<u>RPTR TELL</u>

<u>EDTR CRYSTAL</u>

DO NOT CALL: COMBATING ROBOCALLS

AND CALLER ID SPOOFING

FRIDAY, APRIL 27, 2018

House of Representatives,

Subcommittee on Digital Commerce and Consumer Protection,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 9:03 a.m., in Room 2123, Rayburn House Office Building, Hon. Robert Latta, [chairman of the subcommittee] presiding.

Present:  Representatives Latta, Kinzinger, Lance, Guthrie, Bilirakis, Mullin, Costello, Duncan, Walden (ex officio), Schakowsky, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Staff Present:  Mike Bloomquist, Staff Director; Daniel Butler, Staff Assistant; Margaret Tucker Fogarty, Staff Assistant; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection;

Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Zach Hunter, Director of Communications; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Drew McDowell, Executive Assistant; Hamlin Wade, Special Advisor, External Affairs; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; Lisa Goldman, Minority Counsel; Jerry Leverich, Minority Counsel; Caroline Paris-Behr, Minority Policy Analyst; and Michelle Rusk, Minority FTC Detailee.

Mr. <u>Latta.</u> Well, good morning. I would like to call the Subcommittee on Digital Commerce and Consumer Protection to order. And the chair now recognizes himself for 5 minutes for an opening statement.

Good morning again. We thank our witnesses for being here. We especially appreciate your patience and flexibility, adjusting your travel plans after the hearing was rescheduled from last week.

We want to thank you for being here to help us explore the range of solutions and strategies available to consumers to combat the scourge of robocalls, caller ID spoofing, and telemarketing scams. It is critical that we help consumers understand their options when it comes to robocalls and spoofing.

For example, consumers can download robocall-blocking apps for their mobile phones and contact their landline and wireless providers for call-blocking options. They can register their home or mobile phones with the national Do Not Call Registry, which protects their number from legitimate telemarketing calls they do not want to receive.

And there are other commonsense strategies, like not answering your calls from unknown numbers and not following any prompts if you do not know who the call is from. For example, do not "press 1 to take your name off this list."

Good options are available, but I think all of us, including industry, can and should do a better job of education, particularly with our seniors, to make sure that new scam ideas are stopped quickly.

So what is a robocall? When the phone rings with an automated

prerecorded telemarketing message, that is a robocall.  They are a nuisance and they are illegal.

Yet every day tens of thousands of American consumers report receiving a robocall.  And I would like to just play a real quick robocall, quote/unquote, from the IRS.

[Audio recording played.]

Mr. Latta.  And that message goes on.

A staggering 3.2 billion robocalls were placed nationwide in the month of March, according to one source, alone.  In Ohio's 419 area code alone, my area code, nearly 12 million robocalls were placed.  For every month in the past year robocalls made up the majority of Do Not Call Registry complaints at the Federal Trade Commission.

As technology evolves allowing for a greater volume of robocalls, so are the tactics used to trick consumers into answering.  In the past scammers would fake caller ID information to trick consumers into thinking their bank was calling or the phone number was unknown.

Scammers are now deliberately falsifying caller ID information knowing I am likely to answer a phone call that appears to be local from my family, a doctor, or the church.  Neighbor spoofing, as it is known, is a deliberate tactic behind unwanted calls and texts to both wireline and wireless phones.

Robocalls and spoofing have the potential for real financial harm.  Fraud from unwanted calls amounts to almost $9.5 billion annually, according to the FTC.

It is not hard to see how scammers could use deceptive tactics

to convince people, often senior citizens, to hand over their personal information or to purchase fraudulent goods and services.

Take the IRS tax scam, for example.  You get that unexpected phone message claiming to be from the IRS.  The call might say you owe taxes that must be paid immediately with a credit card or a debit card.

Scammers have been known to use the threat of a lawsuit or arrest by the police to convince victims to hand over bank account information. Consumers may also get out-of-the-blue calls offering to help them lower debt or interest rates or promising other limited-time deals.

Senior citizens are often targets of elderly-specific roboscams relating to Medicare, healthcare, or funeral arrangements.  But they are not the only ones who fall victim to these scams.

Fortunately, American consumers have options and strategies to fight robocalls and caller ID spoofing and to protect themselves, which we will explore today with our witnesses.

The technology and tactics used by scammers may change, but as subcommittee chairman, I remain focused on empowering consumers and keeping them safe from unfair, deceptive, and malicious practices.

Again, I want to thank our witnesses for being here today.

And with that I will yield back and recognize the gentlelady from Michigan for 5 minutes.

[The prepared statement of Mr. Latta follows:]


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

Mrs. <u>Dingell.</u>  Thank you, Mr. Chairman, and thank you for holding today's hearing on robocalls and spoofing.

And thank you to the witnesses for being here today.

Robocalls are a great annoyance for American families, especially American seniors.  One third of the calls now are unwanted robocalls. Just in March, a record 3 billion robocalls were placed to American consumers, and about a quarter of those calls are scam calls.

