The Free State Foundation's
Privacy Seminar

"PRIVACY REGULATION:
WHY, WHAT, AND WHEN"

June 26, 2019
National Press Club
Washington, DC

"PRIVACY REGULATION: WHY, WHAT, AND WHEN"

PANEL DISCUSSION

MODERATOR:

Seth L. Cooper, Senior Fellow and Director of Policy Studies, The Free State Foundation

PARTICIPANTS:

Kelly Cole, Senior Vice President of Government Affairs at CTIA

Lynn Follansbee, Vice President, Policy & Advocacy at USTelecom

Loretta Polk, Vice President & Deputy General Counsel at NCTA - The Internet & Television Association

Michelle Richardson, Director of the Privacy & Data Project at the Center for Democracy and Technology (CDT)

---

* This transcript has been edited for purposes of correcting obvious syntax, grammar, and punctuation errors, and eliminating redundancy in order to make it more easily readable. None of the meaning was changed in doing so.

P R O C E E D I N G S

MR. COOPER: Thank you for joining us today. We are now at the panel portion of our event on Privacy Regulation: Why, What, and When. I will introduce our panelists.

First, we have Kelly Cole, Senior Vice President, Government Affairs, at CTIA, where she oversees CTIA's Hill team in advancing the wireless industry's priorities before Congress. That includes issues not only such as privacy but certainly spectrum policy, 5G infrastructure deployment, combating robocalls, and any number of issues.

We also have with us Michelle Richardson. She is Director of the Privacy and Data Project at the Center for Democracy and Technology, where she leads CDT's efforts to create a user-centered Internet. Her team engages companies and government officials to create policies and technical solutions that protect individual privacy, empower users, and advance social justice.

Next, we have Lynn Follansbee. She is Vice President of Law and Policy at USTelecom. She provides policy analysis and legal and regulatory support to

USTelecom and its members on a range of issues including privacy, consumer protection, universal service, and mapping. She represents USTelecom and its members before the FTC, FCC, and other federal agencies.

And we also have with us today Loretta Polk. She is Vice President and Deputy General Counsel at NCTA, the Internet and Television Association, where she leads NCTA's privacy and cybersecurity, legal, and policy work. She has represented the cable industry on a wide variety of legal and policy regulatory matters, including consumer protection, video and broadband technology, competition, and public safety.

So now each panelist will speak for up to five minutes with some initial remarks on our topic today about Internet privacy regulation. I will give the panelists at the end of that time an opportunity to respond to each other if they so wish. Then I will ask the panelists questions. And, if we have time, we will get some questions from the audience as well before we move into our closing keynote address.

We will just go down the line and I will start with Kelly Cole from CTIA.

MS. COLE: All right, thank you very much. And a huge thank you to Randy and Seth. Thank you for inviting me here today and to the Free State Foundation. And I'm thrilled to see a lineup of three other very talented women. I so love it when that works out.

When I sat down and started thinking about this topic in a little more of a granular way, there obviously seems to be consensus among policymakers, consumers, and industry, in what is turning into being a very data-driven world, that we need to provide more control to consumers over their personal information. And CTIA and our membership very much support a comprehensive, technology neutral federal privacy law that's enforced by the FTC.

There is no doubt that there are a lot of benefits from sharing data. I can get an Uber wherever I am on whatever corner I may find myself. I love the fact that I can save money on my groceries with a loyalty program. But we all need to recognize that the sharing of that data needs to be done carefully and needs to be done appropriately. Or people, frankly like me, are going to turn away from a lot of new technologies that ultimately will benefit consumers.

So a big part of what's driving this debate inside of CTIA is really the importance of consumer trust. At CTIA, we represent the wireless carriers, we represent the phone manufacturers, and the folks that make the guts of a mobile phone. We're in the business of providing an infrastructure that allows people to share that data. So we have every incentive to develop strong and robust privacy rules that ensure our customers come back to us.

