This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

RPTR KEAN

EDTR ZAMORA

PROTECTING CUSTOMER NETWORK PROPRIETARY INFORMATION IN THE INTERNET AGE

WEDNESDAY, JULY 11, 2018

House of Representatives,

Subcommittee on Communications

and Technology,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to notice, at 10:13 a.m., in Room 2322, Rayburn House Office Building, Hon. Marsha Blackburn [chairman of the subcommittee] presiding.

Present: Representatives Blackburn, Lance, Shimkus, Latta, Guthrie, Olson, Johnson, Long, Flores, Brooks, Collins, Walters, Costello, Doyle, Welch, Clarke, Ruiz, Dingell, Eshoo, Engel, Butterfield, Matsui, McNerney, and Pallone (ex officio).

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Staff Present: Jon Adame, Policy Coordinator, Communications and Technology; Kristine Fargotstein, Detailee, Communications and Technology; Sean Farrell, Professional Staff Member, Communications and Technology; Adam Fromm; Director of Outreach and Coalitions; Elena Hernandez, Press Secretary; Tim Kurth, Deputy Chief Counsel, Communications and Technology; Lauren McCarty, Counsel, Communications and Technology; Drew McDowell, Executive Assistant; Evan Viau, Legislative Clerk, Communications and Technology; Jeff Carroll, Minority Staff Director; Jennifer Epperson, Minority FCC Detailee; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Alex Hoehn-Saric, Minority Chief Counsel, Communications and Technology; Jerry Leverich, Minority Counsel; Dan Miller, Minority Policy Analyst; and C.J. Young, Minority Press Secretary.

Mrs. Blackburn. The Subcommittee on Comms and Tech will now come to order. And the chair now recognizes herself for 5 minutes for an opening statement.

Good morning to everyone. And welcome to today's hearing on protecting consumer privacy. And if you have not done so, I would encourage you to get your acronym app out as you try to follow along with what we have before us today.

This is a topic that has attracted attention in a variety of contexts, and one that I am so pleased that we are discussing today. And I want to say thank you to our witnesses who are sharing their expertise with us as we strive to protect customer privacy when communicating in the internet age.

Over 20 years ago, Congress realized the importance of protecting the confidentiality of Customer Proprietary Network Information, CPNI, when consumers use their primary method for instantaneous communication, which at that point was telephone calls.

The rules that the FCC initially adopted to implement the statutory CPNI requirements only covered information from traditional call records. But over time, these protections have evolved to cover new forms of communication like interconnected Voice over IP, or VoIP, calls, and even information collected by telecommunications carriers on mobile devices.

By enacting section 222, Congress established a specific statutory structure that acknowledged that consumers share sensitive data when they communicate over the phone. This was based on the assumption that only the telecommunications carrier had access to that data. In the internet age, telecommunications laws have been disrupted

just like everything else. In some cases, app developers operating systems and Edge providers have access to the same exact CPNI that telecom carriers are required to protect in various ways.

Consumers now use these different forms of communication interchangeably to serve the same purpose. For example, if a consumer uses his or her mobile phone to call someone using the standard telephone function on their cell phone, that call is traveling over the public switch telecom network and would be protected by the current CPNI rules and enforced by the FCC. If that same consumer uses the exact same cell phone to call the exact same person but uses a voice-based app to place a call, the communication would not be going over the PSTN and not be protected by the CPNI rules.

As I said, you need your acronym app for this one.

Both calls are conveying the same information, but the consumer's information in the second scenario is not protected in the same manner as the first scenario. This leads to a problem where consumers do not have the same privacy protections when using the same device for essentially the same purpose.

This is when the FCC's 2016 Privacy Order was a consumer protection vehicle that drove at the wrong target. The Commission's inability to locate all the other traffic out there is precisely when wheels came off.

As I have suggested before, the solution to this problem is broad privacy legislation, which is why I introduced legislation on the subject almost a year ago that steers us in the right direction. The BROWSER Act is comprehensive bipartisan privacy legislation that will give Americans seamless protection across all of their electronic

communications.

As we discuss these important issues today, we need to consider innovation and consumer privacy needs across the entire internet ecosystem so we can arrive at a solution that works for everyone.

At this time, I yield the remainder of my time to Mr. Lance for his opening.

[The prepared statement of Mrs. Blackburn follows:]

******** COMMITTEE INSERT ********

Mr. Lance. Thank you, Chairman Blackburn. And welcome to our distinguished panel.

Section 222 of the Communications Act was enacted during the Act's last major update in 1996. The section mandates the telecommunication entities protect consumer privacy information, as the chairman has said, CPNI.

Since 1996, the internet has revolutionized communications in so many ways. However, as breaches of consumer data repeatedly confront us, we must ensure the rules and regulations protecting consumer information are up to date and applied equally across the internet ecosystem.

The FCC has tried to keep up with the technological innovations over the past 20 years, but an outdated statute limits its efforts. It is crucial we protect consumers' sensitive information, no matter the means of communication, and without hampering innovation.

I look forward to discussing how we can update the law to conform to the challenges and opportunities of the digital age. And I yield back.

[The prepared statement of Mr. Lance follows:]

******** COMMITTEE INSERT ********

Mrs. Blackburn. This gentleman yields back.

Mr. Doyle, you are recognized for 5 minutes.

Mr. Doyle. Thank you, Madam Chair, for holding this hearing, and thank you to the witnesses for appearing before us today.

Digital privacy in our modern era has never been more important. And as our society becomes increasingly connected, it will become even more important. I believe that we can and must do more to protect American's privacy and sensitive information.

This committee's hearing with Facebook's CEO Mark Zuckerberg showed how concerned our members are with the practices of one of the world's largest tech companies. And what that hearing made clear was that the FTC does not have the manpower or authority to adequately enforce its own consent decree against Facebook, let alone proactively police this fast-evolving space.

To solve this problem and to give the American people the protections they are demanding, we are going to need a comprehensive solution that includes more resources, more manpower, and more authority to go after bad actors, and the ability to set rules of the road for the digital economy.

Facebook demonstrated all too well that after-the-fact-enforcement authority can't help us when the damage has already been done.

Europe's implementation of its GDPR rules, as well as California's recently and quite quickly passed privacy law, are clear indications that people at home and abroad recognize the need for strong privacy protections. We in Congress and on this committee need to take that to heart as we are addressing this pressing issue.

Now, with regards to today's hearing and the topic before us, CPNI, or Customer Network Proprietary Information, the FCC enforces the CPNI rules under section 222 of the Communications Act. This section restricts how telecommunication carriers can use and share customer data related to their service. This section and the authority it grants the Commission are some of the strongest privacy laws we have in this country and are intended to give consumers a modicum of protection.

These rules were expanded in 2016 to include broadband services as well. Those rules too were simple but effective.

The three components were, first, if your broadband provider wanted to use your data, it had to ask your permission. Secondly, it had to take reasonable steps to protect that data. And third, it needed to notify you if your data was breached.

These rules were an expansion of the FCC's existing CPNI rules and would have meaningfully enhanced our Nation's privacy laws. However, Chairman Blackburn cosponsored and successfully led an effort to repeal these simple, sensible rules. As of yet, there has been no replacement.

The majority cannot claim that it values privacy when one of its signature achievements this Congress is the repeal of these meaningful rules.

Americans around the country are shouting for more, not less, privacy protections. Whether it is through ballot initiatives, billboards, people want more control over their digital lives. This is why it is so concerning that the FCC is doing so little to enforce its existing protections under section 222.

Thanks to the work by Senator Wyden and his staff, we recently discovered that

real-time location of hundreds of millions of cell phones were being made available by our Nation's wireless carriers without consumers' consent.

At least one company, Securus, used their access to this data to create a service for tracking and locating nearly every cell phone in real time. On top of that, Securus forced families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family members. This seems like no choice at all.

LocationSmart, the data aggregator that made this data available, had such poor security on their website that according to a researcher at Carnegie Mellon University, individuals could look up real-time location data with little effort.

These carriers it seems trusted but did not verify that consumers were giving consent to be tracked, and that gross negligence on their part exposed supposedly protected sensitive data to hundreds of millions of people.

These revelations are deeply troubling, but what is more troubling is the lack of knowledge by the FCC of what appears to be a pervasive practice in the wireless industry.

Similar to the Facebook incident, we still don't even know the extent of this breach and who may have had access to this data.

Madam Chairman, I would respectfully request that this committee hold a hearing on this incident to understand how it happened and to hold the responsible parties accountable.

With that, I will yield back the remainder of my time, and I look forward to the testimony of our witnesses.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

[The prepared statement of Mr. Doyle follows:]

******** COMMITTEE INSERT ********

Mrs. Blackburn. The gentleman yields back.

Mr. Walden has not arrived. Does any member on the Republican side seek to claim his time?

Seeing no one, I will go to -- Mr. Pallone is not here.

Does anyone on the Democrat side seek to claim his time?

Ms. Eshoo, you are recognized.

Ms. Eshoo. Thank you, Madam Chairwoman. And thank you to the witnesses. It is good to see each one of you.

I was surprised when the majority actually called this hearing. I think that there is an urgent need to examine privacy and data protections across the internet ecosystem, but I think this hearing, most frankly, is being held under disingenuous pretenses, and that the majority is inaccurately portraying itself as champions of consumer privacy reform when the record shows otherwise. Mr. Doyle raised this in his opening statement.

In fact, the only action the majority has taken on privacy to date has been to actively roll back existing privacy protections and expose consumers to increased harm. Consumers legitimately feel that they have completely lost control of their personal information. There is not a single one-size-fits-all solution to this, but in 2016, I think we were making progress. That is when the FCC extended CPNI protections to apply to broadband access services. That was a step forward for consumers. It should have been the first step toward protecting privacy at other points in the digital economy, including at the Edge.

But instead, the majority pushed through a partisan repeal of the rules before the ink was even dry on a razor-thin vote of 215 to 205 with 15 Republicans opposed. Everyone on this committee remembers what a bitter fight that was. But in the end, there were pressures that beat out consumer protection. So now as a result, there are currently no strong privacy rules anywhere in the digital ecosystem.

Americans have spent the last 17 months completely vulnerable to privacy exploitation and data breaches without recourse. Our most sensitive information, location data, medical history, Social Security numbers and mothers' maiden names are daily transmitted through networks of companies who no longer have any meaningful obligation to protect it. And I think that the American people are legitimately outraged by this.

So, Madam Chairwoman, I fully support real attempts. And I underscore that word, "real attempts" to seek meaningful solutions for privacy protection across the diverse internet economy. And I think our witnesses here today are going to help to inform our thinking.

So with that, I yield back the balance of my time, and I want -- yes. Oh, Jerry. I will be happy to yield to my colleague from California, Mr. McNerney.

Mr. McNerney. Well, I thank my colleague for yielding.

Despite demands from Americans for more control over the information they share online, last year, Republicans in Congress voted to strip consumers of the power to choose how ISPs use and share their information. Republicans also voted to eliminate important data security protection for consumers.

Now, ISPs are no longer required to take even reasonable steps to secure consumers' personal information. Given the growing cyber threats that our Nation faces, it is critical that we do more and not less to secure consumers' data. That is why I introduced the MY DATA Act, which would give the Federal Trade Commission important tools to protect consumers' privacy and security online. I hope that we can work together to move the MY DATA Act forward.

And does the ranking member wish some time?

Mr. Pallone. Well, let me just say, if I could. Madam Chair, if I could ask unanimous consent to include my statement in the record.

Mrs. Blackburn. Without objection.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

Mr. Pallone. Thank you.

Mr. McNerney. I yield back.

Mrs. Blackburn. The gentleman yields back. The gentlelady yields back. And that concludes member opening statements.

And I would like to remind all members that pursuant to the committee rules, all members' opening statements will be made a part of the record.

We want to thank our witnesses for being here today and taking time to be before the subcommittee. Today's witnesses will have the opportunity to give their opening statements, followed by a round of questions from members.

On our panel today we have Mr. Hance Haney, director and senior fellow at the Technology and Democracy Project at the Discovery Institute. Mr. Rob McDowell, senior fellow at the Hudson Institute, and a former FCC commissioner. And I think she may get the prize for most appearances this year; Ms. Laura Moy, deputy director of the Georgetown Law Center on Privacy and Technology.

We appreciate each of you being here, making your testimony available to us.

We will begin today with you, Mr. Haney. You are now recognized for 5 minutes for an opening statement.