We are now at a point in my household when the hard line rings I tell my husband, "Don't answer it."  And he thought I didn't pay our taxes.  He got pretty upset with me actually.  It took me a while to convince him I had.

I hear repeatedly from my constituents that they want these calls to stop.  One constituent in Ann Arbor wrote:

"My landline and cell numbers are both on the Federal Do Not Call Registry.  I checked.  I am so angry about all the calls from offshore call banks telling me that my computer is broken or that I need help with medical insurance and my college loans.

"Exactly what does the Do Not Call list do?  Not answering and letting someone call back isn't an option, as I have an elderly parent who does call.  I am also not wanting to go to the expense of updating my phone system to get caller ID."

There were many more just like this, and to no one's surprise there wasn't one letter in support of robocalls.

Democrats on the Energy and Commerce Committee have been listening to their constituents and we are taking action.  This week

Democrats are introducing three bills to help stop robocalls.

Ranking Member Pallone introduced the Stopping Bad Robocalls Act, which would strengthen the Telephone Consumer Protection Act and help the FCC take action against robocallers.

Congresswoman Eshoo introduced the HANGUP Act, which would require debt collectors contracted with the Federal Government to get consumers' permission before robocalling or auto dialing consumers.

And last, but certainly not least, today we have released a discussion draft titled the CEASE Robocalls Act. This draft legislation would lift the common carrier exemption in the Federal Trade Commission Act so that the FTC can take action against these smaller voice over internet protocol, otherwise called VoIP services, that are a huge player and heavily involved in illegal robocalls.

I am looking forward to getting feedback from all of you today about the discussion draft.

Today we will hear from witnesses about some of the exciting and promising tools available to consumers wishing to block robocalls. But consumers don't just need new tools. They need new protections.

We have put forward commonsense ideas to stop Americans from being harassed by unwanted calls. I hope we can all work together to move this legislation forward and make progress on the issue because many of us are growing tired of having to leave their phones on silent.

Thank you, Mr. Chairman, and I yield back my time.

[The prepared statement of Mrs. Dingell follows:]

\*\*\*\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*\*\*\*

Mr. <u>Latta.</u>  Thank you very much.  The gentlelady yields back.

The chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

The <u>Chairman.</u>  Thank you, Mr. Chairman.

I share the passion of the rest of the members here about these unwanted, unnecessary, and oftentimes fraudulent calls.  I get them on my cell phone all the time.  They appear to be coming from I think my home at times, they are that good anymore.

And we have got to do something about this.  And we have.  I am going the talk about that in my opening statement here a bit.

And then we appreciate our witnesses for being here.

Robocalls and caller ID spoofing have exploded in recent years, 3 billion calls placed last month alone, they estimate.  And we all get them.  And they interrupt our dinners, they interrupt our family time, they interrupt meetings.  They are real annoying, to say the least.

At worst, they have the potential to scam and defraud both consumers, seniors, and others.  According to the Department of Justice, scams targeting the elderly are increasing dramatically and fraudsters steal an estimated $3 billion from American seniors every year.

It is now more important than ever to educate consumers on how to detect and avoid fraud stemming from these robocalls.

The Federal Trade Commission and the Federal Communications Commission, as well as our committee, have taken steps to protect

consumers from robocalls and spoofing.  Both the FTC and the FCC operate consumer complaint websites and hotlines where consumers can report illegal telemarketing calls.

Reporting can help the agencies crack down on illegal callers and improve the data they share with the industry players and telecommunications companies, who then develop solutions.

The Federal Trade Commission also manages the Do Not Call Registry, where anyone can register their home or mobile phone for free.

Here at the committee we recently passed the RAY BAUM'S Act, which includes provisions directing the Federal Communications Commission to expand and clarify the prohibition on misleading or spoofed caller ID information.  It also requires that they, in consultation with the Federal Trade Commission, create consumer education materials on how to avoid this type of spoofing.  These provisions were signed into law by the President in March.

This is just one of many steps in the right direction.  But as communication technology continues to advance, so do the tools and tactics of these illegal telemarketers, and they use those tactics and tools to evade existing protections.  So we have to stay ahead of them.

So-called neighbor spoofing is one of the most effective new tactics.  It is particularly hard to detect.  Scammers use phone numbers with your area code and/or an area code nearby, and that gets your trust.  Many consumers are likely to answer when it looks like the call could be coming from, let's say, their child's school, their local church, or their dentist's office.

What do we need to do to stop these bad actors?  As I said earlier, I, for one, am pretty sick and tired of them.

We also finished up another tax season last week.  IRS scammers are going after taxpayers as well.  Using the internet and social media, fraudsters can convincingly portray IRS employees by naming a few identifying facts, like your home address or current city of residence.