And we just released over at CTIA the 2019 Annual Wireless Industry Survey, which I thought provided some really interesting data nuggets for why this is becoming increasingly more important for every industry, but in particular CTIA's membership. Wireless demand is growing at an incredibly staggering rate. And these numbers frankly caught me by surprise. Americans used 82 percent more mobile data in 2018 than they did in 2017. I mean, that blew me away: 28.5 trillion megabytes of mobile data in 2018. And, of course, layer on top of that the fact that everything is connecting to everything else. So this whole notion of the Internet of Things just makes this conversation increasingly more important.

The consumer trust angle is something we take

very seriously and we view as very critical. And there is no doubt that consumers care about this issue. I'm sure many of you saw there was a *Morning Consult* poll that came out in May of this year. Eighty-three percent of consumers expressed support for a new privacy law. And 73 percent of those say they strongly believe that data privacy protections should not depend on where they live. Which for, certainly, my members in my association is critical to this overall debate. I actually drove across the country over Memorial Day recess, went through 11 different states. And, whether I was on Facebook driving in between Oregon and Utah or on Amazon buying something between Florida and Georgia, I think it's only fair that as consumers they know what the rules are. And it's completely unfair to consumers to have a patchwork regime of up to 50 different state laws that don't protect privacy the same way.

As we all know, the Internet does not respect state boundaries. That's just not how it works. And so it's obvious to CTIA and our members that we need a national privacy regime.

I come to this as our chief lobbyist over at

CTIA. I spend a lot of time on this issue on Capitol Hill, so I really look at this through the lens of "What is Congress going to do?" And I am hopeful, certainly hopeful, that we get a law this year out of the House and the Senate. The Senate has obviously been spending a lot of time on this issue. There is a gang of six. It recently added Senator Thune and Senator Cantwell to that mix. They're having discussions. But this has been going on for months. These negotiations have been happening for months, which just underlines how difficult this issue is. It is hard, it is dense, it can be emotional. So there are a lot of things that still need to be resolved.

But again, I am very hopeful that we can get a product out of the Senate that can hopefully pass the House. And obviously, our goal would be to see that language and legislation pass by 2020, before we have to deal with California law coming into effect.

I think that's probably my five minutes, so I'm going to hand it over.

MR. COOPER: Thank you. Michelle Richardson, Center for Democracy and Technology.

MS. RICHARDSON: Thank you. We are very excited

about the unique opportunity we're facing right now and the possibility for a federal privacy law. I understand this comes up every five years or so, but this time it feels different. And I would say it's because we know more than ever about how technology works.

You can see the learning curve on consumers collapse in real time. It's partly from great journalism, academic research. And people now understand what's at stake with this data.

You can't say, "Well, just get off Facebook if you don't like Facebook." We have now come to realize that everything is connected – our cars, our homes, our children's schools, our workplaces – and there is no way to opt out of data collection anymore. It has brought us great benefit, but it is time to start dealing with and minimizing some of the risks that it has brought into our lives. And this means rebalancing power between companies and consumers.

We are woefully out of whack and this is because we have sat out the development of privacy law for so long, while we have our sectoral laws like banking and health care, for example. Those now have to represent a

tiny fraction of the data that is created and out there about us and used in ways to make very important decisions about us every single day.

So what would be the principles of what legislation should look like? One, everybody should be treated the same. I think there are questions about banking and health staying where they are. But for everyone else – whether you are a brick and mortar store, a telecom, or a big tech company – we need one set of rules here. We have to move past chunking up the different pieces of our economy because it doesn't really matter anymore. The data is so fluid and it really doesn't matter who holds it.

We need to shift the burden to companies. Like I said, we are in an always-on society and there is no way for individuals to understand and manage all the different relationships they have with companies.

When my boss testified recently, we tried to quantify what it means to be out and online in the world. And we looked at her phone and she has 260 apps on it. That's just her phone, that's not her laptop at home or her work laptop or her Amazon or her connected car or her

Fitbit. She is a tech enthusiast.

When you add up all of those different devices and accounts, there are hundreds if not thousands of companies touching her data and your data every single day. There is no way for any of us to micromanage those relationships, even if you're the smartest person who understands how all of this works.