STATEMENT OF HANCE HANEY, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND DEMOCRACY PROJECT, DISCOVERY INSTITUTE; ROBERT MCDOWELL, SENIOR FELLOW, HUDSON INSTITUTE, FORMER COMMISSIONER, FEDERAL COMMUNICATIONS

COMMISSION; AND LAURA MOY, DEPUTY DIRECTOR, GEORGETOWN LAW CENTER ON PRIVACY AND TECHNOLOGY

STATEMENT OF HANCE HANEY

Mr. Haney. Thank you very much, Chairman Blackburn, Ranking Member Doyle, and Ranking Member Pallone.

Section 222 of the Communications Act requires telecommunications common carriers to obtain customer approval in order to use, disclose, or permit access to Customer Proprietary Network Information.

CPNI consists of call detail information, including the time, location, duration of telephone calls, as well as the telephone numbers from which calls originate and terminate. It also includes billing and other information.

Section 222 does not apply to broadband services, which are classified as an information service. Even though broadband services could be thought of as being provided by telecommunications carriers, the statute and the regulations look to the service provided, not to the provider of the service.

Instead, broadband is subject to the unfair and deceptive acts and practices authority of the Federal Trade Commission. This is the same authority that governs video streaming services, search engines, social networking sites, e-commerce sites, and user-generated media sites.

The FTC privacy framework is technology neutral and it identifies categories of

sensitive information that may give rise to an obligation by companies to obtain affirmative, express customer consent, otherwise referred to as opt-in approval.

Sensitive information includes information about children, financial and health information, Social Security numbers, and precise geolocation data, according to the FTC.

Technology neutrality is appropriate because, as the FTC has observed, broadband providers are no different than other participants in the internet ecosystem in terms of their ability to collect and utilize information about consumers.

The FTC's recognition that the requirement to use opt-in should be limited is also appropriate. Due to consumer inertia, most consumers typically don't take action in this type of situation. The requirement to obtain opt-in approval can be costly and inefficient, even a barrier to innovation.

Consumers benefit from the use of information that companies see and collect in the course of serving their customers, as companies like Google have demonstrated. Advertising underwrites the cost of services that Google offers for free to the public, and there is no reason that advertising couldn't also help offset the cost that broadband providers incur in offering broadband service.

Privacy regulation involves transaction costs and may have anti-competitive consequences if it is applied unevenly. Ideally, all market participants should be subject to a uniform privacy framework administered by a single agency for the sake of consistency.

The FTC's current privacy enforcement practice satisfies these criteria. Admittedly, making the internet more secure will likely always be a work in progress, and

there is a role for both market solutions as well as regulation.

Legislation to enhance consumer privacy protection, if any, should strive for technological and competitive neutrality. In particular, it isn't rational to subject some market participants to heightened privacy regulation just because they were subject to economic regulations in the past.

We live in an era of rapid technological convergence in which is it wise to consider that every participant in the internet ecosystem is a potential competitor at least to some extent. Moreover, privacy protection should be calibrated according to the sensitivity of the information at issue in recognition of the fact that there are transaction costs associated with consumer consent systems.

Opt-in systems are particularly burdensome and should be reserved for only the most sensitive personal information. Where customer information is less sensitive, consumers' privacy expectations should be balanced with the benefits consumers are likely to derive from a dynamic, competitive market, including greater abundance of choices and lower prices. Such a market is one where all providers have similar opportunities to innovate and earn a fair return on investment.

Finally, to the extent possible, regulation should reflect the practical reality that it is difficult to make predictions about how the market will evolve and at what pace, and that the process of calibrating regulation on an ongoing basis as necessary to reflect changes in the market can be slow.

Thank you.

[The prepared statement of Mr. Haney follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

******** INSERT 1-1 ********

Mrs. Blackburn. The gentleman yields back.

Mr. McDowell, you are recognized.

STATEMENT OF ROBERT MCDOWELL

Mr. McDowell. Thank you, Chairman Blackburn, Ranking Member Doyle, and Ranking Member Pallone as well, and distinguished members of the committee. It is an honor to be back before you here today.

I did serve as a commissioner of the FCC from 2006 to 2013. Today, I am a partner at Cooley LLP, as well as co-leader of its communications practice, which is global. I am also a senior fellow at the Hudson Institute, as the chairman pointed out, and I testify today in my own capacity, and the views I express today are purely my own.

Sitting behind me is a remarkable young woman, as my aide-de-camp for the day. She is my daughter Mary-Shea Virginia McDowell. It is always good to have someone watching your back when you are in Washington, so --

Safeguarding sensitive or private information is a concept as old as human beings. The English term "eavesdropping" was created centuries ago when the ancestors of today's data thieves literally lingered under the eaves of roofs to listen to the private conversations of others.

Fast forward to 1980 when the FCC extended itself into the privacy arena in a narrow way as part of its computer inquiry proceedings. It issued rules governing what is now dubbed Customer Proprietary Network Information, or CPNI -- could use some

branding work on that name, I think -- mainly as a safeguard against regulated monopoly local phone companies from using sensitive customer data to help their unregulated affiliates compete against new entrants at the time.

Then Congress codified section 222 in 1996, mandating the Commission to adopt more specific CPNI protection rules applicable only to common carriers. Since then, dramatic changes have occurred in the telecommunications, media, and technology, or TMT marketplace.

The maturation of the internet ecosphere, especially the mobile internet, has produced consumer benefits that were unimaginable 22 years ago when section 222 was codified. And America has led the way in these innovations.

Furthermore, the mobile net has also helped spark trillions of dollars in American economic growth. Brilliant engineers and intrepid entrepreneurs have invented new tools that have dramatically altered and improved our daily lives, forcing business models to experiment and converge.

Section 222, however, has remained the same despite these new market realities. Only telecommunications carriers must live under this law governed by the FCC, while the rest of the players in the dynamic internet ecosphere operate under privacy standards administered by the Federal Trade Commission.

This duality has created a legal and regulatory asymmetry in the diverse internet market. Additionally, America's public policy has evolved to create a regulatory regime that sometimes does not focus as much on the sensitivity of the data that is collected, but rather, it focuses on what kind of market player collects the data. This approach could

be more confusing for consumers, including myself, and companies alike, than would having one set of technology neutral rules that apply consistently across all platforms, including those we can't even imagine today.

Only Congress has the authority to modernize privacy and consumer protection laws to reflect the realities of the 21st century internet marketplace. I respectfully suggest that Congress examine a modernized and harmonized privacy framework that is technology neutral and which focuses on the sensitivity of the data that is collected, rather than the type of entity that collects the data.

That said, any uniform standard should guard against imposing overreaching or unnecessary regulations to help maintain America's leadership in the global TMT economy.

Thank you again for inviting me to appear before you today, and I look forward to your questions.

[The prepared statement of Mr. McDowell follows:]

******** INSERT 1-2 ********

Mrs. Blackburn. The gentleman yields back.

Ms. Moy, you are recognized.

STATEMENT OF LAURA MOY

Ms. Moy. Thank you very much.

Good morning, Chairman Blackburn, Ranking Member Doyle, Ranking Member Pallone, and distinguished members of the committee.

So the subject of today's hearing is Customer Proprietary Network Information, sometimes referred to as CPNI, which I agree with Mr. McDowell that that may need some branding work. That is the information collected by telecommunications providers -- and right now, that means just phone providers -- about subscribers' use of the information. So important information about our communications, like who we call and who calls us, how often we call them, how long we talk to them, and where we are calling from.

And I am really glad we are having a hearing on CPNI because the law that protects CPNI is one of the strongest Federal consumer privacy laws we have. It requires phone carriers to get their customers' permission before using CPNI for purposes other than to provide the phone service. In other words, you are paying for your phone service, and your carrier simply delivers the service without always trying to make an extra buck off your private life.

So your phone carrier can't use the fact that you have been calling banks and

credit card companies to market you payday loans, or the fact that you have been calling an elderly relative and healthcare providers more frequently to market you home health services, nor can it sell that information to outsiders without getting your permission first.

The CPNI privacy law also enables an expert agency to issue regulations that can be modified and updated in accordance with changing technology and business practices. And this is really important.

The CPNI privacy law also gives the FCC robust enforcement authority in the form of fines. And using this authority just in the last few years, the FCC has fined four different carriers for violations of CPNI privacy protections.

The CPNI privacy law should serve as a model for future privacy laws this Congress may consider because of its substantive strength, the regulatory flexibility it offers through rulemaking, and its enforcement strength.

But instead, however, the benefits to consumer privacy presented by the CPNI privacy law has faced some major setbacks. As multiple people in this room have mentioned, last year, Congress, including a number of members of this subcommittee, voted against the application of these strong privacy rules to broadband providers, even though, like the phone, broadband is now an essential service, and like phone carriers, broadband providers enjoy privileged insight into their subscribers' private communication.

And this year, as the FCC eliminated net neutrality rules, it removed broadband providers altogether from the reach of the CPNI privacy law, which, as I said, is one of the

strongest consumer privacy laws we have on the books.

So that brings us to today, and here, as we consider what our path forward should be. It is clear that we must do something. Ninety-one percent of adults in America feel that consumers have lost control of their personal information. And nearly 70 percent thinks the law should do a better job of protecting their information.

Consumers want more privacy protection, not less. This is why the recent elimination of existing privacy protections was so unpopular among the American public.

As Congress considers how to give Americans the privacy protections they deserve, it should keep a few things in mind:

First, prospective rulemaking authority is an incredibly important consumer protection tool. After-the-fact enforcement can be helpful, but an enforcement-only regime does not always create clarity, and because it comes only after a problem has occurred, it does not necessarily protect consumers from the problem in the first place.

Granting rulemaking authority to an expert agency also fosters much needed regulatory flexibility. We don't always know what the next privacy or data security threat will be, but unfortunately, we all know that there will be one. An agency with rulemaking authority can respond to shifting threats more quickly than Congress can.

Second, consumer protections are only as good as their enforcement, so any new protections Congress creates on privacy or data security must be accompanied by strong enforcement authority.

Right now, the FTC does use substantial work on privacy and data security. But with few exceptions, it does not have the ability to seek civil penalties for privacy and

data security violations. In fact, FTC staff and commissioners have appeared before Congress requesting civil penalty authority to buttress their authority. Agencies that are tasked with protecting consumers' private information cannot do it without the proper tools. Civil penalty authority is needed.

Third, Congress should avoid the temptation to address complex challenges with the one-size-fits-all approach. There are different types of actors on the internet with different roles to play, different relationships with and commitments to consumers, different competition environments and different abilities to solve problems. If we adopt a uniform regulatory approach to the entire internet, we are going to be left with the lowest common denominator, something like transparency with enforcement that just prohibits deceptive practices. And that is not good enough. Consumers are asking for more.

I appreciate your commitment to this issue. Thanks for having me. I look forward to answering your questions.

[The prepared statement of Ms. Moy follows:]

******** INSERT 1-3 ********

Mrs. Blackburn. The gentlelady yields back.

And we thank all of you for your testimony. And we will begin our questions and answers. I will begin by recognizing myself for 5 minutes.

Mr. Haney, I would like to start with you. Devices often have much more detail location information than what carrier location provides. For example, later iPhone models integrated location information from various sensors, WiFi, Bluetooth, GPS, cell towers, et cetera, and create a more precise location. Apple calls this data Hybridized Emergency Location, or HELO. Is this feature integrated into the operating system?

Mr. Haney. Yes, I believe it is.

Mrs. Blackburn. And would you classify HELO data as CPNI?

Mr. Haney. No.

Mrs. Blackburn. If you applied current CPNI rules to HELO data, would Apple be permitted to transfer this data to a service like RapidSOS?

Mr. Haney. No, not without subsequent permissions.

Mrs. Blackburn. Okay. Would Uber, which relies on HELO data, be able to function if HELO data was subject to CPNI rules, or would the app become unusable due to individual opt-in consent mechanisms every single time a user opens the app?

Mr. Haney. In terms of ability to function, no, probably not. In terms of the consumers, they probably suffer from opt-in fatigue.

Mrs. Blackburn. Okay. Thank you.

Mr. McDowell, how is the data that is collected by mobile apps different from the data collected by a telecom provider? Because it does not sound that different to me.

Mobile apps are collecting the time an app is used, the duration, and the location of where the user is when they are using the app. And we heard through our algorithms hearing that we recently did how all this collection goes even a step further and anticipates my future choices, plans, and decisions.

So aren't these the same details a telecom provider collects and are protected under the CPNI rules? And what are the rules protecting this information from a mobile app, and what level of opt-in has the consumer performed?

Mr. McDowell. A lot of questions there, Madam Chair.

Mrs. Blackburn. Yes.