To avoid falling prey to these calls and others never give personal identifiable information over the phone.  Government officials will never ask you for your bank account information or Social Security number over the phone.  Consumers should hang up and then they should call the IRS office and check if it was a legitimate call.

And the bad actors keeping evolving.  So we need to make sure that our consumers have what they need to stay ahead of them.  There are a wide array of technical and marketplace solutions consumers can use to block, avoid, or otherwise protect themselves from robocalls or caller ID spoofing.

There are now 500 call-blocking apps for Android, Apple, and other devices.  Many home phone providers offer the option to add robocall-blocking functions to their service for free, and today, because of our witnesses, we will hear from some of these innovators.

And again, we thank you for your work and your willingness to be here.

I have found, too, if I just let it go to voice mail they never leave voice mail, and then I know it is just a spoof.

So anyway, Mr. Chairman, I will yield back the balance of my time.

Thanks for having this hearing.

[The prepared statement of The Chairman follows:]


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

Mr. <u>Latta.</u>  Thank you very much.  The gentleman yields back.

The chair now recognizes the gentleman from Texas for 5 minutes.

Mr. <u>Green.</u>  Thank you, Mr. Chairman.  I will be brief.  I just want to thank you and the ranking member for holding this hearing.

This is one of the biggest complaints I get from senior citizens. And actually at my house, when I go back home after a week, I get calls saying the IRS is going to come over and I owe taxes.  And I hear constituents complain about that, and I explain to them the IRS doesn't call you and tell you by phone.  You will get a letter and keep in touch with us.

The other frustration is that on my cell phone, I haven't applied for a loan for many years, but I keep getting texts saying:  Your $250,000 loan has been approved.  I thought about saying:  Send it to me and I will go to Costa Rica or someplace.

But it is frustrating to seniors, particularly if you are home all day, or young mothers who have children that they are worried about with all these kind of calls.  So we need both the two agencies, the FCC and FTC, see what we can do.  If they don't have the tools for it we need to do it.

And I thank you for having the hearing.

[The prepared statement of Mr. Green follows:]


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

Mr. <u>Latta.</u> Well, thank you very much. The gentleman yields back.

And that will conclude the member opening statements. The chair would like to remind members that, pursuant to committee rules, all members' opening statements will be made part of the record.

And again, I want to thank all of our witnesses for being here with us today, taking the time to testify before the subcommittee. Today's witnesses will have the opportunity to give 5-minute opening statements followed by a round of questions from the members.

Our witness panel for today's hearing includes Mr. Ethan Garr, the chief product officer of RoboKiller; Mr. Aaron Foss, founder of Nomorobo; Ms. Maureen Mahoney, the policy analyst at Consumers Union; and also, Mr. Scott Hambuchen, the executive vice president of technology and solution development at First Orion.

So again, we want to thank you very much for being here.

And, Mr. Garr, you are recognized for 5 minutes. Thank you.

**STATEMENTS OF ETHAN GARR, CHIEF PRODUCT OFFICER, ROBOKILLER; AARON FOSS, FOUNDER, NOMOROBO; MAUREEN MAHONEY, POLICY ANALYST, CONSUMERS UNION; AND SCOTT HAMBUCHEN, EXECUTIVE VICE PRESIDENT-TECHNOLOGY AND SOLUTION DEVELOPMENT, FIRST ORION**

**STATEMENT OF ETHAN GARR**

Mr. Garr.  I think we are going begin with a clip.

[Audio recording played.]

Mr. Garr.  Chairman Latta and members of the committee, I am Ethan Garr from RoboKiller, and what you just heard was one of our Answer Bots wasting a telemarketer's time.

Answer Bots are the solution to the robocall epidemic, and on June 19, 2021, RoboKiller and our Answer Bots will have solved this problem.  See, on that date, at our current trajectory, we will have 10 million users deploying hundreds of millions of our time-wasting Answer Bots.

This will reduce spammers' revenue by more than 50 percent.  That is enough of a disruption to their bottom line to put them out of business.  We are attacking spammers where it hurts, in their wallets.

RoboKiller answers the calls it blocks with these Answer Bots, and they are smart.  They know how to press 1 to reach the human behind Rachel from Cardholder Services.  They know how to turn the tables on spammers and waste their time instead of yours.  This is time that they

no longer have to scam and steal not just from our users, but from anyone else, as well.

This problem has gotten worse despite call-blocking technologies, despite legislation and enforcement.

But we are different. Our call-blocking competitors have approached this problem from the caller ID angle. But spoofing, caller ID blocking, and other tools limit the value of such approaches. It is a cat-and-mouse game that can really never be won. We are not interested in playing the game. We would rather steal the cheese that the spammers are after.

The spammers' business model is based on making billions of calls, knowing that only a small percentage will get answered, and an even smaller percentage of those will connect human telemarketers with viable targets. They don't have to be surgical in their strikes. Robocalls let the most vulnerable in our society self-select themselves as victims.