We would like to see clean lines, too. We understand there needs to maybe be some play in the statute that allows for innovation or advertising. But the most important thing we can do here is set some clear lines and boundaries about what's inappropriate. We now know what types of data use lead to exploitive, abusive, or privacy violations and we just need to be clear about that. And I would agree with FTC Commissioner Phillips that it is Congress's job to actually draw those very clear lines.

And finally, we have to just get at the issue of collection, sharing, and use of data. I think that probably sounds silly, but by the time you talk about all the other issues out there, you realize you never actually got around to the privacy part of the privacy law. Which

is, what are the rules for collection, use, and sharing of data. And I think we are maybe a little too negative about what's possible. There are huge advancements in technology now and ways to process data in privacy protective ways. It is not impossible. So if we have large companies that are going to do very advanced data processing, we should expect very advanced privacy policies from them.

I can get into more detail later. But I will just say, also, beware of sideshow issues. This is going to be controversial.

One, transparency. I think a lot of people want to start with transparency: "Just tell people what happens with their data." I don't want you to tell me what you're doing, I don't want you to ask me. I just want you to stop doing things that are exploitive or violating privacy. That's the entire point of the law. We are in a unique situation where we need our government to negotiate a better deal for us. There is nothing that we as individuals can do about this, no matter how much information we have.

And, two, we need to move away from user

responsibility. We need to make it much easier for what people understand, on the surface, products to be enforced. So, for example, when I use Google Maps, I understand it's going to track my location. That's the whole point of it. I don't know that some silly game I put on my phone for my child is surreptitiously collecting it solely for the purpose of selling it. We have to limit those secondary uses that are not apparent on its face.

We want to move away from the model of data as something you own and that you should be paid for. This has gotten more traction over the last few months. I really didn't expect it to. But we have to be realistic that, again, that model doesn't affect the collection, use, and sharing of your personal data.

And I think people would be shocked to find out how little their data is actually worth. There was a great story in the *New York Times* about precise geolocation tracking from your cell phone. And apps that are collecting it and selling it on the open market get about 10 cents to 25 cents a year per user. So who is going to take the time to go get their two cents for the location data from the hundreds of different companies that have

it? It is not going to be a way to actually change systemically how this works.

MR. COOPER: Thank you. Now we will move to Lynn Follansbee, USTelecom.

MS. FOLLANSBEE: Hi, thanks for having me here today. Just for those of you who may not know, USTelecom represents broadband providers. Our association was traditionally the old wire-line telephone companies, but we are now broadband providers and Internet service providers. So that is where we come from. Our association also represents not only the biggest broadband providers but also some of the very smallest rural providers throughout the country, sometimes just as small as serving one town.

So this is important. This privacy issue is important not just to some of our biggest members but also to our smallest. Quite frankly, when there is regulation in this space, the impact has to be considered down to the very smallest provider, not just what the big companies have to understand.

USTelecom supports the adoption of a strong national privacy framework governing all the stakeholders

in the Internet ecosystem. As other folks have said, we think it's really important to balance the need for strong, clear protections for all American consumers with an approach that continues to allow for the unparalleled innovation that has driven the Internet economy to where we are today. Our companies have always put a priority on their consumers. And I know, going back to just a few years ago in 2017, our multiple associations had reaffirmed their commitment to the FTC policies on transparency, consumer choice, data security, data notification. And we have a longstanding set of principles that we abide by, have always abided by, and continue to abide by up to today, even in the midst of this giant debate that we're having.

The need for federal legislation that establishes a strong national privacy law will make it easier for consumers across the country. It will be really clear for them. And this existing and expanding patchwork of state privacy laws is only creating a fragmentation in the protections and resulting in inconsistent protections for consumers. National privacy legislation that preempts the state privacy laws would avoid this patchwork and provide

a really consistent, clear way for consumers to navigate this space. Additionally, we believe that legislation would serve as a good opportunity to further clarify and enhance the FTC's role to police privacy practices and protect consumers, while at the same time preventing inconsistent regulations and helping to expand innovation.

MR. COOPER: Thank you. And Loretta Polk, NCTA.