Mr. McDowell. All excellent ones. So, first of all, an app can actually collect more data than a carrier would have access to. For instance, if you scan a UPC code, the price of something in a supermarket, there is an app that can tell you if there is a better deal nearby. So it knows where you are, it knows what you are buying, it knows your price points. It knows a lot about you all of a sudden, the demographics, based on that thing that you are buying. That is just one of many examples.

You know, it is the 10th anniversary this week of the Apple App Store. So happy birthday to the App Store. I think it is a wonderful thing. And there are, I think, 1.5 million apps in that app store. And certainly, Apple has some terrific standards that it tries to live by there. But those apps, you know, with 1.5 million, or whatever the actual number is, there are just as many ways of gleaning information about consumers, where they are, what they are buying, what they want, what they are saying, how they look. There is a lot of aspects there that carriers don't necessarily have access to.

So the CPNI rules would be sort of a -- or the data that CPNI governs would be sort of a subset of what all the other information that apps collect.

Mrs. Blackburn. You mentioned we need to modernize and harmonize the protection rules. So I want you to elaborate just a touch on that point.

Mr. McDowell. Absolutely. So from a consumer's perspective, there is certain information that we find sensitive. And this can vary from consumer to consumer, of course, but -- and other information not. So if you think of your information regarding your health or your financial information, things like that, those are easy examples of what we consider to be sensitive, and you don't necessarily want the whole world, or very few people, having access to that, versus you are conducting a search to buy a new car. Maybe you want to have the greater world know that you are looking for this kind of car at this type of price point. So that is less sensitive information.

So that is what I was trying to illustrate too, is as consumers, we care about the type of information. It doesn't matter who has that information. There aren't politically favored or politically disfavored entities out there. We are concerned about anyone breaching that or disclosing that information in a way that we don't agree with or the way that we don't command.

Mrs. Blackburn. Okay. I appreciate that.

Ms. Moy, I have a question for you. In the interest of time, I will submit that.

I yield back my time and recognize Mr. Doyle.

Mr. Doyle. Thank you, Madam Chair.

Ms. Moy, it was recently revealed that our Nation's top wireless carrier shared

real-time location data of hundreds of millions of Americans with third parties without consumers' consent. This access was used by at least one entity, Securus, as part of a service to enable their customers to determine the exact location of hundreds of millions of cell phones in real time without user consent.

How is it possible that such a massive data breach of such sensitive data could occur, and why do you think the FCC was in the dark on such a widespread practice?

Ms. Moy. Those are really good questions, and questions that the agency itself should be asking. So in this instance, Securus was getting information through these data brokers, location aggregators, that were sourcing it directly from the wireless carriers who were giving these data brokers direct access into their location information.

We know about the Securus case, but about a month ago, Verizon told journalist Frank Bajak of the Associated Press, that about 75 companies have been obtaining its customer data from LocationSmart, and another broker called Zumigo, I think. And I want to emphasize that this is really private information. Location can tell someone about where you work, where you live, where your kids go to school. In a recent Supreme Court decision, the Court likened location data maintained by phone carriers to electronic ankle bracelets.

With respect to what -- how this could have happened, I mean, clearly, the carriers have not been taking location privacy seriously enough, if they were enabling data brokers to take over the customer consent process and then not properly policing it. But ultimately, the responsibility falls with the FCC to ensure that carriers are actually meeting their statutory obligation to protect that information.

Mr. Doyle. So tell me, if a Federal regulator is captured by industry and declines to assert their own authority, what role does the private right of action or enforcement authority by State attorney generals play, and how can that maybe be a check on a reluctant agency?

Ms. Moy. That is a great question, because we have something sort of like that under the -- well, we do have that under the Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act, which is a 1998 privacy law that specifically involves the information that children share with a provider of an online site or service, grants State attorneys general the authority to bring civil actions against companies that they believe have violated the Act -- or have violated, actually, the regulations passed by the FTC under that act on behalf of citizens of the State in the event that the agency itself, the Federal agency, doesn't do that.

I think that is a really important and strong privacy enforcement tool. It has been used by multiple State attorneys general, and it would be great to see something like that in additional privacy laws moving forward.

Mr. Doyle. Tell me, do you think Chairman Pai's past work for Securus is reason for him to recuse himself from any investigation or enforcement action?

Ms. Moy. I don't know that I can answer that directly, except to say that I do; it does raise some red flags that he does have a past working for a company that is accused of wrongdoing in this particular instance.

Mr. Doyle. Let me ask you, do you think Americans have fewer privacy protections as a result of the broadband privacy CRA?

Ms. Moy. As a person who advocated strongly for those broadband privacy rules and thinks that they are really important, yes, I do. I think that privacy is in a worst place, especially when you think about your home internet connection. An internet provider can see not only information about all of the websites that you visit, including those that pertain to your health information, your political viewpoints and so on, but can also see information about Internet-of-Things connected devices. So perhaps information about when you are opening your garage door, when you are using your baby monitor, maybe even when you are using your connected toothbrush or connected mattress. There is just -- they can see maybe when there are guests in your home and additional devices. There is just a lot of really sensitive information that a network provider has access to, and consumers, unfortunately, have no choice but to share that information with those providers.

Mr. Doyle. Do you think Americans are better off with the FTC enforcing privacy protections on broadband providers as some in the majority have alleged?

Ms. Moy. Frankly, no. And the reason is -- well, there are multiple reasons, but part of it is that the FTC doesn't have rulemaking authority, so it can't create perspective rules-of-the-road on this issue. And its enforcement tools are really limited. It doesn't have the same kind of bite to its enforcement that the FCC does.

You know, as I said, the FCC has brought multiple actions against carriers in the past few years for CPNI violations with fines attached. The FTC doesn't have that type of authority.

Mr. Doyle. Thank you, Madam Chair. I yield back.

Mrs. Blackburn. The gentleman yields back.

Mr. Olson, you are recognized for 5 minutes.

Mr. Olson. I thank the chair. And welcome, Mr. Haney, Ms. Moy. And a special welcome to the McDowell family, our commissioner, and his daughter Mary-Shea is right behind his left shoulder.

We talked before the hearing. She is a junior in high school, about to go off to college, and I take great pride, as your father does as well having -- my wife went to Duke University like your father. You won't become a North Carolina Tar Heel. Never, ever. So thank you for that.

But to the business ahead, Commissioner McDowell, we have all become familiar with the idea of targeted advertising. As you know, companies grab our data and, you know, when we buy something -- like, for example, I bought a lot of Houston Astros World Series hats, Jose Altuve jerseys, George Springer bobblehead. All of a sudden, ads popped up, when I got on the internet, with the Astros, the Rockets, the Oilers, pro-baseball. Obviously, they are targeting me with direct ads because of my behavior on the internet.

Google and Facebook as well do this automatically. Users like myself have to opt out most times, because I don't want those targeted ads. Most people don't want those ads. But if a telecommunications provider does this automatically, the exact same behavior that Googles and Facebooks do, that is illegal.

Can you explain that? Doesn't that sound anticompetitive?

Mr. McDowell. Well, it does create that asymmetry that I was talking about in

my opening remarks. So that is because of section 222 and the FCC's enforcement of that. So it creates -- you know, we have a diverse internet ecosphere. There are business models that have come forth in the past decade, even the past year or two, that we couldn't even imagine a year or two ago, right. So we don't know what is coming up next, what brilliant entrepreneurs are going to think of.

So we don't know how -- ways they might be using our data. But you do have 222, section 222, offering one standard and FTC sometimes administering a different standard.

Mr. Olson. Mr. Haney, in your opening statement, you state that, this is a quote, "privacy protection encourages broadband usage and therefore promotes broadband investment," end quote. So this should incentivize broadband providers to invest heavily in privacy protection.

Is this what you see in the marketplace? Does it work in the market?

Mr. Haney. I think in the marketplace, privacy protection can be strengthened in the marketplace, but I think that current privacy protection is working in the market to incentivize all providers to invest, to create for consumers more abundance of choices, lower prices, services that we can't even imagine at this point. And I think that to the extent that Congress through legislation enhances consumer privacy, that it is very important, not only to be certain that all providers are created equally, but also that the privacy regulation is not overly burdensome.

Mr. Olson. Thank you.

Back to you, Commissioner McDowell, about my Houston Astros hats purchases

swarm me with ads. Most consumers, as we mentioned, don't want their call detail information released to third parties or used for targeted ads. It doesn't matter if that call comes from a digital telephone or even an app.

Do you believe the best way to address this problem would be with one technology neutral privacy rule that covers all call detail information?

Mr. McDowell. I think one standard would be very helpful and would allay a lot of confusion among consumers and market players of all kinds alike.

You know, so when I was at the Commission in 2007, we expanded the CPNI rules to what we call interconnected Voice over Internet Protocol providers, or interconnected VoIP, as we call it. But if you are not an interconnected VoIP, if you are just VoIP, using internet protocol through an app, then it is not regulated by 222. But to the consumer, it is the same function. It is a voice -- internet voice and video call to someone.

One type, if it is interconnected, is regulated in 222. Another type, if it is not interconnected to the PSTN, the public switched telephone network, is not. So that creates that asymmetry and a lot of confusion for folks, I think.

Mr. Olson. Well, thank you. I will close with a comment on Hurricane Harvey. During your tenure at the FCC, you were pushing hard after hurricane Ike hit my hometown about putting your lines below the soil, bury them. We did that for Harvey. Those lines stayed up the whole time. Information critical for emergency were being flown all across Houston areas. So thank you, thank you for that.

Go Blue Devils. Beat the Tar Heels forever.

I yield back.

Mr. McDowell. I did not ask him to say that.

Mrs. Blackburn. The gentleman yields back.

Mr. Pallone, you are recognized for 5 minutes.

Mr. Pallone. Thank you, Madam Chair.

Today's hearing highlights how much consumers on the internet have lost over the past year and a half. Consumers' privacy protections, consumers' data security protections, and consumers' net neutrality have been ripped away. So I think it is a rough time to be online.

The Republicans delivered a one-two punch when they rolled back consumer broadband privacy rules and then repealed the net neutrality safeguards that ensure the internet remain free and open.

So let me start, Ms. Moy, can you explain how these two anti-consumer actions worked in concert to give consumers fewer privacy protections online?

Ms. Moy. Sure. Yeah. So the first was these set of rules that really implemented section 222, the CPNI law, which, as I said, is one of the strongest consumer privacy laws that we have, and apply it to broadband providers. And unfortunately, Congress undid those rules, undid those regulations with the CRA resolution.

But even after the CRA resolution, section 222, at least the statute of it, still applied to broadband providers until the net neutrality -- the more recent net neutrality order that undid the net neutrality rules, as well as Title II classification.

So consumers now are left without the statutory protections of 222 to apply to broadband information and are left only with the baseline prohibition on unfair and

deceptive practices under section 5 of the FTC Act, which more or less just prohibits carriers -- well, broadband providers from doing things other than what they have told consumers in a consumer-facing statement they would do.

Mr. Pallone. Well, thanks.

Let me ask Mr. Haney. It is evident that in the internet age, so many different entities have access to our private information. And you also make mention of this in your written testimony. So if you could tell me, what types of companies, other than phone companies, have access to information traditionally thought of as CPNI, and are they subject to as stringent regulations as telecommunications companies?

Mr. Haney. I mention video streaming services, search engines, social networking sites, e-commerce sites, and user-generated media sites as examples. And currently, they are subject to the same privacy regulation as broadband providers, but as I mentioned, broadband is not the same thing as a common carrier telecommunications service. And therefore, only the common carrier telecommunications service, what we think of as telephone calls or any voice communication, excepting a voice app that is not interconnected to the public switched telephone network, that would be the only category that would be subject to the privacy protection that Ms. Moy supports.

Mr. Pallone. All right. Thank you.

Let me go back to Ms. Moy. I was alarmed by the reports of the vast throes of location data that third-party aggregator LocationSmart was making available to anyone on the web. It seems to me that we don't even know yet the entire scope of that incident. So do we know how exactly and how many companies or individuals have

access to the data that LocationSmart was making available and what these data were used for?

Ms. Moy. We don't know. You know, we know the one specific example of Securus, we know that in some detail because there were public records posted on the Georgia Department of Corrections website that showed screen shots from what the Securus platform looked like. And alarmingly, it enabled users of that platform to enter in the phone number of any phone in the country, upload a document of any sort, and without that document being scrutinized, they could obtain real-time location information for any individual in the country.

We do know, as I said before, from an AP report that 75 companies reportedly had access to location information through LocationSmart pertaining to Verizon customers. But I think it is safe to say that this is just the tip of the iceberg, right? I mean, if all four major wireless carriers were outsourcing a location information access to these third-party data brokers, only one of which is LocationSmart, then we are probably just seeing the very beginnings of what could be a massive investigation and a lot of privacy violations.