So a relatively small pool of humans, often on the other side of the world, are just waiting for their auto-dialed robocall systems to connect, waiting for someone's grandmother to press 1 and say "hello."

But Answer Bots' inanimate identities cannot be stolen. Their invisible wallets can't be infiltrated. They can keep spammers wrapped up on calls for hours.

And they are protecting you even if you don't have RoboKiller. Every minute our Answer Bots are engaging telemarketers is a minute they don't have to speak to someone else.

Our competitors are helping their users, but they are also helping scammers.  Telemarketers are happy to skip a well-educated executive with a call-blocker app to get to the elderly grandmother who they know is more likely to fall victim to their scams.  With Answer Bots our users are helping everyone.

Unfortunately, you can't solve this problem with legislation alone.  A three-man IRS scam operation in a seedy, nondescript room in another country isn't worried that the long arm of the American justice system is ever going to knock on their door.

As it became cheaper and cheaper to make calls, the incentive to deploy more robocalls has increased exponentially, as did the incentive to ignore the laws.

The Do Not Call Registry did exactly what it was supposed to do, but, unfortunately, not at all what people expected it to do.  So stopping the tiny percentage of legal robocalls that fell under the Do Not Call list purview was almost no help to consumers who were expecting a panacea.

Beyond the Do Not Call list the government's efforts have been well intentioned and well executed.  They just don't have broad implications on the problem.  Despite the FCC and FTC's well-publicized multimillion dollar enforcement actions, with that estimated $9.5 billion in yearly phone scam revenue these efforts are just not a real deterrent.

No, the real solution to this problem is already in the app store, and it is called RoboKiller.  And you can take pride in the fact that

the government efforts have made this happen.   We weren't in this fight until the FTC had the vision to look beyond legislation and enforcement towards innovation.

When the FTC created the Robocalls:  Humanity Strikes Back competition in 2015 they got us, TelTech, into this fight.  We have been innovating for 14 years, helping consumers use technology to protect their privacy and security on their phones.

From unmasking blocked calls with TrapCall, to recording calls with TapeACall, to helping people keep their numbers secure with SpoofCard, we have always been focused on giving people control of their phones.

The robocall competition ignited our passion and is accomplishing your goals to help Americans end the robocall epidemic.

We have already started to see the impact.  When we heard a telemarketer say in an exasperated voice, "Oh, no, everyone has got RoboKiller today," we knew we had turned the tide.  When we heard another angrily yell at one of our Answer Bots, "Oh, which one are you, the guy with the baby, the guy on the movie set?" then we knew we were winning the fight.

From an adorable Southern belle to a guy dealing with a gazelle running around his apartment, our robots are hilarious, but just as important, they are effective.

Earlier this week we were able to showcase RoboKiller and Answer Bots at the FTC and FCC's joint technology expo, and today we have the privilege of testifying in front of this subcommittee.  If you want

us to help you solve this problem, please do more of this.  Help us get more attention so that we can speed up our growth.

We are not worried about putting ourselves out of business by solving the problem.  We have built a culture of innovation.  So when the scammers start ringing doorbells after we have solved this problem we will have a solution for that, too.

Answer Bots wasted more than 25,000 hours of human telemarketers' time last month.  For 150,000 users that represented hundreds of thousands of blocked calls and the peace of mind that when their phone rang it wasn't a harassing call from a scammer.  For thousands of other Americans who have yet to purchase RoboKiller, that was 25,000 hours where they, too, were protected from those otherwise engaged telemarketers.

This robocall problem has grown into a true epidemic.  Ever since I have been speaking, 2,700 unwanted calls are being made to American citizens every second.  But it is over.  RoboKiller and our Answer Bots are on the case.

Thank you very much.

[The prepared statement of Mr. Garr follows:]


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

Mr. <u>Latta.</u>  Thank you very much for your testimony today.

And, Mr. Foss, you are recognized for 5 minutes.  Thank you.


**STATEMENT OF AARON FOSS**


Mr. <u>Foss.</u>  Chairman Latta, Ranking Member Pallone, and members of the committee, thank you for giving me the opportunity to appear before you today.

My name is Aaron Foss.  I am the founder of Nomorobo and the winner of the FTC Robocall Challenge.

And since launching in 2013, Nomorobo has stopped almost 650 million robocalls from reaching American citizens.  And while that number is huge, it is a mere drop in the bucket of this problem. According to our data, approximately 40 percent of all calls on a landline network are unwanted robocalls.

So I am here today to give you a view from the trenches.  And let me start off by telling you the good news.  The same technology that created this problem, low-cost Voice over IP service, is now being used to successfully stop it.

In its first year Nomorobo stopped 15 million robocalls from reaching American consumers.  That was in the entire first year.  And we are now stopping double that amount every single month.  Thirty million robocalls a month are being stopped by Nomorobo.  And this is much better than the old solution of, "Only answer numbers that you recognize."

