TikTok challenges.

Alan Butler:

So I think that there's definitely a greater public understanding of that set of issues within TikTok versus other social media apps.

Jessie Bur:

So because there seem to be some people that are still so stringently calling for a ban or trying to implement it, Patrick, I know when you and I were talking earlier, you mentioned that there's some

existing federal laws that could potentially get in the way of a ban going into effect because Congress has in the past protected the ability to access information from other countries.

Patrick Toomey:

Yeah, that's right. In some ways the ban proposals today harken back to a period of time during the Cold War when there were calls to ban individuals from countries that were perceived to be hostile to the US from sending artwork, sending works of literature to the United States, artists from Cuba and other countries. And what Congress did in the face of those calls to prohibit the free flow of information was it passed something called the Berman amendments in the '80s and '90s, which amended EEPA, the Emergency Economic Powers Act, and ensured that the president couldn't use those emergency powers to block the flow, the importation or exportation of information. And that was one of the key grounds that when President Trump sought to ban TikTok in 2020 and WeChat, that multiple courts around the country relied on those Berman amendments to say these bans are illegal and struck them down.

Patrick Toomey:

And so what some of the proposals today would do would essentially gut the Berman amendments, would either limit their reach or would try to go around them to allow the federal government to ban TikTok or to take other steps. But I want to connect just briefly those immensely important forms of expression that were the impetus for the Berman amendments with what people use TikTok for today. Because I think there's an assumption, especially if you're like I am, older than 40, maybe that TikTok is mostly about just entertainment and funny videos, but it has more than a billion users around the world, 150 million users in the US. And it's used for everything from news, access for civic engagement, financial literacy.

Patrick Toomey:

There is an incredible amount of expression that people both post there themselves but then access also. And access to information is part of the First Amendment, falls within the First Amendment's protection. So it's not just about people's ability to speak, but it's also about people's ability to listen to foreign speakers who are talking about COVID lockdowns in China or democracy protests overseas. And so one of the points that we are emphasizing today is banning TikTok, like banning a newspaper or banning a radio station, is the kind of step that an authoritarian government like China's would take, is not the kind of step that the government in our democracy should be taking.

Jessie Bur:

And would a ban like that create an element of legal precedent for lawmakers or a president or whomever to go after any app that they didn't ideologically agree with, the large user base?

Patrick Toomey:

I can start by saying it is certainly a slippery slope. Many of the top apps in the Google and Apple app stores right now come from China. And many of the proposals that are being written would not, some of them would apply only to TikTok like Montana's ban that was adopted yesterday. But some of the federal proposals would give the government far broader powers to, in the right conditions, ban a range of apps.

Patrick Toomey:

And I think the other piece of that precedent setting question is, what does the US banning an app say to other countries around the world? Of course, China has already taken steps to restrict information, but it gives other governments that have not yet taken those steps a much greater foothold or talking point to say, "Well, the US is banning apps, we should do it too." And you start down that road and you really have a splintering of the internet, I think.

Jessie Bur:

And many government agencies at the federal and state level have banned their employees from using TikTok on work devices, which is a lot more cut and dry. They can require whatever they want for their IT. But do you think that those agencies are missing the larger point of all the social media apps and the data that is exposed by using them?

Alan Butler:

Yeah, I think that one set of concerns maybe that we haven't talked about quite as much is there's data access and data protection concerns related to the user information that's collected by TikTok surrounding services. And then there's also the sort of outward capabilities of the mobile devices themselves, and which, if any of those are exploitable or accessible, basically like mobile devices with apps as an attack vector in the cybersecurity space.

Alan Butler:

And I'm sure that's an area of significant concern for federal IT officials, for example. But again, not unique to TikTok. I think that that requires a more fundamental, again, both rule set, norm set and actual practical application for app store vetting of apps, meaningful control over what apps can actually do, again, both at the legal and technological level.

Alan Butler:

So again, I do think there is a little bit of a missing the forest for the trees with focusing so much just on this one app because of its particular ownership structure.

Patrick Toomey:

All I'd add on that is we certainly think of decisions by government agencies about what software goes on those devices as a completely different question. And there can be real risks. TikTok has been banned, but there are stories just a few years ago about Strava exposing the location data of service members and those types of wearable health and exercise devices revealing sense of information. Those are perfectly legitimate concerns.

Patrick Toomey:

What we're seeing with TikTok though, is that some states haven't just moved to ban it on government devices, but have also moved to ban it on university campuses where they're students at public universities. So I think those types of situations raise a different concern. Students on those campuses are using TikTok on their personal devices for, again, First Amendment protected expression and activities. And so those may need to be evaluated in a different way from the employee device bans.