Mr. Pallone. Do you have any suggestions what the FCC could do to help us better understand the scope of this incident problem?

Ms. Moy. So the CPNI rules do require carriers to maintain records about who has access to customer CPNI, using the customer consent model. And so the FCC ought to be able to, using its investigatory authority, ought to be able to demand those records from the major wireless carriers, and that trail of records should lead them right down

the path to finding out how many violations there were. You know, and if those records don't exist, then that is a violation in and of itself.

Mr. Pallone. Thank you. Thank you, Madam Chair.

Mrs. Blackburn. The gentleman yields back.

Mr. Lance, you are recognized for 5 minutes.

Mr. Lance. Thank you very much. And I apologize to the panel for shuttling. We have several subcommittees this morning. This is a very important topic, and certainly we want to proceed in a bipartisan way on it.

Given the rules implementing 222 continue to distinguish between local and long distance service and impose authentication requirements that are 20 years and perhaps out of date, do you believe that the current rules make sense in today's modern marketplace or do you believe that we should update them reflecting consumers' current expectations?

And this is for the panel in its entity. Mr. Haney?

Mr. Haney. I believe the rules, sir, are out of date. They were designed, not only to protect consumer expectations, but they were also designed to try to allocate competitive advantages and competitive disadvantages in the marketplace as new entrants joined the market to compete with traditional incumbents. That dynamic is no longer relevant, and so I believe that the rules can and should be updated. But I do think it is important, sir, that the rules should apply equally to everyone. Every provider in the internet ecosystem is in a position to see and to collect information about consumers, some of it sensitive.

Mr. Lance. Mr. McDowell.

Mr. McDowell. I would agree with Mr. Haney in that the rules are out of date. You know, 22 years ago was when Congress passed section 222. Every aspect of the internet ecosphere is completely different now than it was then in terms of data collection as well.

And one also point to follow up on the exchange with Mr. Pallone, is that, you know, if you have a device, like Mary-Shea's little brother Cormac, he has a hand-me-down iPhone, but he is not a subscriber, so he lives off the land, so to speak, through unlicensed. And those transmissions -- voice, video, apps, gaming, whatever -- would not be covered, right, except by the FTC. They are not covered under 222.

So this starts to talk about the limitations or point out the limitations, and there are millions of nonsubscribers such as our youngest child, Cormick.

Mr. Lance. Thank you.

Ms. Moy.

Ms. Moy. Thank you. So the regulations almost were updated, as you know, and the updates to those regulations would have applied to phone providers who are subject to the CPNI rules as well as to broadband providers to whom the CPNI rules had been extended. And so -- you know, so that included, for example, an update of the data security provisions in the CPNI rules to do away with some of the more prescriptive things that was maybe an older approach to data security and to replace it with a more flexible, reasonable security standards -- or reasonable security measures standard in

accordance with several factors, such as the nature and scope of the carrier's activities, the sensitivity of the data that it collects, and so on.

So I do believe that updates to the rules such as those that were almost enacted that were passed in 2016 and then reversed by the CRA resolution would be appropriate. And the question is just how we get back to where we are.

Mr. Lance. Would they have applied across-the-board?

Ms. Moy. They would have applied to phone carriers as well as to broadband providers. If you are asking if they would have applied to other entities such as apps and so on, no, they would not. And I would completely support rulemaking authority to apply similar regulations to --

Mr. Lance. I am a co-sponsor of the chairman's legislation, the BROWSER legislation, and I would hope that the distinguished panel would look at it. And the chairman has taken the lead across this country in this area, and I am pleased to associate myself with what the chairman is attempting to do here. And I certainly agree with the panel that we need to update the procedures.

Mr. McDowell, if Congress enacts new privacy legislation, should information about calls be treated the same regardless of how a call is made?

Mr. McDowell. If Congress looks at this, yeah, again, back to one uniform standard, I think that that would be very helpful to everybody involved. As we are finding out today, it is a complicated issue. It doesn't need to be as complicated.

Mr. Lance. Thank you. And, Chairman, I yield back 32 seconds.

Mrs. Blackburn. The gentleman yields back.

Mr. Welch, you are recognized.

Mr. Welch. Thank you very much.

Mr. Haney, do you believe that the CPNI rules as they apply to telecoms have served a good function to protect privacy of telephone users?

Mr. Haney. I think the rules were more onerous than they needed to be, but --

Mr. Welch. Well, I -- go ahead.

Mr. Haney. I think that the requirement to get opt-in consent actually inhibited innovation, because as it applied to the incumbents in the marketplace, it is very difficult to get opt-in consent from consumers.

Mr. Welch. All right. I am going to come back to that. Do you think that the privacy protections, though, that were outlined in the CPNI did ultimately protect privacy rights of the users?

Mr. Haney. Yes, sir.

Mr. Welch. And would you have a problem having that privacy protection applied across all technologies?

Mr. Haney. I think if it applied across all technologies, it would be a huge improvement.

Mr. Welch. So CPNI across all technologies you would be supportive of?

Mr. Haney. Well, except for the fact that I do believe it is overly burdensome.

Mr. Haney. All right. I am going to try to summarize what I am hearing. Because, number one, all three of you, I think, want technology-neutral provisions, correct? And I don't think there is opposition up here to having it be

technology neutral.

Number two, you want a uniform enforcement so it is not complicated, right?

Mr. Haney. Yeah.

Mr. Welch. So, three, there is a big debate about this opt in or opt out. And essentially, that is the burden. Who is going to be protected? Is it going to be the consumer and he or she has the opportunity to opt in or opt out versus the burden that the opportunity costs for the technology provider.

Isn't that essentially what it boils down to?

Mr. McDowell. If I could add to that, yes. So certainly, and earlier what Mr. Haney said, there is the potential for opt-in fatigue, as we see with the GDPR in Europe. I don't think that is the standard we want to operate on. I think that would actually suffocate our internet ecosphere, but --

Mr. Welch. Let me --

Mr. McDowell. But uniformity, that concept, I think --

Mr. Welch. But here is the thing. I am a consumer. I don't have a clue how all these things operate, and that is how most of us are. I would feel much more comfortable if I was able to opt in or not. If it was the opt-in approach, I would feel more empowered.

Mr. McDowell. You know, coming over the horizon too real quick -- sorry -- we ought to probably have another hearing some day on blockchain and the evolution of blockchain and how that is going to help privacy protection. That is a whole other technological argument --

Mr. Welch. You know what, I actually got to say I don't buy that.

Mr. McDowell. Okay.

Mr. Welch. And here is why. There is always something over the horizon. All right. None of us have a clue as to what is going to be developed next year. But what we do have is the capacity to hit a key stroke and say we will opt in or we will opt out. Right?

And what I understand -- what I am hearing from you is that your apprehension of the opt-in is it will diminish innovation. All right. And I am not quite sure why you say that. I mean, this is like a key stroke. I mean, the amount of information that they can get over the computer can include a key stroke from Peter Welch on opt-in or opt-out, right? It is not a big deal, really.

Mr. Haney. Well, as we look at consumer behavior, when they are offered the opportunity to opt in, let's say one-third, for example, chooses to opt in. But when they are offered an opportunity to opt out, a very small percentage of consumers --

Mr. Welch. No, exactly. You have precisely defined the issue. Who is going to be the default winner or loser on this? And if the technology company has access to the information and then can sell it, then they are going to reap some reward for that. And you would like to think -- or you suggest that that is necessarily going to be a better product for me? I am not sure that is right. But I would like to be the one making the choice.

So I think the number one issue is who bears the burden here, because I know the companies would prefer to get and use all the information they can.

And then number two is a basic question about rulemaking. There has got to be some flexibility. And there is a lot of folks here who don't believe that Congress or anybody else should be doing any rules any time, any place, for any reason. I am not one of them, all right. Because that means that it is kind of the anarchy out there.

So do you have any opposition, you or Mr. McDowell, to some rulemaking authority as part of enforcement?

Mr. McDowell. To the FTC?

Mr. Welch. Well, the -- we can have a debate about FTC, FCC, the uniformity. I am sympathetic to having a uniform standard, but there has got to be real enforcement, in my view.

Mr. McDowell. Sure. So, historically, FTC has been the expert agency for privacy.

Mr. Welch. Right.

Mr. McDowell. So the FCC has had a very narrow aspect of this; only the common carriers and only regarding certain information for certain purposes under what we call CPNI. The whole rest of the universe in the privacy universe has been the FTC.

So I am not opposed to having the FTC with some limited rulemaking authority in this space.

Mr. Welch. Okay. I yield back.

RPTR ALLDRIDGE

EDTR SECKMAN

[11:14 a.m.]

Mrs. Blackburn. The gentleman yields back.

Mr. Shimkus, you are recognized.

Mr. Shimkus. Yeah.

Thank you, Madam Chairman.

To my colleague from Vermont, I wouldn't be so dismissive of the blockchain debate in this because -- and, Peter, if you got a second, I am sorry to interrupt -- because, you know, the country of Estonia has full data protection on personal health records, on data; they are totally wireless, phone app, every government entity. And they are a small country, but it is all blockchain-developed. And if you are following cryptocurrency and that debate, that is all blockchain too.

So I do agree that we ought to be looking at this as far as this privacy debate somewhere in the future on a different data because this could solve a lot of the problems of -- I am not the big cryptocurrency guy, but as far as an individual accessing other internet-provided government functions, I think Estonia has proven the safety of the use of this type of system. So I just want to throw that out since you mentioned it.

But I do want to go to Commissioner McDowell because of your position -- former position in the FCC. So we have some questions.

You have heard that this committee held a hearing with Facebook a few months ago. And if you didn't hear, you should have heard. There have been reports that

Facebook had collected call records and SMS data from Android devices and had the Facebook app installed going back for years. Our subcommittee chairs just sent letters to Google and Apple regarding their collection handling of location data amongst other information that is at the core of their operating systems.

Given your experience as an FCC Commissioner, I expect you are pretty familiar with filings. My understanding is -- and we are not, Members, we don't really follow how these filings occur. My understanding is that wireless carriers have a whole regime associated with serving these same devices. Those records are considered extremely sensitive personal information. They are CPNI and are subject to privacy regulations strictly enforced by the FCC.

What kind of reports are these entities required to file?

Mr. McDowell. So, under CPNI -- I am going to whip out my cheat sheet here because the Code of Federal Regulations can get kind of weedy. So they have to file an annual report. And, actually, under the FCC's privacy order from 2016, these reports were going to go away, and now they are back but only on common carriers. So that is just important, again, part of the asymmetry problem. But they have to first have an affirmation that the company, the carrier, has operating procedures in place to ensure that it is complying with the CPNI rules. Second, it has to explain how those operating procedures ensure compliance. Third, they have to report on any actions taken against data breach -- data brokers, rather. And data breaches are another story. And, number four, report on customer complaints concerning data breaches.

And then, when it comes to data breaches, they have to first notify law

enforcement and then wait 7 days before notifying the consumer. So there is a lot going on. But those are annual reports filed with the FCC.

Mr. Shimkus. What kind of consent must the provider obtain?

Mr. McDowell. So, you know -- so, for instance, if you want to pay your phone bill through your bank online bill pay and you want to see your call detail, you can't do it through your bank website unless you go to your carrier, your phone company, your wireless company, whoever it might be, and give them consent to share that information with your bank, for instance. So that is a form of opt-in.

Mr. Shimkus. And you mentioned that, in case of breach, there is -- they need to file notification of that, correct?

Mr. McDowell. Data breaches, they do. Absolutely.

Mr. Shimkus. That is all I have, Madam Chairman.

And I yield back my time.

Mrs. Blackburn. The gentleman yields back.

Let's see.

Mrs. Dingell, you are recognized for 5 minutes.

Mrs. Dingell. Thank you, Madam Chair.

I think that you have seen from this hearing that consumers are -- and what we are talking about every day when we are talking to people that consumers are consistently losing control of their private information across the board. First, it was Equifax; then Facebook. Now we have talked about LocationSmart today, a third-party aggregator of cell site location information, which has made Americans' location data

available to anyone with an internet connection. And I think that is what people don't understand. And when we are talking about where someone's phone is what we are really talking about is real location time any minute because I bet most of us in this room have a cell phone in their purse or their pocket right now.

These breaches of trust cannot become normal. And I worry that, with each passing scandal, we are becoming numb to this gross invasion of privacy. You know, I talk to people, and they say there is nothing we can do about it. But there is something that we can do about it. It is why we need to be talking, and I think too many people don't understand how much data there is and what people are doing about it.