And when I first started this crusade carriers believed that FCC regulations prohibited them from blocking robocalls.  But since the FCC clarified that those regulations do indeed allow robocall blocking, carriers have been quick to act.  Today Nomorobo is supported by most of the major VoIP carriers in the United States and directly integrated with some of the largest.

And mobile technology companies, like Apple and Google, have also done a great job in making their smartphone ecosystems robocall-blocker friendly.  They now allow developers to create and distribute robocall-blocking apps to hundreds of millions of users.  This wasn't always the case, especially when I started.

And there used to be a lot of fear when it came to stopping robocalls.  Many people thought that technology couldn't differentiate between good and bad robocalls.  And Nomorobo proved this incorrect.  The service is 97 percent effective, and our false positive rate is only one-tenth of 1 percent.

So on the one hand I know that for over 1.6 million Nomorobo users we have solved their robocall problem once and for all.  Their phones are now peaceful and quiet.  And I wish I could stop my testimony right there and we could end the conversation right now.

Unfortunately, I can't.  It is a jungle out there, and the robocallers have started to use more advanced tricks and tactics.  We have to continually stay one step ahead of the bad guys.  Simple blacklists are no longer as effective in stopping robocalls as they once are.

Last summer we noticed an explosion in neighbor spoofed calls. These are the calls where the robocall caller uses a fake number that looks very similar to the recipient's number. Last summer they used to represent less than 2 percent of all robocalls, but beginning in July of 2017 they represented almost 20 percent of all robocalls. That is a 10X increase.

Now, luckily, technology like Nomorobo can quickly detect and stop new robocalling patterns like neighbor spoofing. And while the carriers are also working on a solution, verifying and certifying caller ID, it is still years away.

Robocallers are flexible and quickly and continually change their tactics. The tools to fight them also have to be flexible and adaptable.

We are at a very interesting point in the robocall battle. Technology has proven that it is the safe and effective solution in the fight. Regulators have cleared the path for carriers to roll out robocall-blocking solutions to their customers. Consumers have shown that they want these services, they trust these services, and are even willing to pay for these services.

And robocall blocking is a virtuous cycle. The more people that use robocall blockers, the less effective robocalling becomes. The less effective robocalling becomes, the less robocalls are made. Everyone wins, except for the robocallers.

And to close, I just want to remind everyone why we are solving this problem. This isn't just about stopping a minor annoyance.

Robocalls present a significant threat, particularly to some of our most vulnerable citizens.

I was reminded of this the other day when I received the following email.  As everybody knows, my testimony is sworn so I am really not making this up.

It said:  "My name is Phil.  I just wanted you to know how thankful I am for your service.   I have a bad brain injury and the calls I was getting fooled me.   Thank you for offering the service for free. My income has been tough to manage, and adding an extra cost, even small, can add up each month."

I thank the committee for continuing to do everything in its power to make robocall-blocking solutions, like Nomorobo, available to all Americans.

[The prepared statement of Mr. Foss follows:]


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

Mr. <u>Latta.</u>  Well, thank you for your testimony.

And, Ms. Mahoney, you are recognized for 5 minutes.

**STATEMENT OF MAUREEN MAHONEY**

Ms. <u>Mahoney.</u>  Chairman Latta, members of the subcommittee, thank you for the opportunity to speak today.  I work for Consumers Union, the advocacy division of Consumer Reports.

Since 2015, in response to complaints from thousands of consumers who told us that robocalls were their top consumer complaint, we have conducted our End Robocalls campaign, which calls on the major phone companies to offer to all of their customers free, effective tools to block unwanted robocalls.

Nearly three-quarters of a million people have signed this petition, and they have told us that they are overwhelmed by the harmful, abusive, and irritating robocalls that intrude on their privacy, take their money, and allow scams to enter their homes.

Robocalls have reached epidemic proportions.  Since 2006 the number of complaints to the FTC about violations of the Do Not Call list has exploded.  And the volume of robocalls is on the rise, as well.  Last month, 3 billion robocalls were placed to consumers in the United States.

Unwanted calls undermine the quality of the phone service for which consumers pay dealer.  For example, sometimes these robocalling campaigns relentlessly target certain consumers.  One consumer told

us that she received an estimated 100 calls in a single day, which blocked incoming and outgoing calls for significant periods of time. Others have told us that unwanted incoming robocalls have delayed them from calling a medical professional.

And robocalls cost consumers money.  Vulnerable consumers, such as the elderly, may be unduly susceptible to telemarketing pitches for products that they don't want or need.  Scam calls like Rachel from Card Services also seek to separate consumers from their money fraudulently.

Consumers with prepaid or limited-minute calling plans may end up paying for robocalls.  And often consumers have to pay for call-blocking devices or services, which further push the costs of robocalls onto consumers.

We appreciate the progress that the phone companies, the FCC, and the FTC have made thus far in addressing robocalls.  For example, AT&T and T-Mobile have begun to offer free robocall-blocking tools to their customers.