Jessie Bur:

Right. And I think we've touched on a couple elements of this, but what would a true data privacy protection law or regulation require to get at the heart of the data that many of these social media apps collect?

Alan Butler:

Yeah, I think there's been, as I mentioned, a phenomenal amount of work done. Obviously this has been a long-running effort by many entities and organizations, us and others, ACLU included. But even in the last year and a half, two years, the evolution we've seen in the conversation around privacy standards has been phenomenal.

Alan Butler:

The bill I mentioned, the American Data Privacy Protection Act adopts really for the first time at the federal level of proposed standard that would impose data minimization rule, where you actually have substantive limits on what data entities can collect, personal data they can collect, how they can use it, and in what circumstances it can be transferred. And even a more heightened standard protecting sensitive data categories, which include a lot of things like precise location, health information, biometrics, and other sensitive data. And we really think that that's what's necessary.

Alan Butler:

There's been a long-running conversation in the past about different types of data regulatory models focused a lot on opt-out versus opt-in and how consent flows work. And we truly believe that that is not where the conversation needs to go at this point, that we really need to talk about directly and substantively restricting improper uses of data that we.

PART 2 OF 4 ENDS [00:22:04]

Alan Butler:

... restricting improper uses of data that we see as harmful and as major threat vectors for these types of apps.

Jessie Bur:

Right, because is the average person even able to fully understand what kind of data they'd be signing away in that context?

Alan Butler:

Right. A lot of focus in the past, again, has been on, let's say, setting up the set of individual rights under a traditional data prediction regime. Rights that are, in no doubt, important of access in some cases to delete perhaps or correct data, but focusing too much on an individual rights based approach is a losing game when the amount of time it takes for the average person to do that for every single app they use quickly outpaces anyone's ability to actually manage that process. And you don't want to end up with a situation where we just live in a world of popups and notifications. "Oh, I see that." And just wiping them all away. That's why we believe fundamentally it needs to be about limiting the unnecessary collection and use of people's personal information.

Jessie Bur:

Patrick, do you have anything you'd want to add to that ideal data privacy?

Patrick Toomey:

I think we agree that collection in the first instance is where you start and agree with the other kinds of proposals that Alan mentioned. On top of that, we certainly don't think that the platforms are angels, and that's why we think there need to be these regulations. Another dimension of bringing accountability to the platforms is greater transparency, and there are hard questions about how to give researchers and academics and journalists access to information about how the platform's algorithms work, but that is another piece of the puzzle.

Patrick Toomey:

One of the concerns in this area is disinformation, propaganda, amplification. And in order to really assess the effects of those recommendation algorithms, we need to be able to understand how they work, and not just in the bits and pieces that the companies share, but with access from independent people outside the companies. And so I think that's another piece there. There's privacy issues there too. It's not an easy solution, but there needs to be more that can help us understand how the algorithms work and what effect they have on audiences.

Jessie Bur:

And do you think that members of Congress and now because of the Montana law, state and local lawmakers, by and large have the political or the technological acumen to effectively craft this kind of legislation?

Alan Butler:

I think that the process, again, that we saw over the last year had been a robust one. I mean, the ADPPA last year went through subcommittee and committee markup. And overall, I think that the feedback and input that we saw from across the spectrum was all very positive. Obviously, on the house side, not every individual member is going to be in the weeds of the technical level of the law, but I think also a good law that addresses privacy and data protection doesn't have to be deeply technical because the standards need to be able to be applied across different apps and services. And it's really just about making sure that the law doesn't break things or that the law actually works in practice.

Patrick Toomey:

I think there's a learning curve and there are a lot of legislators who are genuinely committed to understanding how all these different platforms and tools work and coming up with solutions based on that. I think there are examples though, where the technical part of things has not been the central concern. I think we see that in Montana's bill. The questions about how it would be implemented and enforced, the basic mechanics are that TikTok is not allowed to operate within Montana and app stores like the Google App Store and the Apple App Store can't offer TikTok to people within the state of Montana. But certainly there are ways that users could, in theory, get around attempts to geofence and prevent people from Montana by using VPNs. People connect to cell towers out outside of Montana State lines. So there's a lot of questions about technical implementation, and there's been a lot of criticism amongst experts about how Montana wrote its bill, even if one agreed with its goal, whether this would be the way to accomplish it.

Jessie Bur:

And this legislation for a single state is almost inviting these companies that we've established collect large amounts of personal data to collect more data from people all across the country. And so Montana's having an outsize effect on the data of people outside of the state borders.