So, Ms. Moy, I know you have answered questions, but I would like to dig in a little more.

Can you talk more about LocationSmart, how they obtain their information, and talk a little more about who had access formally but who informally or illegally could have gotten access to that information and what they might have done with it?

Ms. Moy. Sure. Yeah. So, you know, again, LocationSmart claims to have -- or was providing access to information, location information, for virtually any mobile phone user in the country. So it had direct access to the location information provided by all of the major wireless carriers. And it was providing that information informally.

I mean, and this really seems like the carriers essentially outsourcing access to their customer sensitive information and the whole consent process, right? So, if the carriers don't want to deal with trying to get consent on a case-by-case basis, for

example, applications that want to access the information from the carrier side or websites, that the carrier was outsourcing this function to a data broker, the LocationSmart company. And LocationSmart presumably is supposed to have been getting and keeping records of customer consent for every instance in which it was providing that location information. It was not doing so. It was not -- LocationSmart was not doing that for a long period of time. We don't know exactly how long, but we do know that the securest platform that, again, would have enabled anyone -- this is the sort of formal access to location information that you are talking about -- would have enabled anyone who worked in a prison and had access to the securest location-based services platform to just type in a phone number and upload any documents -- no one at the company was looking at those documents, according to the information that they told Senator Wyden's staff -- and then get real-time location information for anyone.

So this was going on for a long period of time. Apparently, either the carriers didn't know about it or didn't care. The FCC either didn't know about it or didn't care. And with respect to informal access, the LocationSmart platform also was not secure. So some security researchers demonstrated that they were able to -- that they were able to gain access to location information through the LocationSmart portal without having formal access to that system.

Mrs. Dingell. Ms. Moy, let's keep building on that.

Do you believe cell site location information is covered customer proprietary network information under the statute?

Ms. Moy. Yeah. I am really glad that you asked that question because it

certainly is information about one's use of the telecommunication service that is accessible to the carrier only by virtue of the carrier-customer relationship. And it is information pertaining to the location of the user. So, under the statute, this does, in my belief, meet the definition of CPNI. And so, to me, it does appear to be a CPNI violation that was happening on a massive scale.

Mrs. Dingell. So do you believe there were violations of section 222?

Ms. Moy. It does appear that way to me.

Mrs. Dingell. I will yield back my 29 seconds, Madam Chair.

Mrs. Blackburn. The gentlelady yields back.

Mr. Latta.

Mr. Latta. Thank you, Madam Chair.

And thank you all for being with us today.

Mr. McDowell, if I could start my questioning. There are many ongoing conversations in the realm of data privacy. The Digital Commerce and Consumer Protection Subcommittee, which I chair, has held several hearings on these issues, and we will hear from the entire FTC next week about their work in the area.

In your testimony, you mentioned the formidable protections of the FTC. And I have been clear about my support for the FTC's enforcement authority and even introduced a bill to make sure that the FTC's jurisdiction remained in place in the face of the legal challenge.

Do you believe that the FTC is equipped to handle privacy matters for the vast portion of the economy under its jurisdiction from Main Street stores to some of the

largest companies in the world, including common carriers, for their ever-increasing noncommon carrier activities?

Mr. McDowell. So I think in terms of privacy, it is the expert agency on privacy, and it is very well equipped in a lot of ways. They have brought hundreds of actions against a variety of companies, including broadband internet service providers in the privacy realm and have fined them, et cetera. So, from that perspective, yes.

Again, going back to kind of the premise of my opening remarks, though, we do need some harmonization and modernization, I think, of standards. They are an agency roughly the same size as the Federal Communications Commission in terms of budget, in terms of number of attorneys and economists and engineers, although fewer engineers there than at the FCC. So they might need help in that regard as these issues become more thorny and more widespread.

Mr. Latta. Thank you.

Let me follow up again, Mr. McDowell. I understand that under the current CPNI rules, telecommunication providers file annual compliance certifications. I also have a bill that strives to reduce the regulatory burdens on small businesses out there.

Do the rural telecom providers in my district have more stringent requirements than an edge provider offering similar services?

Mr. McDowell. Yes. So that goes back to that dichotomy, that duality between what a telecom carrier has in terms of their obligations under section 222 versus an app provider that might be providing the same functionality, let's say voice, through an app that is not regulated by 222.

Mr. Latta. Okay. Not picking on you. Another question.

In your testimony, you discussed how you voted to extend the CPNI rules in 2007 when you were Commissioner to cover a practice where data brokers, otherwise known as free texters, were obtaining unauthorized access to CPNI and then turning around and selling personal telephone records.

In 2013, the FCC also found that the CPNI rules applied to data collected on a mobile device if directed by the carrier. Under the section 222 authority given to the FCC, how far can the FCC extend the CPNI rules to cover current and future practices and services impacting telecommunication services?

Mr. McDowell. Excellent question.

So the Federal Communications Commission -- it gets to be alphabet soup pretty quickly -- is limited to applying section 222 to common carriers. If you are not classified as a common carrier, 222 can't apply. FCC does not have the authority. Only Congress could change that if it wanted it to.

Mr. Latta. Okay.

And, Madam Chairman, I yield back the balance of my time.

Mrs. Blackburn. The gentleman yields back.

Ms. Eshoo, you are recognized.

Ms. Eshoo. Thank you, Madam Chairwoman.

And thank you again to the witnesses and to Commissioner McDowell. It is really a special pleasure to see you again and to have your daughter with us as well.

I am so frustrated listening. I mean, I have learned. But the whole case of

privacy and what the Congress has done, I really think, needs to be restated. Congress is responsible for having wiped out privacy protections for the American people, period. That is why we are where we are. The CRA wiped it out. Whatever was left or whatever net neutrality contained in it relative to any protections, scorched earth, gone.

Now we have the BROWSER Act. It does nothing meaningful for real privacy. There is no rulemaking authority. There is no civil penalty for enforcement. There is no data security. It preempts any kind of State laws. California just passed something which is very strong. And, actually, when the strong bill came out, the interests went to work to water it down to a few drips of water, and Californians were outraged. And there was such pressure on the State legislature based on what Californians said that it came out strong. But the BROWSER Act preempts that. It also preempts the FCC, the expert telecom agency.

So where are we? I mean, 17 months and counting, blah, blah, blah, blah. Anyone that has voted, in my view, on -- for these things has to answer to their constituents when they complain to us, Independents, Republicans, conservative, right wing, left wing, Democrats, everyone, when they say: This is what has happened to me.

So, you know -- I mean, let's be honest about where we are. All right. So everything has been wiped out, in my view. There isn't anything protecting anyone. Where do we go from here? I don't think 220(b), whatever it is -- that really covers something very small. We are talking about a landscape that is very different, as you said, Commissioner McDowell, when that was placed on the books.

I don't believe that the -- there is a reason that some people want the FTC. The

FTC doesn't have what it needs to enforce a darn thing, in my view. And I don't know if Congress is going to step up and give them all these authorities that the FCC had.

All of a sudden, they love the FTC. FTC can't do a damn thing. It doesn't have any teeth to do it. They have asked Congress for a false set of teeth, but they haven't been purchased yet.

So, Ms. Moy, where do you go from here? Where would you start building something?

Ms. Moy. Thank you for the question. Thank you very much.

Ms. Eshoo. Yeah. Well, I mean, I am so darn frustrated. And it is like we are dancing around something that is really lovely, and we are just going to plant a few flowers, and then everything's going to bloom. Everything's been wiped out. That is why we are in the place that we are.

Ms. Moy. I think you are right, you know. So the internet does raise a bunch of important questions about privacy. But just because we now have apps that collect health-related information and wearable health devices, we don't have doctors in here complaining that they should not be subject to HIPAA. And we do not have schools in here asking that they not be subject to not be FERPA, the Federal privacy law, just because there are now educational apps and educational data is being collected over the internet.

We shouldn't do away with the existing privacy regulations that we have just because we are lacking privacy across the board. We need to keep and build on the privacy protections that we do have. And that is where I would say that whatever we

are going to have moving forward, it has to have rulemaking authority, strong enforcement authority, as you say, including civil penalties. And it ought to have a role for the State attorneys general who have much greater resources across the 50 States and territories than one Federal agency can have alone.

Ms. Eshoo. Let me just give Commissioner McDowell a few seconds. I know that we may not agree on some of this, but I want to hear what you have to say very quickly.

Mr. McDowell. So the CRA overturned the requirements on carriers only. This wasn't the entire internet ecosphere. So that goes back to the FTC.

Ms. Eshoo. So what is left? What is left? Who is protected and how?

Mr. McDowell. So through the Federal Trade Commission. So that is broadband and all the rest. So that is through the Federal -- if you think the FTC needs more resources or a different statutory standard, then that is certainly Congress' prerogative.

Ms. Eshoo. Okay.

Thank you very much.

Mrs. Blackburn. The gentlelady yields back.

Mr. Guthrie, you are recognized.

Mr. Guthrie. Thank you, Madam Chairwoman. I appreciate that.

And, Commissioner McDowell, in your testimony, you mentioned Marty Cooper and the first cell phone. You also discussed how competition is an important part of how CPNI rules came into existence. In addition to protecting consumers' privacy, the

rules were originally intended to promote competition in the emerging enhanced services market by preventing the regulated side of AT&T from sharing information with its nonregulated information services side.

And we have come a long way since the device Mr. Cooper had. But a legal landscape that reflects this evolution is not necessarily followed. It appears edge providers are freer to innovate as information is shared across all sorts of affiliated entities.

What effect does the current regulatory structure have on thwarting new entrants?

Mr. McDowell. So if the new entrant is not a common carrier, section 222 does not apply. So we have lower regulatory barriers. You are probably going to see more innovation and investment. That has sort of been the story of the internet ecosphere, or other markets as well. You could make a lot of case studies there.

So, if there is a new entrant in the telecom market, they would have to live under section 222.

Mr. Guthrie. So it is a disadvantage versus the edge providers for --

Mr. McDowell. It is a different -- yeah. It is a slight --

Mr. Guthrie. The more restrictive --

Mr. McDowell. Yeah. It is trickier.

Mr. Guthrie. More restrictive regulated.

If you argue unregulated allows you to -- or lower regulation allows more entrants, then they are more regulated.

Mr. McDowell. Correct.

Mr. Guthrie. Okay. So, Mr. Haney, what is the functional difference between placing a call from a smartphone using my wireless carrier's network and using a third-party app?

Mr. Haney. The only difference is legal. And the carrier -- using the carrier is subject to the full panoply of FCC privacy regulation; using an app that is not interconnected to the public switch telephone network is subject to the FTC the same as the rest of the internet ecosystem.

Mr. Guthrie. So completely similar products are completed --

Mr. Haney. Completely different treatment.

Mr. Guthrie. Different treatment.

Should my information be subject to different privacy protections depending on the network that I use?

Mr. Haney. No, sir, I don't believe so.

Mr. McDowell. If I could put a finer point on it, though. If it is unlicensed -- so you can have that transmission, as I tried to point out earlier through unlicensed. You are not a subscriber. That is not common carriage. It is not regulated. But the same functionality to the consumer, that would be unregulated.

But if it is through a carrier, it doesn't matter how that carrier is supplying it or providing a service, then that -- then section 222 would apply.

Mr. Guthrie. It is treated differently.

So the same -- I guess my point I am trying to get at is the same product is treated

differently based on --

Mr. McDowell. How it is done.

Mr. Guthrie. So, also, Mr. Haney, you stated the goal should be to prevent regulations from hamstringing some market participants but not others. And the logical way to do that is by ensuring that all participants in the internet ecosystem are treated the same.

Is there a role for Congress to achieve that goal through legislation, or is that preferable to rely on the Commission?

Mr. Haney. Sir, the FCC cannot do it. The FCC does not have legal authority to enhance privacy more broadly speaking than just telecommunications common carriers. So, if the goal is to provide the FTC with rulemaking authority, civil penalties, what have you, then that would require an act of Congress.

Mr. Guthrie. Okay. Thank you.

Well, I appreciate your answers to my questions.

And I concluded my questions, and I yield back.

Mrs. Blackburn. The gentleman yields back.

Mr. Butterfield, you are recognized.

Mr. Butterfield. Thank you very much, Madam Chairman.

And thank you to the witnesses for your testimony today.

As consumers, we are inundated with privacy policies from the companies with which we do business, whether it is financial institutions or doctors or hospitals or even ISPs and edge providers. We are forced to read these long legal documents on small

mobile device screens. And the older you are, the worse it is. Trust me, I know.