In addition, the FCC has approved new rules that give phone companies the leeway to immediately block certain clearly illegally spoofed calls that they see coming through their networks.  They have also opened an inquiry into the development of caller ID authentication technology to address call spoofing.  And the FTC has initiated a series of contests, as my copanelists well know, to encourage developers to create and innovate antirobocall technology.

But more action is needed to fully address the robocall problem.

The blocking under the FCC's new rules will not reach the vast majority of robocalls. Essential legal protections against robocalls under the Telephone Consumer Protection Act, or the TCPA, remain at risk. And enforcement efforts have not been enough to stop illegal robocalling. Therefore, we support the following additional reforms.

First, the FCC should require providers to offer technology to identify and block spoofed and unwanted calls. Congress can assist by supporting the ROBOCOP Act, which would direct the FCC to develop rules to implement these technologies.

Second, ensure that consumers have strong legal protections against unwanted calls. The D.C. Circuit Court of Appeals recently struck down portions of the FCC's 2015 rules covering the definition of an autodialer and the safe harbor for robocalls made to reassigned numbers. The FCC will likely open a proceeding to explore open issues related to the definition of an autodialer, and we urge them to implement rules that maintain important protections against unwanted robocalls so that consumers have a means of controlling or stopping them.

Third, increase protections against unwanted debt collection calls. Congress should pass the HANGUP Act to remove the exemption placed in the TCPA for Federal debt collection robocalls. While the exemption should never have been passed in the first place, we urge the FCC to issue rules to implement the provision to provide clarity and to ensure that consumers have a way to limit and stop these calls.

And finally, empower the FTC to counter illegal calls. Congress

should allocate to the FTC greater resources for enforcement and the development of antirobocall technology.  It should also remove the common carrier exemption in the FTC Act so that the FTC can directly call on phone service providers to be part of the solution.

Thank you for your attention to this important consumer issue, and I look forward to addressing any questions you have.

[The prepared statement of Ms. Mahoney follows:]


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

Mr. Latta.  Thank you.

And, Mr. Hambuchen, you are recognized for 5 minutes.


**STATEMENT OF SCOTT HAMBUCHEN**


Mr. Hambuchen.  Chairman Latta, members of the subcommittee, thank you for giving me the opportunity to appear today.  I am Scott Hambuchen, an executive with First Orion Corporation.

Today consumers are being scammed out of hundreds of millions of dollars and are now conditioned to not answer the phone unless they know who is calling.  This lack of trust in the voice channel must change.

First Orion partners with carriers to offer their subscribers protection from scams and unwanted calls.  First Orion also offers consumers mobile apps, such as PrivacyStar, to protect their cell phones from these calls.  These offerings use sophisticated analytics to identify calls that are highly likely to be scams.

First Orion analyzed over 34 billion calls this past year and labeled 3.5 billion of them Scam Likely, giving consumers a warning before they answer.  In addition, consumers can opt in to blocking calls labeled Scam Likely so their phone never rings.  In 2017 we blocked over 500 million of these calls for consumers.

Most of the larger carriers have launched some form of scam protection.  First Orion is the chosen provider for T-Mobile's groundbreaking offering last year, deploying our Scam Likely solution

to over 58 million subscribers for free.  We also know there are over 500 apps in the Google Play and Apple App Stores that are free or available for a small month monthly charge.

Despite these efforts, we are still getting fraudulent and unwanted calls.  The fraudsters are sophisticated, evolving their practices to avoid being labeled and blocked.  They operate like a business and constantly change their tactics to appear legitimate.

Scammers use methods that legitimate callers often use, such as prerecorded messages, automated robocalls, and altering their caller ID, commonly referred to as spoofing.

Some robocalls are legitimate and wanted, such as automated notices from your child's school.  And yet some scams are not robocalls.  Both are still growing.

Spoofing is no different.  Legal spoofing by a national pharmacy chain letting customers know their prescription is ready and spoofing the number for the local pharmacy is helpful.  However, neighbor spoofing, inserting a random number with the same area code and prefix as the called number to get a consumer to answer a scam call, is illegal and much harder to detect.

Let me be clear.  We are in an arms race, not a marathon with a finish line, at least until we make it unprofitable.  Our approach provides consumers the best information available -- who is calling and why -- allowing consumers to decide if they should answer.

We also allow consumers to block future calls from that number or call category.  We offer more information, including a calling

number, the company name if available, the call category, and the ability to file complaints that we send to the FTC.

We take great care in applying labels using sophisticated algorithms based on calls we see, input from consumers, and many other sources of intelligence. No one piece of data ever generates a Scam Likely label.

Our labeling methods are constantly evolving to respond to new threats. In response to neighbor spoofing, we have evolved our analytics to soon start identifying individual calls, not just the calling number, as Scam Likely. As a result, we expect the number of identified scam calls to rise from 12 percent today to 15 percent.