MS. POLK: Great. Thanks, Seth. I guess the beauty of going last is I can say there's a lot of commonality among the speakers here at the table. There is broad alignment around a lot of the issues in the privacy debate. And as we heard from Commissioner Phillips, there are forces in Washington and abroad that are driving action toward privacy. After years of working on this issue, we may finally see Congress move forward. All of this is combined with the FTC's ongoing examination of competition and consumer protection policy in the 21st century. And this has all intensified, in our view, the need for Congress to comprehensively address privacy at the federal level.

For over 30 years, cable operators have taken steps to ensure the privacy of their cable television

subscribers in accordance with strong protections enacted by Congress. And cable broadband providers similarly have been guided by the key principles that embody the FTC's privacy framework that's been developed over several decades. The privacy protection measures taken by cable companies reflect not only federal policy and law but a business imperative to strengthen customers' trust, as we heard earlier, and by showing that we are responsible stewards of our customers' personal data.

But with the online abuses that have come to light in recent years, it's time, we think, for lawmakers to go a step further and codify strong and enforceable consumer privacy protections for the Internet. We, like others, support establishing a uniform technology and competitively neutral national policy for privacy that protects consumers from harmful misuse of their data but also allows for innovative new services. We think broadly applicable national standards would serve the important interests of protecting consumers and promoting responsible data uses and innovation in the digital age.

This means the consumers should have meaningful transparency, choice, and control of their data security

with respect to how it's handled, regardless of where they are or what product or service they are using. Consumers should also have reasonable rights to access, delete, and correct their data. And federal privacy standards should be flexible and agile enough to allow for changes in technology and business models.

The federal framework should be built on FTC authority to continue to enforce violations and, where lacking, the law should provide the agency with necessary resources and authority to be optimally effective.

Regulatory parity. That is a very important issue for our companies. It is critical in a vibrant and dynamic segment of the economy to ensure that market forces and consumer preferences dictate marketplace outcomes. Parity ensures that consumers are afforded consistent privacy protection as they navigate the digital marketplace, regardless of the identity of the entity they are interacting with and the service they are using, or the nature of the technology employed.

As we've heard throughout the day so far, the potential for national fragmentation of privacy policy and regulation from the emerging patchwork of state laws has

heightened the importance and urgency of enacting a single national policy related to privacy in the U.S. Otherwise, companies' day-to-day practices in the management of data would need to vary state by state, when network infrastructure and systems and the Internet itself are borderless. A patchwork of state and local laws imposing diverse obligations on how companies collect, use, and share data will only confuse and disrupt the consumers' online experience, and also potentially impose disparate costly burdens on businesses. Consumers will benefit from the predictability and consistency of a uniform national privacy policy over conflicting state-by-state regimes.

So a few more points. While only Congress has the authority to comprehensively establish a single national privacy framework administered and enforced by the FTC which preempts state law, the FTC, as the nation's lead privacy enforcer, has an important role to play going forward. The Commission can continue, under its existing authorities, to make progress on privacy policy and guidance in tandem with legislative efforts in Congress. Indeed, the work the Commission does now in advancing a national privacy framework can help shape the approach

taken by Congress.

The FTC's longstanding privacy framework continues to work effectively to balance the various goals on both the consumer and business side. But as the Commission revisits consumer protection in the 21st century, we think it should look to refine its framework in light of recent developments and emerging issues. This might include strengthening mechanisms for safeguarding consumers against unexpected access or use of their data by third parties, improving or supplementing the notice and choice model to provide consumers with additional privacy protection, promoting the use of effective de-identification techniques and controls, and identifying harms that the Commission's privacy framework should address. It also should look at adapting its framework with respect to new areas around artificial intelligence and algorithmic discrimination.

So in sum, there is broad support for baseline privacy legislation. The challenge, as we've heard, is translating widely agreed-upon principles into a substantive legal framework in a complex area.

The cable industry is committed to working with

government and stakeholders to meet this challenge and to enact a comprehensive national privacy law that provides consumers and companies alike with a consistent set of rights and obligations that both strengthen privacy protection and advance competition and innovation.