Sometimes we are even told that we cannot access a certain essential application for work or otherwise without quickly agreeing to the question. So I don't have it directed to any -- either of you. If anyone wants to respond, you certainly can. Do you think consumer privacy disclosures are effective in letting consumers know the kinds of information about them that is collected, how it is used, and whether and with whom it is shared?

Ms. Moy. I think you are raising a really good point about the deception standard, right, which is the FTC, the Federal Trade Commission, just has this authority to prohibit unfair and deceptive trade practices. So, when it comes to privacy, most of the time for consumers what that means is that our privacy is only protected insofar as we are reading privacy policies, agree with what is in them, actually have a choice about whether or not to agree to that -- you know, in theory, we have a choice -- and then that the company doesn't do something with our information other than what they claim.

And so this is why it is so important. We all know that there are so many instances in which we share our information, but we really don't have a choice. We don't have the time to read those privacy policies. Maybe we can't read them. They are very difficult to read. Maybe we are required, as you say, to have access to a service for work. And when we really do have no choice but to share information with a business that is going to use it for some other purpose, then it is so important to have standards in place that prevent that information from being used in other ways without our permission.

Mr. Butterfield. What say the Hudson Institute? Do you have some thoughts?

Mr. McDowell. So one aspect of all this debate, by the way, too, is the aspect of contract law and tort law. So every day there are class action lawsuits filed against a variety of market players in this space or other spaces too.

So the idea of foreign contracts in any industry, whether it is the internet or something else, anything, that is as old as America, if not older.

But, also, the idea of class actions as well as being a deterrent against these wholesale violations of contract or of common law that a contract might fly in the face of common law. So this is a whole other aspect of this whole debate which is important to know.

Mr. Butterfield. Okay.

Mr. Haney. May I just add that there may very well be a need to create more baseline regulation to -- for -- you know, to satisfy what we can all agree consumers expect to remain private. But there is no way the prospective regulation can anticipate everything that is going to happen in the marketplace. So there is, I think, an important role for user agreements.

And, also, in addition to class action lawsuits, press reaction, consumer outrage, the kind of response we have seen to secure it, I mean, all of those things I think play a role in terms of protecting privacy.

But I agree with you. I don't read the user agreements. They are incomprehensible most of the time.

Mr. Butterfield. That kind of leads me into my second and last question, and

that is, are you aware of any, I am going to say serious research, or do you have any ideas of how to make privacy policies more consumer friendly?

I know there is a lot of chatter about it, a lot of conversation. But is there any serious research going on about how we can go to the next level?

Yeah.

Ms. Moy. I know that there is -- there has been some good research here, including by a team of computer scientists led my Lorrie Faith Cranor at Carnegie Mellon on privacy policies. But I am not sure that there are any great solutions right now. Unfortunately, the legal complexities associated with these disclosures are extremely difficult to translate into a user-friendly --

Mr. Butterfield. That is what I needed to hear.

Any agreement with what she just said?

Mr. McDowell. It is complicated, to paraphrase Avril Lavigne.

Mr. Butterfield. It is complicated. Okay.

Do you associate yourself with Mr. McDowell?

Mr. Haney. Yes, sir.

Mr. Butterfield. Thank you.

I yield back, Madam Chair.

Mrs. Blackburn. The gentleman yields back.

Mr. Johnson, you are recognized.

Mr. Johnson. Thank you, Madam Chair.

Hopefully, I can see around to see all of you, but thanks for being here with us

today. Important topic that we are talking about.

You know, section 222 defines CPNI in part as, and I will quote, information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunication service subscribed to by any customer of a telecommunication's carrier and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, end quote.

Mr. McDowell, is this information similar to the information obtained by app developers and other edge providers who know, by nature of their relationship with the users of their platform, just how much consumers are using the app, when they are using it, where they are using it, and what they might even be searching for on that platform?

Mr. McDowell. It can be similar. And app providers and websites can actually gather even more data. And the reason being, it is increasingly true because more and more Web traffic is becoming secured, in other words, to where an ISP can't see what is transversing across its networks.

So what app developers can gather is a larger umbrella than what is covered by CPNI, which is viewed as a smaller subset of data, but very important data.

Mr. Johnson. So should we have similar rules to protect that kind of data? I mean, they seem awfully similar.

Mr. McDowell. So you are asking if we need CPNI rules to apply broadly to everybody. Is that what you are asking or the other way around?

Mr. Johnson. Well, should it apply to this kind of data that I just described to you --

Mr. McDowell. Yeah.

Mr. Johnson. -- third-party edge provides are collecting?

Mr. McDowell. You need -- yes. I think you need clarity here so that everyone knows what the rules of the road are.

Mr. Johnson. Okay. All right.

And again to you, Mr. McDowell. Do consumers differentiate between the various voice and texting services available on their phones, or do they view, for instance, Verizon mobile service and Google Voice as essentially the same service?

Mr. McDowell. The same functionality from the consumer's perspective.

Mr. Johnson. Okay. Section 222 protects the private information contained in traditional subscriber line bills. It also protects the location information of customers. Today's smartphones provide a host precise geolocation information on each device. This precise geolocation can locate a person within feet of their actual location. The network providers cannot access this information, yet we know the Android operating system does in order to serve ads to the device.

Is there a reason why the operating system should have this sort of precise information but not the carrier?

Mr. McDowell. So it is an excellent question. Your device can triangulate off of WiFi signals, cell towers, Bluetooth, any sort of radio frequency energy that is emanating if it knows where that is coming from. Then it can triangulate and tell you where this device is right now.

So carriers can tell where you are vis-à-vis a cell tower but not necessarily

specifically where you are. This has a lot of implications with 911 location accuracy and things like that. So there are times when you want everyone to where you are, and there are times where you don't want anyone to know where you are. And it shouldn't matter if it is telecom carrier or an app provider.

Mr. Johnson. Today, I don't know that consumers know who knows where they are. I am not sure they know where they are in this kind of interconnected environment.

Final question: What do you think of the consumer being given opt-in rights for this data in order to choose for themselves who they share it with?

Mr. McDowell. And we talked about this earlier, and the finer point on the discussion from earlier, which is opt-in gives consumers a lot of power for each time this issue comes up, right? So that is a good thing.

The downside to it -- and this is where we as policymakers, folks have to wrestle with it -- is the idea of opt-in fatigue. If you think of how many usernames and passwords you have for various websites and apps and everything else, and they change a lot -- you should be changing them a lot if you are not -- that is exhausting.

So opt-in can become exhausting. Can there be a mix, maybe a blend of opt-in or safe harbor, for instance, as well, that you know you are going to get a certain standard of protection in a safe harbor that does not require an opt-in? That is one idea which I think deserves some discussion.

Mr. Johnson. Okay. All right.

Madam Chair, I yield back a whole 10 seconds.

Mrs. Blackburn. The gentleman yields back.

And, Mr. McNerney, you are recognized.

Mr. McNerney. I thank the chair.

Ms. Moy, every day consumers are faced with another data breach undermining the choices they have about their privacy. But despite this troubling trend, last year, the Republicans in Congress voted to do away with reasonable data security requirements for internet service providers.

So how did the data security rules protect consumers before they were overturned?

Ms. Moy. Thank you.

Yes. So the broadband privacy rules would have required broadband providers and phone providers to take reasonable measures to protect their customers' information from unauthorized use, disclosure, or access. And they also would have required providers suffering a breach to notify affected consumers within 30 days. There were a bunch of factors to determine what reasonable security measures might look like in the rules, but, unfortunately, as you said, those rules have been eliminated.

Mr. McNerney. Are the ISPs subject to any data security rules today?

Ms. Moy. No. There are no concrete rules right now that apply to broadband providers.

Mr. McNerney. So it is the Wild West then, isn't it?

Ms. Moy. It is, in fact, the Wild West when it comes to data security.

Mr. McNerney. Okay. Can you explain why it is wrongheaded for Congress to repeal privacy rules in the name of protecting consumers?

Ms. Moy. So, you know, a colleague of mine had a great analogy here, which is, you know, if you have a house with a broken roof, you don't raze the house to the ground; you fix the roof. And I think that we are looking at something similar when it comes to privacy. You know, consumers are concerned about loss of control over their private information across the board. That suggests a need for greater and stronger privacy protections everywhere.

And as I said, I do think that it is important to modernize the Federal Trade Commission by giving it important tools, like rulemaking authority and strong enforcement, civil penalty authority. But we should not be doing away with existing privacy laws we have, like broadband privacy, but also health privacy, education privacy, and so on.

Mr. McNerney. Well, there are some privacy proposals, such as the BROWSER Act, that don't include specific protections for data security.

Do you think consumers have meaningful privacy protections without data security protections?

Ms. Moy. No. You know, I think they really -- privacy and data security go hand in hand. Consumers are -- what they are complaining about is a loss of control over their information. And that loss of control can come in the form of a business failing to get a customer's consent to use their information in a way that the customer didn't anticipate. But it can also come in the form of a business failing to safeguard the information from unauthorized access by malicious attackers or even by employees within the company as was the case with AT&T a few years ago in a case that ended up

resulting in an FCC enforcement action.

Mr. McNerney. What are some of the guiding principles that we should be considering whenever thinking about data security legislation? You have already given those, but --

Ms. Moy. I have. You know, but one that we haven't talked a whole lot about, I think, is really preemption. You know, and I know that this -- although this is not the topic of this hearing today, this subcommittee has considered a number of pieces of legislation to standardize data security and breach notification requirements that apply to companies.

But, unfortunately, many of those proposals would eliminate State law on data security and breach notification. And there are so many great and wonderful strong, innovative laws that are taking place at the State level that preempting all of those laws would be a net loss for consumers.

Mr. McNerney. Well, you have a way of answering the question right before I ask.

You testified that Congress -- that the State AGs should have enforcement authority. Does the BROWSER Act do this?

Ms. Moy. No, unfortunately not.

Mr. McNerney. Thank you.

Mr. McDowell, in addition to section 222 of the Communications Act, there are also important data security protections under sections 631 and 338. How important are these protections for consumers? And what can the FCC do to ensure that they are

being followed?

Mr. McDowell. They are similar in spirit. So 631, for instance, is regarding your video viewing habits, what you view. So it is about protecting consumer information. The FCC has enforcement authority, fining authority, et cetera, over those sections.

Mr. McNerney. Okay. Good. You think those are good and should continue to be enforced. But the FTC doesn't have the resources to enforce.

Mr. McDowell. Well, look. The FCC and FTC are similarly sized and almost identically sized agencies. So, again, you know -- and also back to the State preemption issue. It is a matter of how many agencies you are going to have with different standards for different piece parts of a converging internet ecosphere, and that is what becomes confusing.

Mr. McNerney. All right. I will yield back.

Mrs. Blackburn. The gentleman yields back.

Mr. Long, you are recognized.

Mr. Long. Thank you, Madam Chairman.

Mr. Haney, it is my understanding that the location information considered CPNI, if it is associated with a call over the telephone network. But it seems like tech companies have the ability to track location information not just associated with their app but with a variety of apps or an entire mobile device in some instances.

Who has better insight into location information, telecommunications providers or tech companies?

Mr. Haney. Sir, I believe it is tech companies.

Mr. Long. Under current law, what authority governs the collection of location information by smartphone manufacturers, operating systems, or apps?

Mr. Haney. That was the Federal Trade Commission.

Mr. Long. How does the authority differ from FCC's CPNI requirements?

Mr. Haney. The FCC's CPNI requirements are prospective regulation. It is very clear. The FTC recognizes that this is a dynamic marketplace -- the technology is always evolving -- and that it is impossible to anticipate everything and draft a regulation to address it. And so the FTC tries to be more flexible and to respond after there is a problem instead of trying to anticipate every problem.

Mr. Long. Okay. Thank you.

Madam Chairwoman, I yield back.

Mrs. Blackburn. The gentleman yields back.

Ms. Clarke, you are recognized.

Ms. Clarke. I thank you, Madam Chairwoman. And I thank our distinguished panelists for their testimony here today. Let me also thank our ranking member for convening this important hearing regarding privacy, an important topic for all Americans.

Under the FCC's broadband privacy protections, broadband providers had to get opt-in consent sharing most types of consumer's data. Unfortunately -- I believe unfortunately -- our Republican colleagues in Congress wiped those privacy protections off the books.

Ms. Moy, when I am using my internet connection at home today, are there any clear opt-in or even opt-out requirements that apply to how my ISP collects and uses my

data?

Ms. Moy. No. There are not.

Ms. Clarke. Okay. And what are the rules that apply to my broadband provider when it collects or uses my data? Specifically, what can the FTC require under section 5 of the FTC Act?