Of course, any algorithmic approach has some errors. Reported cases of false positives are a fraction of 1 percent for us. So calling parties can easily fix an incorrect label, we launched CallTransparency.com, a website that provides legitimate callers the opportunity to register their numbers and avoid the Scam Likely tag.

The FCC has wisely established a light touch regulatory regime that allows continued development of call labeling and blocking solutions, with the potential for profound consumer benefits. We also commend the multiyear FTC focus on these issues and their role with complex multiagency enforcement actions.

Finally, we will continue working with call originators to further enhance our solutions, although we do oppose any regulation or industry efforts that may help scammers, such as call block indicator tones.

To conclude, the one area where First Orion believes that industry and government can do more together is expanding consumer education about scam calls and what tools are available to them.

Mr. Chairman, First Orion appreciates the opportunity to appear today.  We are available to provide any additional information the committee may request.  Thank you.

[The prepared statement of Mr. Hambuchen follows:]


******** INSERT 1-4 ********

Mr. Latta. I want to thank all of our witnesses for being with us today. We really appreciate the information.

And that will conclude our witness opening statements, and we will move onto the 5-minute questions from our members, and I will recognize myself for 5 minutes.

Mr. Foss, since you won the FTC Robocall Challenge, what are the challenges your company has experienced in getting Nomorobo developed and installed on landline and mobile phones?

Mr. Foss. So I think that the major challenge that we had has changed. So when we first started off it was absolutely the carrier integration problem. That seems to be thawing.

What the major problem I think right now is, is on the customer, the consumer confusion side. I even hear this mentioned a lot now where people say to put your landline and your mobile number on the Do Not Call list.

There is actually no point in putting your mobile number on the Do Not Call list. The way the TCPA is written, it is actually illegal to call mobile phones unless you have expressed written permission.

So when I actually even hear things like, "Well, you know, my number is on the Do Not Call list, why do I keep getting calls?" or when people say, "Well, put your mobile and your landline on the Do Not Call list," then what are you going to do there? I feel like it is very, very confusing right now.

I think the biggest problem with the adoption of these things is that consumers don't really understand. If they understood that there

were these technologies that are available, if they understood where the government steps in and know what it can do to help, I think that that would go a long way now.

Mr. <u>Latta.</u>  And going along with that then, where have you received support and encouragement in that mission to protect your consumers?  Where has that support been?

Mr. <u>Foss.</u>  From the consumers themselves.  And maybe it is just like, you know, an American trait.  We have a great military.  We have great police.  And people still protect themselves in their own homes through various means.  They have firearms.  They have security systems.  Americans do take protecting themselves as a responsibility.

So I think that the easiest place that we have been able to find it, when consumers understand that they can go and protect themselves, that they don't have to rely on the government, that they don't have to rely on the carriers, that really empowers consumers to protect their lines.

Mr. <u>Latta.</u>  Thank you.

Mr. Garr, as a winner yourself, can you share the challenges and support for the RoboKiller company's experience since the FTC contest?

Mr. <u>Garr.</u>  Sure.  I also would say that we have gotten incredible support from consumers.

People are really angry about this problem.  My uncle calls me up probably once every 2 months and screams about the robocalls and telemarketers he is dealing with.

Consumers are passionate about solving this problem.  So we see,

especially in ratings and reviews, that customers are really passionate about what we are doing.  They want us to succeed and make their lives better.

Certainly the challenges are that scammers are constantly working at this problem, too.  So more randomness, new technologies, that is always a challenge.

We are always getting a lot of support from the FTC and the FCC. Since we won the competition we are really fortunate to be really partnered with these agencies.  Again, being invited to speak today, having the chance to go to the technology expo on Monday, these are really important to our growth.

We really feel like we have a solution in RoboKiller and our Answer Bots that scales.  The only way it scales is if we get the word out there, and being able to participate in things like this has really been a supportive part of the effort.

Mr. Latta.  Let me ask this, if I could ask everyone real quickly, because I don't have a lot of time.  But what can be done to stimulate more technological solutions and marketplace innovations to help consumers fight back against robocalls and spoofing?

Maybe, Mr. Hambuchen, we can start with you and just work back down real quick.

Mr. Hambuchen.  Thank you, Mr. Chairman.

Well, we certainly think awareness with consumers is a big part of that.  The more complaints they file, the more data we have, the more we will be able to combat this.

As you know, our business, we look at labeling and giving consumers choice in blocking these calls, and so the more information we have, the more we can fight the scammers.

Because what you have to realize is these scammers are very sophisticated. They are using data and technology today much like a marketer, a direct marketer would to target these individuals. And so to combat that we need more data, more sophistication, and more analytics deployed in the carrier networks to detect that.

Mr. Latta. Ms. Mahoney, I have got about 40 seconds left.

Ms. Mahoney. Thank you.