MR. COOPER: Thank you, Loretta. Thank you to all the panelists. Is there anyone who has a response to anything they've heard to this point? Okay.

Well, I'll jump right in with some questions here. And I will direct this first one to you, Kelly. You work on the Hill. Is there any kind of legislation in Congress that you see on the horizon? I mean, you mentioned a Senate gang of six. Do you have any more meat to put on those bones or a sense of where that's going?

MS. COLE: I wish I did. No, there are a lot of bills, frankly, floating around Capitol Hill right now. You know, it's the issue *du jour*; everybody wants to get in the game on privacy.

I think the bipartisan gang of six that we've seen is probably the farthest along in doing the work in a thoughtful, meaningful way. The fact that it is bipartisan, and you literally have members from Senator

Wicker to Senator Blumenthal, you've really got the spectrum of ideology there. And they're all sitting down and working through these issues.

Just this morning I read that Senator Wicker would not make a commitment that we would see a bill before the August recess. So, like I said, these are very difficult, dense issues. I think the good news is that they're actually talking about what we would hope would be discussed towards the end of the process. And things like private right of actions, state preemption, some of these really big, thorny, meaty issues that are, frankly, going to take some time. But I'm hoping that means, to Michelle's point earlier, that they have dealt with the true privacy issues, and they're hashing out those final remaining really controversial issues. That's my hope.

MR. COOPER: Michelle, you talked about having Congress set clear lines and boundaries addressing, separate from consumer consent, certain uses of data that are just harmful to consumers. Can you give some examples of things Congress should consider as being beyond those boundaries?

MS. RICHARDSON: There are two things that we

often focus on at CDT. One is discrimination. And this is not price discrimination, but the data is being used and processed constantly in ways that make decisions about people. This could be big stuff like mortgage rates or the advertisements you see for educational institutions. Or it could be small things, too. Because all this is so opaque and hard to track, we need to be more aggressive in making sure that it isn't obscuring things we don't want to happen.

The second thing, though, is that we are really leaning hard on limiting secondary uses. What we find in FTC enforcement and talking to people, even people at small businesses, is if you're offering the actual service someone requested, they are very forgiving. They understand that there is a universe of things that has to happen with their data. But it is always that secondary use, where it is something wholly unrelated, that offends people. And that's what is also the most dangerous. Because the data is usually going to someone who doesn't even have a relationship with the person. Frankly, what do they care? No one is going to hold them accountable. It's hard to track this.

So we would say those are two areas where you can do clear lines. And we know that makes people uncomfortable. But I think it will benefit small businesses, consumers, and enforcers to work on a smaller list of activities or data sets and make clearer rules.

MR. COOPER: Loretta, you were talking about the issue of patchwork state regulation and the conflicts that that would impose. I don't want to be imposing things on the panel, but there seems to be a consensus that we need to have some kind of national standard.

Now, the FTC held a hearing on June 12 that featured state AGs and state officials. And I would say there seemed to be a consensus going in a very different direction. I remember one state official saying that simply having multiple privacy regimes doesn't, by itself, make things impractical. And that talk of harmonization among privacy regimes would create a lowest common denominator approach.

That's a very different viewpoint. Do you have any response to these kinds of arguments from the state side against preemption?

MS. POLK: Well, first of all, I think we would

fundamentally disagree with the premise that harmonization means that a privacy policy at the national level is going to be weak. I think everyone at the table here and all of us working on this would like to see a comprehensive law that gives consumers significant rights going forward with respect to the use, collection, and sharing and disclosure of their data. So I don't think it necessarily means there's a rush to the bottom here, in terms of a national level.

I do think state AGs have a role and should be given the opportunity to stand in the shoes of the FTC where it's appropriate to bring a lawsuit in a state where their citizens have been affected by the national law. But, of course, the FTC would have the overriding authority there to step in if needed. I think state AGs have an important role going forward. But preemption of state individual privacy laws is critical going forward, given the potential adverse effects of a patchwork.

MR. COOPER: All right, thank you.