Patrick Toomey:

I think that could be one consequence because now, TikTok needs to know where everyone is. Are they in Montana or out outside of Montana? It will need to know where individuals are in order to permit them access to the app or not. And so you could have this ironic follow-on effect where TikTok now is collecting more granular location information than it would otherwise be doing.

Alan Butler:

And one of the themes that we've been building on a lot as we analyze and look at both the federal bill, the state bills, and rule makers that are going on in California and Colorado, and also the regulatory actions at the FTC is really looking at data minimization, minimizing collection, as Patrick mentioned, and retention of data as a cybersecurity measure because the more data that is there, the bigger a target is on the companies that are holding it. And so deeply counterproductive and ironic if the result of a single state trying to ban TikTok for privacy reasons is to exacerbate privacy risks where they really should be, again, focusing on minimizing both the data that our other apps are collecting and what can be done with that data in a meaningful way that we think could be really effective.

Jessie Bur:

And as far as I'm aware, I don't think we have anyone here who's writing laws, but for the people who are working IT at agencies or just concerned about the exposure of their workforces, what are some considerations that you guys would recommend for those IT people that are just trying to make sure that they're protecting their agencies and their employees to the rest of their abilities?

Alan Butler:

I mean, I think to the extent that folks are looking at different apps or services, obviously there's been an improvement, as Patrick's said, about transparency with Apple's ATT and other services about actually displaying what types of data apps can access or use. So that's a helpful way when there's internal auditing going on, and a lot of some app stores and a lot of apps have maybe improved some of the individual controls. But again, it's hard at an individual level, especially if they can't be set organization-wide. But I think those are some of the better tools we have at the moment.

Patrick Toomey:

I mean, the only thing I'd add is if you're working at a company that's designing a system that's going to collect information, as I'm sure you know and have thought about, thinking through exactly what data is needed and for what purposes and is collection necessary. I think in the past, we've seen instances where data's collected just because it's available, with the idea that it can be used commercially in some ways going forward. And that's the kind of thinking that the laws and protections that Alan's describing, we've been talking, about are designed to foreclose by making sure that there's a really close fit between the need to collect information, the sensitivity of the information, and how it's ultimately used and potentially retained.

Jessie Bur:

And do you think agencies today, without any changes to law, have some avenues to hold apps like TikTok or any of the social media apps' feet to the fire a little bit and make them aware that there could be consequences for excessive data collection?

Patrick Toomey:

I can start by saying, I mean, with respect to TikTok, there already is a process in place, the CFIUS process, Committee on Foreign Investment in the US, which has been evaluating TikTok's acquisition by ByteDance for a number of years. And one of the proposals that grew out of that process is this proposal Project Texas it's called, to House Americans, the data of American TikTok users inside the United States to at least better protect it from any demands from the Chinese government. And those negotiations are ongoing, but that's one example of the government exercising the ability to review these types of risks when it comes to foreign entities.

Alan Butler:

I also think that this may happen at a higher point in the chain of decision making at agencies, but at some level, federal agencies are signing very large contracts with some app vendors or providers, especially if you're talking cloud or if you're talking larger service set apps. And there's the ability to put terms and contracts. I mean, if you look at, even recently, some of the new consent orders or actions that are coming out of the Federal Trade Commission, where they're putting meaningful restrictions on entities' ability again to collect and use certain categories of sensitive data, that sort of thing can be a key point at the negotiating table. And even many apps have default settings about what they collect and how do you take precise geolocation information as an example. That's a setting that can be changed. And maybe if you have sufficient buying power as a federal agency, you can impact that and influence it. Maybe not even for yourselves, but for others as well if it's a broader change.

Jessie Bur:

And by writing off social media apps like TikTok, are agencies missing out on the opportunity to communicate with constituents...

PART 3 OF 4 ENDS [00:33:04]

Jessie Bur:

... on the opportunity to communicate with constituents where they are?

Patrick Toomey:

I think it depends on the agency and what its goals are and how it evaluates the app and some of the risk we've talked about. I think, from the perspective of a non-profit, not a government agency, TikTok has proven a very, very important channel for reaching especially younger audiences. There are many people who get their news on TikTok today, many people who are there to learn about the world, and that can include the activities of government agencies that are there to help serve and protect the American people. So, I think that should be part of the equation when evaluating whether to use the app.

Jessie Bur:

And are we able to pull the poll back up real quick? Because I am curious, to close us out ... Wonderful, thank you. Has anyone here changed their minds?

Speaker 2:

No.

Jessie Bur:

I guess raise your hand if you did change your mind. No? Okay. So we're still a very suspicious audience. That's fair, I think. I think that-

Speaker 2:

[inaudible 00:34:09].