Ms. Moy. At this point in time, there are no rules. The FTC can prohibit unfair and deceptive trade practices. But it has very little power to do anything where there are privacy violations unless a business has actually exceeded what it told consumers in its privacy policy, which, as we know, most people don't read.

Ms. Clarke. Oh, boy.

Over the past several years, the extent to which corporate conglomerates will discriminate to improve their bottom line has come into focus. Whether it is broadband providers, redlining low-income communities, or Facebook discriminating against certain groups when it comes to housing advertisements, the result is marginalizing families in their communities.

I am concerned that the lack of meaningful privacy protections is only going to make these problems more pervasive. For that reason, I think Americans are in desperate need of strong privacy protections wherever they go online.

Ms. Moy, can you tell me how sacrificing privacy protections, like our Republican colleagues did with their privacy CRA, can have a desperate impact on some consumers, particularly those in communities of color?

Ms. Moy. Thank you, Representative. That is a really important question.

And I think that it really helps us put a finer point on what we are really concerned about when we are thinking about harms associated with privacy violations.

When a company -- when a business, whether it is a broadband provider or another type of company, has information about our private lives and they use that information to target content and advertisements to us, the targeting may result in reinforcing existing social disparities, right? Keeping us in our boxes. Limiting the educational opportunities that are available to us, the job training opportunities and, indeed, the job opportunities themselves, financial opportunities. And these are some of the results that may come from collecting information from consumers.

I think that that is why it is so important to have strong privacy rules where, as with some entities in the ecosystem, consumers really have no choice but to share information about their private lives that could reveal things like sensitive demographic information or financial status.

Ms. Clarke. Thank you.

As we consider legislative solutions to protect privacy, I am guided by the belief that any successful solution must not require our constituents to become lawyers or engineers in order to understand their rights and to protect themselves and their personal information. The privacy rules of the road can't change dramatically -- can change dramatically depending upon where someone goes on the internet. Rather, consistency, uniformity, and technological neutrality are keys to any privacy solution. Do you all agree on the panel?

Mr. Haney. Yes.

Mr. McDowell. Yes.

Ms. Moy. Yes.

Ms. Clarke. Very well.

Madam Chair, with that, I yield back.

Mrs. Blackburn. The gentlelady yields back.

Mr. Costello, you are recognized.

Mr. Costello. Thank you, Madam Chair.

Mr. McDowell, as Mr. Doyle referenced earlier, and, to me, what was just discussed about selling location data to third parties sounds more like an issue of consent and how we can make sure consumers truly understand what they are consenting to before they use a service. I think Ms. Moy alluded to that in terms of third-party consents. Oftentimes you don't even know what you are consenting to.

But I also understand that the FCC, and possibly even the FTC, are looking into what exactly occurred here. And will we have them both in front of the committee soon so we can ask additional questions of the investigation at the time? This is my question. I think this highlights the asymmetry in the current rules. If this was an edge provider who had shared location data, would it be subject to the same regulations?

Mr. McDowell. Not section 222, no.

Mr. Costello. Could you point to any regulation that it would?

Mr. McDowell. Not unless it has some affiliation with a carrier, so no.

Mr. Costello. Okay. Related also to section 222. CPNI, VoIP, et cetera, when you break it down -- my smartphone here. If I tap the phone app icon to make a call,

there is one set of rules. But if I tap the Google Voice app icon to make the call, which I don't do, there is another set of rules.

Can you talk about the practicality of having separate regulatory regimes in that sense? And should consumers expect their data to be treated the same regardless of what technology they use, to use the term "technology neutral"?

Mr. McDowell. Absolutely. Again, to your point, to the consumer, there is no difference. It is the same functionality. You want to convey a voice message in real time, have a conversation with somebody in real time. So it doesn't matter whose app or whose network or if it is licensed or unlicensed or it is through a carrier or through an edge provider -- by the way, I think they are all tech companies. I know we try to draw distinctions between ISPs and the tech community. I think they are all technology companies. And they are all great American success stories. But nonetheless, from the consumer's perspective, there shouldn't be any difference regarding what information --

Mr. Costello. And so the regulatory framework should be uniform.

Mr. McDowell. I agree, yes.

Mr. Costello. Up and down.

Mr. McDowell. Yes.

Mr. Costello. Ms. Moy alluded to, in her statement, the issue -- and we have read it elsewhere -- with States attorneys general. And, Ms. Moy, I will give you the opportunity to address this as well.

I understand that taking FTC regulations and having someone else enforce it at the

FTC, the argument goes, isn't being aggressive enough? But do you see -- do you have concerns with that? And then, after you answer that, Ms. Moy, aren't there some differences, though, with the statute that you are referencing just in terms of the technical expertise required to interpret vis-à-vis the statute that you were pointing to.

So Mr. McDowell and then Ms. Moy.

Mr. McDowell. Sure. And State attorneys general can do a terrific job protecting consumers on a number of fronts. My concern, though, is having 50 different standards or --

Mr. Costello. Totally.

Mr. McDowell. -- or more with all the territories. And that is going to really harm American global competitiveness in this space. So, again, back to uniform standards, not 50-plus standards State by State in the internet, which is borderless, right? It is an interconnected network of networks. The packets fly all across --

Mr. Costello. Isn't there also a fair amount of interpretational flexibility with those 50 attorney generals? I mean, the statute that Ms. Moy is referencing is pretty -- like, that is pretty straightforward, as I understand it.

Mr. McDowell. You know, I think to your point, if you are saying if there is going to be one standard, a national standard, but State attorneys general could enforce it, that is another conversation altogether.

Mr. Costello. Ms. Moy, your comments.

Ms. Moy. Thank you.

So, you know, I think that part of the issue here is that the FTC, while it does a lot

of great work on privacy, it has a staff of just over 1,000, if I recall correctly. It doesn't have an office of engineering and technology. It doesn't have an engineering department at all. And its jurisdiction ranges as broadly -- you know, although it does a lot of internet privacy work, it also polices, for example, the consumer-facing statements made about pomegranate juice, right? You know, I mean, it has an incredibly broad jurisdiction with very limited tools to enforce.

So it is really important to have additional enforcement actors, additional cops on the beat, as it were, to ensure that businesses subject to the regulations passed by the commission are, in fact, being followed.

Mr. Costello. But wouldn't you think if the FTC needed those additional policemen, as you used the term, they would request them, or they would find a way in their budget to have them?

Ms. Moy. So, yes, perhaps.

Mr. Costello. Might that be called something different than -- I mean, you referenced the FCC division there. Might they be operating in a different division with the same type or better expertise on enforcement?

Ms. Moy. Perhaps. But another thing that State attorneys general do is they talk to businesses that are based in their State. You know, they do a lot of guidance in addition to enforcement.

Mr. Costello. Thank you. I yield back.

Mrs. Blackburn. The gentleman yields back.

Ms. Matsui.

Ms. Matsui. Thank you, Madam Chair. And thank you to the panel for being here today.

We have talked about many things, and maybe I might be repeating myself. But I think we should sort of listen and try to figure out from you all where we might be going forward because when you look at it, this concept of protecting proprietary consumer information began with the monolithic telephone era, which was pretty far back. And with the 1996 Telecom Act came a more precise focus on CPNI protections against unauthorized use, access, and disclosure. And it includes, among other types, phone numbers, dial and duration of calls placed to these numbers.

But we all know that most consumers don't make any distinction at all between where these phone calls are delivered in packets, over the internet, or through switch access lines.

But we all understand the need for context-specific privacy regulations that are responsive to the types of consumer relationship and sensitivity of information collected and shared to actually afford consumers the privacy protections they expect and they figure they are getting, for some reason.

Ms. Moy, as different technologies provide similar services, what distinctions remain necessary or become unnecessary to protect sensitive consumer information?

Ms. Moy. That is a very good question. And it is a really hard one that we are all grappling with right now.

But, nevertheless, I do think that consumers have different relationships between the carriers that they contract with, that they pay a monthly subscriber fee to, that they

expect they are paying for service as they do with the entities that are doing business over the internet. Just as when you send a letter in the mail to a friend, you have different expectations about what the mail carrier will do with the address information and the date on the outside of the envelop. So does the consumer have different expectations about what, again, the entity that they are just paying to transfer the data on their behalf will do with their private information as opposed to the companies with which they do business.

That said, I do agree that there are certain services that consumers use now that have become so pervasive, so dominant that they are essentially unavoidable. And I look at unavoidability as, really, one of the key factors when it comes to considering what level of privacy protections should apply. When services truly are unavoidable for consumers and they have to share sensitive information, then I think that heightened privacy is appropriate, just as with healthcare, education, and finance.

Ms. Matsui. Okay. Could you get into more detail there? What do you think is unavoidable here that we are talking about?

Ms. Moy. So, without talking about specific entities, I do think that there are certainly certain advertising platforms that are so pervasive as to be essentially unavoidable for consumers to share information with. There are -- you know, as I believe it was Congressman McNerney -- or, no, I am sorry. It was Congressman Butterfield referenced certain services that consumers feel they must have a -- they must take part in because an employer requires it, for example. That may rise to a level of unavoidability for a consumer. And I think that, you know, when we start seeing

services rise to the level of being essential or unavoidable, then we require heightened privacy.

Ms. Matsui. Okay. How about -- Mr. McDowell, Mr. Haney, any comments on this?

Mr. McDowell. So I think -- I am not sure if this is what was said, but I want to make sure we understand that there doesn't have to be a difference between who you pay money to for a service versus you are giving your personal data for a free service. You are actually surrendering something for free services as well. So they are not entirely free.

But, again, back to one uniform consistent tech-neutral standard, I think that is the way to go.

Mr. Haney. I agree.

Ms. Matsui. Okay. CPNI rules enacted require opt-in consent from consumers before a carrier can share information. But we know that it is often the case the third party to an online platform can and does receive data and information on the consumer. And the website may be used as an analytic tool from a third party; the website servers could send information on the user's visit back to the third party and allows that third party to access data similar to that gathered by the website.

While this may be commonplace, it means that each user may have information aggregated by a party with whom they have no direct relationship or knowledge. There are a lot of parties here. So the third party accesses consumer data with whom the consumer does not have a direct relationship. How do consumers have a meaningful

choice in how that data is used?

Ms. Moy. That is a great question. That really gets to the heart of what the problem is with falling back on a general deception standard without rulemaking authority or anything else for the FTC to clarify -- clarification, perhaps of its unfairness authority, rulemaking authority for it to create rules around things like data brokers and data security as well would be necessary.

Ms. Matsui. Okay. Thank you.

It looks like I have run out of time. Thank you very much.

I yield back.

Mrs. Blackburn. Mr. Flores, you are recognized, 5 minutes.

Mr. Flores. Thank you, Madam Chairman. I want to thank the panel for joining us today.

When I do something with this phone, there is -- I see four groups of people that is harvesting data from it. So not only is the cellular carrier getting information, but your app provider is getting information. The IOS folks, the operating system folks, are getting information, and theoretically, the ISP is as well if it is connected to WiFi.

So you have all talked about the need for a technology-neutral solution to address privacy. So I would like to get into the weeds a little bit today.

As a policymaker, what are the three or four most important things that that policy should have to protect the privacy of the American consumer?

So we will start with you, Ms. Moy. And let's go quickly, because I have some --

Ms. Moy. At the risk of sounding like a broken record, I think it is crucially

important to -- you know, first of all, I do think that sectoral laws have a place and are really important to protect consumers in instances like health, education, finance, and telecommunications where there are heightened privacy obligations and requirements.

But in addition, I think that whatever baseline we are going to have, if it is to be administered by an expert agency such as the Federal Trade Commission must include rulemaking authority to provide flexibility, regulatory agility, as we think of it, as well as robust enforcement tools, including civils penalties.

Mr. Flores. Okay. Mr. McDowell.

Mr. McDowell. Sure. Transparency, uniformity. But also, most importantly, probably consumer choice. I would support rulemaking authority for the Federal Trade Commission but in a very limited way.

Mr. Flores. Okay. All right.

Mr. Haney.

Mr. Haney. Yes, sir. I think that enforcers should consider burdens on industry as they affect consumers, as they may affect innovation. I think that the FTC has got it right in looking at the sensitivity of the information at issue, so I think that is very important.

Secondly, I think it is very important that the rules apply equally to every participant in the markup so that everybody has the same opportunities to innovate and to earn a fair return on investment.

Mr. Flores. Okay. Great.

Mr. McDowell, we had a question a few minutes ago about 50 States attorneys

general being used to pursue privacy -- policy relief for consumers. One of the things -- I mean, California has passed a law 2 weeks ago.

Would you agree that that is the wrong approach as well, to have 50 different State standards?

Mr. McDowell. Yes, I disagree with that approach.