Lynn, during your talk, you discussed a national framework and, as part of that, an enhancement of the FTC's authority and its role. How can an overarching

privacy statute that could be very broad confer rulemaking authority that can address something in a way that doesn't give too much power, too much discretion to the FTC? As we heard from Commissioner Phillips this morning, a lot of consumers have very different expectations and how they want to use data. How can you control for something like that in legislation that touches on FTC authority?

MS. FOLLANSBEE: Well, I think the key, and I think Commissioner Phillips touched upon this, is that if the FTC has some limited rulemaking authority, it could potentially help down the line so that we're not back revisiting this issue in a few years. We're talking about trying to balance the need for consumer protection but also allow for innovation. The Internet is where it is today because there have been great innovators who have expanded it to all these cool things that you and I get to do over the Internet. I don't think I go to a department store anymore; I'm an Amazon addict. That's something that I think is a really great part about the Internet.

So I think you can carefully walk that line by giving the FTC some limited rulemaking authority in order to allow for changes as we move over time. There are new

innovative ways for the Internet ecosystem to grow. And use rulemaking to help work through it as it changes.

MR. COOPER: Okay.

MS. FOLLANSBEE: And additionally, let me just say also I think we're very supportive of giving the FTC some additional resources. Right now, I think there are about 40 people that work in their privacy office. And if you think about the largesse of this issue, there should be way more than 40 people working on privacy.

MR. COOPER: Now, Michelle, when Commissioner Phillips spoke today, he mentioned private rights of action, civil penalties, and FTC authority to impose civil penalties for first-time violators. Do you have any views on those particular kinds of remedies?

MS. RICHARDSON: Sure, I will add something on private right of action. I think people are oversimplifying it. You hear people say, "We want to be able to sue over everything," and others say, "We want to sue over nothing." And there are a million options in between. The reality is, right now, there is a right to sue in all 50 states. Taking that away from consumers is a big change. It is a serious decision to tell people

they are not allowed to access an entire branch of government. That's what people are suggesting. That's a big deal.

So is there some set of harms that we think are so important or are better served by individual litigation? And so I would point to the 50 states, they have mini-FTC Acts. They have their unfair excepted practices, too, and that's how they do privacy enforcement.

You could look at them and they are very diverse. Some ban class actions, some have a very limited harm standard, some don't allow recouping fees. There are just so many options here that we should talk about to make sure that consumers can be protected. Because I think even if you've got the FTC, and you have your state AGs, there are going to be violations that only impact a small group of people. Or an individual. If something happens to your data, do you expect the FTC to actually sue for you? Not going to happen.

So if we are going to preempt all these state laws, we need to be realistic about how we make sure users can be empowered to protect their own interest in some

situations.

MR. COOPER: Kelly, I want to take it back to you, getting back to the Hill and legislation, there isn't a lot out there yet. But can you at least comment on, the things that you really don't want to see coming into privacy legislation?

MS. COLE: Private right of action. (Laughter.)

MS. COLE: Yes, that would definitely be on the list. And I do look at this in sort of the opposite frame. Like, what do we need to have in there? We would include things like state preemption, which is really, really important when you talk about creating a potential patchwork of 50-plus regimes. That's just not something a consumer is going to be able to manage and it starts not to mean anything.

We need it to be technology neutral, to the point that was made earlier. We believe everybody should be treated the same under this regime. And really important to the sectoral point, we want to make sure we don't have multiple regulators. Really, the FTC is the right place to house this authority. They have the expertise. They've already brought over 500 privacy-related actions.

They know what they're doing, let's put them in charge.

And then on the rulemaking piece, we're not against a limited role for rulemaking. We just want to make sure it's actually limited.

And I think the Commissioner made a perfect point. We don't want this to turn into a net neutrality debate where every four years or every eight years, we're seeing these massive swings, which give no consistency, no predictability to consumers or to industry in how to provide these protections to consumers.

MR. COOPER: Thank you. I would like to direct another question to Loretta. Now, the FCC, the Federal Communications Commission, does have a kind of narrow slice of privacy jurisdiction. Yes, this could easily go to Lynn, and I would be interested in your take as well. It has to do with CPNI, customer proprietary network information. That's the subscriber information that voice telephone providers, cable providers, DBS providers have or they receive from their subscribers, and then the FCC has authority over their collection and use of that subscriber information.