Jessie Bur:

Like you said, it's a cybersecurity summit. Most of the people here are going to be very leery of any kind of threat, but I do think that this is a really valuable discussion to broaden our understanding of what the threat landscape is beyond just a particular app.

Speaker 4:

I mean, I just [inaudible 00:34:31].

Jessie Bur:

Okay. I don't know what that says about what we've been talking about here, but I'll take it. All right, excellent. And we've got like three minutes left, so if anyone has a question. Let's see here.

Speaker 4:

Yeah, so-

Jessie Bur:

Oh. You go ahead.

Speaker 4:

... is there any other company in the same position as TikTok?

Jessie Bur:

Is there any other company in the same position as TikTok? In what regard?

Speaker 4:

Why are we focusing too much on TikTok itself? Because I know China-

Jessie Bur:

Right.

Speaker 4:

[inaudible 00:35:08]. Is there any other reason other than China?

Jessie Bur:

Is there any other reason besides China that people are so fixated on TikTok?

Speaker 4:

Correct.

Alan Butler:

I mean, I think the reason I mentioned earlier, in addition to the connection with China, I think there is, between the TikTok challenges and sort of a lot of the discussion around the types of content that are on TikTok, I think there has been an increased focus on that app because of content moderation issues.

Patrick Toomey:

I mean, I think it's also the size of the platform, but that raises the slippery slope question, because I think three or four of the top 10 apps in the App Store are based in China today. So if we start by banning TikTok because it's in China, based in China, because it has many users, where does that lead us? And I think that's a big part of the concern, and we think that there are other measures that could be taken to mitigate those risks without banning that entire app and preventing 150 million Americans from using it, from preventing hundreds of thousands of Montanans from both expressing themselves there and from accessing information from others.

Speaker 4:

Thank you.

Jessie Bur:

We've got one up here on the front. Got it. We've got a mic running to you. Give him one sec.

Speaker 3:

Thanks. So it's hard for me to disagree with anything that either of you have said from a technical analysis. I'm curious what your thoughts are from a practical analysis, what's going on in Montana as a representative reaction, based on what you just said, probably on volume. It makes me wonder, if you have an opinion on this, what is actually going on in Montana? Is it a learning deficit that they're reacting because they don't understand? Or do you think there is some other agenda that they have?

Speaker 3:

Because the backdrop to that question is, how do we as a nation, and you're part of it, how do we keep up with the speed of these situations that are going to constantly happen with AIML lurking in the background? How do we maintain the principles that you're advocating, again, which I, on your technical analysis, I cannot disagree with, but practically, how do you keep pace? I'm defending an asset, my nation. It's always harder to defend the asset. It's a lot easier to find the vulnerability and attack the asset than you're ... The defender's always reacting. Do you think there's something else going on in Montana?

Patrick Toomey:

I mean, I think that there's a generalized concern about the geopolitical risk that China presents today in many parts of the country, but that has prompted some very extreme steps that aren't justified by at least what the public evidence shows right now. And in certain ways, hearkens back to some of those efforts to ban works of art and literature in previous eras.

Alan Butler:

I think that there are ... I don't want to say it's a learning deficit. I mean, I think that there are parallel actions happening across the country in the last few years that there is a mounting response to the problem of both invasions of privacy online, these sort of related national security type threats, and also the issues of proliferation of things like harmful content, disinformation, misinformation. So we see Montana passes the TikTok ban. Other states are passing laws focused specifically on content harm for children that have a wide range of interventions and sort of pluses and minuses to them, right? So Utah passed a bill that has a significant age verification component that we're not fond of, as well as more kind of fundamental bands on access that I'm sure you and others have positions on.

Alan Butler:

And in contrast, California passed a bill called the Age Appropriate Design Code that's much more focused on how apps and services are designed with respect to the information they collect about children and how they use that in different ways. For example, to target content. And meanwhile, California, Colorado, Vermont, Virginia, a bunch of states are passing privacy bills at the same time. So I do think that there is mounting action across the board, even when there's one example of Montana doing just an outright ban on one app, that I do think speaks well to our national response. Our national response is not summed up in the Montana bill. I think it is the full gamut of activity that's going on, and there really is a call to action to really get a handle on these apps and how our personal data's being dealt with.

Jessie Bur:

I think that's a fantastic way to end things. Thank you guys so much for taking the time. This has been an amazing discussion, and we have reached the end of our time, but I want to thank all of you guys for watching and participating, and hope you enjoy your next panel.

PART 4 OF 4 ENDS [00:40:27]