Mr. Flores. Okay. You were going down a direction a few minutes ago talking about blockchain, and you got cut off, unfortunately. And it seems to me like blockchain may be one of the technology solutions that addresses a lot of these policy issues.

Can you expand on that? You didn't get a chance to before.

Mr. McDowell. Sure. Real quick.

So, first of all, it is already part of our lives. And as we start to roll out the internet of Things, you are going to see more and more blockchain applications. And there is a tremendous amount of entrepreneurism and investment in this space, a lot of experimentation. And it is actually very pro-consumer, empowers consumers tremendously. And it is different from encryption. Technically, they are two different things. So I think it will solve a lot of issues.

And the quick backdrop on that is I think the first time I testified before this committee was 1998, so 20 years ago this summer. I am just recalling, in front of Chairman Dingell. And it was on slamming, which was the unauthorized switching of your long-distance carriers. That is not as much of an issue any more, right? So long distance isn't even a thing anymore. So markets change. Technology changes. So I think blockchain is going to be tremendously helpful as it develops.

Mr. Flores. Okay. Is there any change in your answer regarding what we should have in a 21st century privacy policy solution in light of the fact that blockchain is on the horizon?

Mr. McDowell. Well, flexibility and light touch. And I tried to put that in my pre-filed remarks, that light touch, we have to make sure we are not cutting off innovation and experimentation and investment.

Mr. Flores. Exactly.

Ms. Moy, a question for you. In the context of the FCC's broadband privacy proceeding, you argued against pay for privacy because of a lack of broadband service options.

What are your thoughts on a pay-for-privacy solution when it comes to Facebook and other similar providers?

Ms. Moy. Thank you for that question. I think that that is a really good one.

My concerns about pay for privacy -- so I do not believe that privacy should be a luxury available only to those individuals who can afford it. That is the place where I start with when I am thinking about pay-for-privacy issues. That is particularly the case where, as with broadband, you are looking at an essential service. So -- and something where consumers really can't avoid sharing information about themselves. If consumers have no choice but to share information with a broadband provider in order to participate in the modern economy, then they should not be required to pay a premium that they cannot afford in order to protect that information from additional uses.

And so my position on pay for privacy in the broadband context was that

premiums that may be charged or discounts given should not be coercive in nature to consumers nor should they make privacy options essentially practically, as a practical matter, unavailable to consumers who cannot afford them.

I think that if we are looking at other services, then the threshold question is, is this service essential, a service that consumers cannot avoid sharing information with? If so, then I would have the same feelings about pay for privacy.

Mr. Flores. Thank you.

I think with regard to competition in the broadband space, I think as 5G rolls out on the near-term horizon that we are suddenly going to see that extra competition that will help the -- you know, absent a solution on privacy for the ISPs, I think we are going to have a market solution that helps us get there.

That is the last of my questions. I yield back.

Mrs. Blackburn. The gentleman yields back.

Mr. Engel.

Mr. Engel. Thank you, Madam Chair.

Companies across the globe are changing the way they collect and use consumer data, and we are seeing more sophisticated practices, which obviously results in more challenges to American's privacy.

Ms. Moy, you testified that agencies tasked with protecting consumers' private information should be given rulemaking authority. And you referenced remarks from Commissioner Maureen Ohlhausen when she asked Congress to give rulemaking authority to the FTC.

So my first question to you is whether you think that rulemaking authority should be given to the FTC, the FCC, or both.

RPTR KEAN

EDTR SECKMAN

[12:11 p.m.]

Ms. Moy. So I think that each agency needs rulemaking authority for the areas in which it has expertise. We have separate expert agencies for reasons. The Federal Communications Commission has greater network expertise and communications expertise. And, again, has this Office of Engineering and Technology, a whole staff of network engineers that the Federal Trade Commission lacks.

The Federal Trade Commission, on the other hand, is responsible for enforcing this baseline general privacy standard across the entire ecosystem, including, as I was saying before, the marketing of products like pomegranate juice.

So the Federal Trade Commission needs rulemaking authority for general things, like data security obligations that ought to apply to all entities. It probably needs a clarification of its unfairness authority, particularly in light of recent court decisions that call into question how strong its authority is under that, under the statute.

The Federal Communications Commission still requires rulemaking authority to implement those sections of the Communications Act that it is responsible for implementation and enforcing.

Mr. Engel. Does the FTC have the resources it needs for enforcement? For instance, I was told that the tech lab only has six people in it.

Ms. Moy. That is right. That is right.

You know, I mean, I think the Federal Trade Commission is doing the best job that

it can with a relatively small staff, but, again, a staff of 1,100 people for the entire agency can't possibly be enough to police all of the unfairness and deceptive potential practices of all companies across the entire country, including privacy of the entire internet ecosystem.

Mr. Engel. Ms. Moy, let me continue.

As you know, one of the proposals that we are considering in this committee is the BROWSER Act. And if you can, could you discuss the rulemaking authority contained in the BROWSER Act and whether it will make for better and clearer privacy enforcement?

Ms. Moy. Right. If I am correct, the BROWSER Act does not give rulemaking authority. I think that that is problematic. I think that any -- as I was saying before, I think that any privacy law that we have in this area ought to have rulemaking authority and civil penalty authority and strong enforcement provisions, ideally an enforcement role for State attorneys general as well, or even private citizens.

Yeah, I mean, so I think that the BROWSER Act could be strengthened for sure.

Mr. Engel. So you just said private citizens. Should Congress consider granting private citizens the right to bring civil actions against companies for violating privacy regulations?

Ms. Moy. I do think that if Congress is serious about ensuring that businesses actually adhere to the standards set forth in the statute, then a private right of action is one of the strongest enforcement mechanisms you can have to ensure that that takes place.

Mr. Engel. Now, rulemaking authority may help to protect consumer privacy but

such protections still need to be enforced in order to be effective.

So let me ask you this: Do you think the FCC has done an adequate job of enforcing section 222 which establishes the duty of telecommunication carriers to protect the confidentiality of proprietary information?

Ms. Moy. I think that, at times, it has. It has not always been consistent, which is one of the reasons that it would be great to have additional enforcers, additional cops on the beat that can enforce those regulations.

In recent years, the FCC brought actions against four different carriers for CPNI violations, but since the change in administration, I don't believe there have been any.

Mr. Engel. Would more robust enforcement help fend off some of the abuses that have come to light recently such as what is happening with LocationSmart.

Ms. Moy. Certainly. I mean, I think we still haven't seen anything come out of the LocationSmart scandal. You know, it could be one of the largest privacy violations that we have had in recent years, maybe as big as the, you know, the Facebook-Cambridge Analytica scandal, but all we have heard is crickets from the FCC.

Mr. Engel. Thank you. I see my time is up, Madam Chair. Thank you very much.

Mrs. Blackburn. I thank the gentleman.

Mr. Bilirakis, you are recognized.

Mr. Bilirakis. Thank you, Madam Chair.

I appreciate it very much. Mr. Haney as broadband was able to spread over the last 20 years, the rise of killer apps received a boost from the light-touch policies we put

in motion. Gmail and Google Voice are two such services.

Gmail has been in the news recently as reports indicate that, even though Google said it would stop scanning the traffic, the company still permits software developers outside of Google to scan Gmail inboxes.

Google said that it only gives data to outside developers it has vetted. So it only gives data to outside developers it has vetted -- again -- and to whom users have granted permission to access email.

However, that still means software developers are able to review who sent an email, who it was sent to, the time sent, and the contents of the message itself, which might contain health information, financial records, or other sensitive personal information.

Is any of this information protected by the CPNI rules?

Mr. Haney. No, sir, it is not.

Mr. Bilirakis. It is not.

Mr. Haney. It is not. It doesn't relate to telephone calls that have actually called. It doesn't relate to duration of the telephone calls, the timing, or the phone numbers of the calls that were made. So CPNI would not apply to that situation.

Mr. Bilirakis. Thank you for answering me that.

Again, Mr. Haney, you mentioned a few times that often systems are burdensome and are reserved only for the most sensitive personal information.

Can you expand on the cost of the compliance with, again, with the CPNI rules?

Mr. Haney. I listed one example in my testimony. One of the

telecommunications common carriers attempted to get opt-in approval across its subscriber base, and it was successful only 29 percent of the time or 29 percent of its customers. And the cost that incurred was over 20 dollars for every affirmative response that it got. And so -- and there are other studies that come up with, or other examples, other anecdotes that come up with simply results. Most of the time, consumers take no action. And this is verified because when they're offered the chance to opt out, very few choose to opt out.

And so I think the FTC is really, really on to something here by trying to categorize the most sensitive information that warrants the, you know, the top, the highest protection, and, similarly, to try to identify more routine information, information that is not as sensitive, that doesn't require the most burdensome protection.

Mr. Bilirakis. Okay. Very good. I think you answered my third question as well. So I appreciate it very much.

And I yield back, Madam Chair.

Mrs. Blackburn. The gentleman yields back.

At this time, I recognize Mr. Collins for 5 minutes.

Mr. Collins. Thank you, Madam Chair.

Thank you. When you have multiple hearings going on at once, here we go.

What I want to talk about, really, are the kinds of apps that we now know are being offered by various retailers in the name of giving you discounts, you know, the frequent buyer program, or whatever. But we know that, in some ways, if you loaded that app on to your phone, all of a sudden, whether it is a Target or a Walmart or

whomever, they may be able to track other information unknowingly.

So, Mr. Haney, I want to break this down a little bit. If you have such an app on your phone, you are in a retail establishment and you are going to use this, perhaps, for discounts or other things, can you talk about, a little bit, how that might work?

Mr. Haney. Well, when I go to Home Depot, I believe my Home Depot app on my phone, it can tell me what aisle I'm looking for. It can tell where I am in the store, what store I'm in. I couldn't probably imagine every use that some of these brilliant people that are designing these apps, you know, are contemplating. But the phones have multiple sensors in them, and apps can access some of the same information that other apps can access because it is stored in the operating system.

And as far as whether, you know, it is fair to expect consumers to anticipate all of the different uses, all of the different ways they can be tracked, I don't believe it is fair to expect them to anticipate that in every case.

But I do think that policymakers need to think in terms, not what agency has an office of engineering and what doesn't; I mean, we are talking about some very similar issues here. We are talking about irrespective of whether the underlying telecommunication services are being used for voice communication or an app that never connects with a Public Switched Network, we can always agree that what we are talking about is a voice communication.

And I think that, again, striving for uniformity and striving, if we are going to increase the baseline through regulation, anticipatory regulation, if we are going to increase that baseline, let's just really strive to make it the least burdensome that we

possibly can, to not try to anticipate everything that the marketplace may dream up. Let them experiment a little bit. But it may be appropriate to increase the baseline.

Mr. Collins. I think that is all of our concerns. Everyone wants a discount, and you don't know what you don't know. And so, in this case, it could be your WiFi; it could even be your microphone, certainly your GPS. And I think my concern would be, once you leave the store, is that off? I know, on my phone, I have got an app -- it asks me, do I want to keep my location open all the time, or do I want to have my location only working when I have activated it? And most folks don't even know how to turn that on or off. So we are all about protecting our consumers, but this technology is going way faster --

Mr. Haney. Yeah.

Mr. Collins. -- than anything we could imagine on the consumer protection front. We don't know what we don't know. So, I guess, Mr. McDowell, I guess you would agree most consumers don't anticipate or know to the extent to which somebody could be tracking them.

Mr. McDowell. First of all, I want to associate my remarks with Mr. Haney's just now. They were terrific.

Absolutely, we don't know what we don't know. We don't know what is coming over the horizon. So there is that balance between we want to make sure we have this robust experimental marketplace that I believe firmly brings us more benefits than harms, but it does bring us harms, and so what do we do about those as policymakers?

Mr. Collins. Well, I appreciate that. Sorry I was late, Madam Chair.

But I yield back and thank the witnesses for their testimony.

Mrs. Blackburn. The gentleman yields back.

And there are no other members at this point wishing to ask questions. So we appreciate all of you being here today.

Before we conclude this hearing, I ask unanimous consent to enter into the record the following documents: An article from Axios, an article from Fast Company on location tracking, an article from Ars Technica on call record scraping.

Without objection, so ordered.

[The information follows:]

******** INSERT 3-1 ********

Mrs. Blackburn. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions. And I ask the witnesses to submit their responses within 10 business days upon receipt of the questions.

Seeing no further business to come before the subcommittee today, and as you all see, there is agreement that we need to address the privacy and data security issues, without objection, the subcommittee is adjourned.

[Whereupon, at 1:25 p.m., the subcommittee was adjourned.]