So if we've got that out there, that FCC

authority and we're looking at an overall national framework, where does the CPNI go? Does that stay where it's historically been, at the FCC? Or does that get folded into the FTC or whatever agency takes over? Do you have a position on CPNI?

MS. POLK: Well, of course, the FCC reinstated the reclassification of broadband providers as information service providers, not telecommunications providers. So that affects the applicability of Section 222. We'd argue that Section 222 was written in a telephone-centric context and the legislative history, the statute itself, all of the rules under it relate to traditional telephone service. And so we've argued that it's not a basis for regulating in the privacy area.

So I don't know if Lynn wants to elaborate on this.

MS. FOLLANSBEE: Yes, I think that's exactly it. The CPNI rules were written a long time ago with respect to telephone service. And where we are now, with Internet service and broadband service, is so much larger than what's encapsulated in the CPNI rules. Obviously, when the FCC attempted to take jurisdiction, back when the net

neutrality rules were that broadband was under Title II, we definitely fought that and said, "Absolutely not, we think it's information service." And so, fortunately, right now, currently, the FTC has the authority and we think that really is the best place.

The reality is, even when the FCC had Title II authority over our companies in this, we argued that the FCC really did not have the kind of expertise that the FTC has, as we've talked about up here. The FTC has a long history with their FIPPs, and they have just been doing this a long time. They've spent a lot of time in this space and we think it's really the appropriate place.

MR. COOPER: Kelly, let me follow up and ask you about that. The FCC had, for a very limited time, asserted its jurisdiction in the privacy sphere in a much bigger way, Congress later repealed its regulation. Is that something that you're having to push back against at this point in terms of the Internet privacy issue today? Are all sides pretty much willing to say that we can keep that separate, we can keep the net neutrality stuff out of this? Is that a debate that's still happening?

MS. COLE: Not so much in the privacy space. I

mean, yes, occasionally, you hear the argument about the privacy CRA, from a political perspective, not necessarily from a policy perspective. I'm hopeful at least they're separated enough that we can truly have a privacy debate and focus on the FTC.

And I would just echo everything that Lynn and Loretta just said. From CTIA's perspective, we don't think the sectoral laws, as they relate to CPNI, make sense anymore. We've moved beyond that. And we don't want dual regulation. If we're going to do this, let's do this right and let's house that jurisdiction at the FTC, where frankly it makes the most sense.

MR. COOPER: Michelle, there was a 2017 survey by NTIA. And it said that Americans' number one fear in going online was identity theft or identity fraud. And that's kind of a different set of harms than we've mostly been talking about here. We've mostly been talking about commercial uses and collection of data and sharing it and selling it. But there's a little bit more of a bad actor element here involved, of course, with that. It's sort of equally data security as well as data privacy.

Do you support federal legislation that would

deal with data security in particular and those kinds of ID fraud issues? Or perhaps data breach notification, those kinds of issues? Should that be part of this? Or is that a separate thing? I would be interested in your whole take.

MS. RICHARDSON: Yes, we have a model bill on CDT's website. And we did include data security. We think it's time to level up and have a federal standard that everyone must take reasonable efforts to protect data. Understanding that "reasonable" is very different, depending on the type of data you have, how you use it, the size of your operation. These are the rules that the FTC has actually had out for years. This is consistent with international standards and where the states are going already.

We think they should be not controversial. And there's a lot more agreement around data security than there is around privacy. So I think we were a little disheartened to hear that there are rumors that the first draft of the Senate bill may not have data security in it. And so if there are any decisionmakers listening, we would strongly urge them to include data security. This all

needs to happen at one time.

But breach notification, let it go. The moment passed. I don't know how many ways to say it. It was 15 years, never happened. And there's now data breach in all 50 states. Just let it go. It's a very different issue from the substantive data security. So it can be severed. And, frankly, it's not as important as actually saying, "Take reasonable efforts to secure data." That could lead to systemic change and better practices.

I think people are disappointed with how data breach has turned out. We thought it was going to cause reputational harm to companies that would allow consumers to vote with their feet. And it would change behavior. And it hasn't.

So focus on the data security, actual standards. Let the breach notification go. The moment has passed. And we're happy to support people as they try to draft the data security section.

MR. COOPER: Yes, Loretta.

MS. POLK: I was just going to add that we think that it's important to codify the FTC's reasonable data security measures work in any statute that comes out.

MR. COOPER: Okay, Lynn, we'll stick with the FTC for a minute. In a typical FTC enforcement process, it's a complaint served by the FTC. It goes before even the Commission. And if the result is unfavorable to the party that's the defendant, they could appeal to a court of appeals.

That kind of process, will that work? Is that kind of scalable if it takes on something as big as Internet privacy? Is that where the rulemaking comes in and that alters things? Do you have a view about that?

That's probably more of an insider FTC question, institutionally.

MS. FOLLANSBEE: For the FTC, if they have some limited rulemaking authority, it would probably enable easier enforcement. If there's a complaint to the FTC and they have rulemaking authority and there are some clear rules, then it's much easier to bring an enforcement case. So we would support that.

MR. COOPER: Okay, looming in the background, Kelly, you had mentioned the California privacy law. Do you have a view or a critique of that law? If that were the national standard, would that be okay? Is the problem

that it's coming from the state level?

MS. COLE: Yes, we have some real concerns with the California privacy law. And this was a law that was literally pulled together in days. It's taken months, literally, for the gang of six just to work through the issues that they have been working through in the Senate. So to think that you could throw something together like that in literally hours is just completely unrealistic.

So they have their definitional problems in that law that, frankly, we're working very hard to see if we can get fixed. And there's an effort by industry across the board to see what we can do to make improvements to that. But I would certainly not recommend that Congress start with that as its base.

MR. COOPER: Lynn, did you have a view on the California law?

MS. FOLLANSBEE: No, I would agree absolutely with Loretta.

MR. COOPER: Maine has one as well, recently. Okay.

Well, we're getting near the end of all of my questions and all of our time. We've got two minutes. So

I am interested in seeing if anyone from the audience is interested in offering a question. And I see someone in the back there.

QUESTION: Hello. Richard Morris with the Competitive Enterprise Institute.

I wonder, just for any of the panelists, if we do see a big, comprehensive privacy bill come out of Congress like we're imagining, that polices the digital privacy policies of for-profit companies, should a bill like that also include aspects that police the digital privacy of government employees and government agencies as well? Should they be subject to the same standard, I guess?

MS. RICHARDSON: I would argue no, and I say this actually as someone who spent a lot of time on law enforcement and intelligence issues. It's just such different equities. And the consumer issues are so hard to sort out. If you add on employee, law enforcement use, and other things, it will fall under its own weight.

MR. COOPER: Okay, looks like we have one other question, right over here. The microphone is coming.

Please identify yourself when you ask the question.

QUESTION: Hi, my name is Will Rau (phonetic). I am an intern at Comcast.

So it seems like all the panelists agree that it would be somewhat harmful if states were passing their own privacy legislation because they could contradict one another or confuse consumers. But in terms of national legislation, it seems like there is a lot of gridlock right now. So do you think that states have an obligation to pass their own data privacy laws simply to protect people while they're waiting for a more national one to pass? Or should states simply just wait?

MS. RICHARDSON: I will point out that most of the state legislatures are winding down, and no other state was able to pass a comprehensive law this year. So the patchwork is still a year or two away, maybe.

I think what you'll see in the meantime are maybe biometrics laws. Those are still hot right now for states that aren't ready for the big picture, or Maine with the ISPs. And you're going to continue to see people dabble, regardless, whether they should or not.

Hopefully, that will inspire Congress to move faster. There's nothing you can do to stop them in the

meantime. And as a privacy advocate, we're really torn.

What if this takes five years? We can't wait five years for privacy protections. We're going to be in a different Internet in five years.

MR. COOPER: All right. That will conclude the questions today. I would like to thank all of the panelists. And please give a round of applause.

(Applause.)