We think the FCC should require the phone companies to implement advanced call-blocking technology. I think that will provide important incentives for perfecting and improving it. And we also commend the FTC for its efforts so far to spread this technology, and we think they should be allocated more funds to be able to continue these efforts.

Mr. Latta. Thank you.

Mr. Foss, I have 17 seconds.

Mr. Foss. I will go with educate, education, making consumers aware of what is out there and showing them that it is a real solution.

Mr. Latta. Thank you.

Mr. Garr.

Mr. Garr. In my very short time here, real time information is always useful. We can always use that to be more effective in deploying our Answer Bots for the consumers.

Mr. <u>Latta.</u>  Thank you very much.

My time has expired, and I recognize the gentlelady from Michigan for 5 minutes.

Mrs. <u>Dingell.</u>  Thank you, Mr. Chairman.

Ms. Mahoney, I would like to explore some of your testimony regarding the FTC's authority under the Telemarketing Sales Rule to stop these illegal robocalls.

I am concerned by reports that there are a handful of small Voice over Internet Protocol, VoIP, services that are enabling these calls.

During the Senate hearing on this same topic last week we learned that these small VoIP carriers openly advertise short-duration calls, which is code for robocalls.  They even offered to blend robocall traffic in with normal calls to avoid detection.

Ms. Mahoney, are these VoIP services contributing to the proliferation of robocalls?

Ms. <u>Mahoney.</u>  Thank you for your question.

Again, we commend the FTC for its work so far on the robocall issue, their enforcement efforts in particular.  But we did learn last week from the Senate hearing that there are carriers wherein their primary line of business is to carry this fraudulent traffic.

I think if the FTC had more authority to go after them, they could use their enforcement muscle to really help crack down on this illegal activity.

Mrs. <u>Dingell.</u>  Thank you.

Do you think that going after the carriers that aid and abet

illegal robocallers would help reduce the number of unwanted callers?

Ms. <u>Mahoney.</u>  I do.

Mrs. <u>Dingell.</u>  I certainly think that shutting these operations down would be an effective enforcement tactic, but when it comes to these unscrupulous VoIP carriers the FTC says its hands are tied because common carrier activities are exempt from the FTC Act.

Today we are releasing a draft bill that would lift that exemption for FTC enforcement against illegal telemarketing and robocalls, something that the FTC has testified that they support in the past.

Does Consumer Union support expanding the FTC's authority under the Telemarketing Sales Rule to reach common carriers?

Ms. <u>Mahoney.</u>  We do.  We think this is a good idea and will help the FTC crack down on this illegal activity.

Mrs. <u>Dingell.</u>  In 1990 Congress passed the Do Not Call Registry after hearing numerous complaints about unwanted calls.  That law worked for a while, but one quick glance at your call history shows it is clearly not working anymore, and all of you have testified making that clear, too, that we need to do something.

Ms. Mahoney, do you agree that existing law is insufficient and more can be done here in Congress to help consumers rid themselves of these unwanted calls?

Ms. <u>Mahoney.</u>  Yes.  We have long been calling on the phone companies to offer free, effective antirobocall blocking technology. We do think the FCC should require the phone companies to offer this technology so that all consumers are covered.  For example, consumers

with traditional landline phones do not have effective, free protections against these robocalls.

So those are the important reforms that we would support.

Mrs. Dingell. Thank you.

And I yield back the remainder of my time, Mr. Chairman.

Mr. Latta. Thank you very much. The gentlelady yields back.

And the chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

The Chairman. Thank you very much, Mr. Chairman.

I was actually just trying to download one of your apps here. I am real ready to do this.

Look, I think we are all really frustrated. We now know that the Do Not Call Registry isn't that effective because these people are operating illegally to begin with. We have been through TCPA issues. It is already illegal to robocall a cell phone.

And it seems to me that technology holds the best promise here, because we can make some changes in statute probably, but at the end of the day isn't it really you all and your brain trust that are going to come up with the technology every day to try and stay ahead of the spoofers every day because they got people doing this, right?

Do you want to address that? I mean, what is the best thing a consumer can do? And what should we do to get at this?

Mr. Garr. We passionately believe that disruption of the telemarketers' business is the key to solving this problem. We believe that our Answer Bots, which wastes scammers time --

The <u>Chairman.</u>  Love it.

Mr. <u>Garr.</u>  -- can solve this problem.

Yes, they are entertaining, yes, they are fun, yes, you can create your own.  These are great things for consumers.  But they serve a really important, valuable purpose.  That, again, is time.

Not just that our user is protected.  If you are downloading RoboKiller right now, yes, you will be protected from that call, but the great thing is that somebody else is being protected at the same time because the calls that we are blocking and answering with our Answer Bots are wasting those spammers' time.  And I am telling you, sometimes it is for 47 minutes at a time.

The <u>Chairman.</u>  See, I really like that, because I want to get even with these people.

I remember a decade or so ago when pop-up ads were the rage on the internet.  Every time I would work on a Word document or something, you have these pop-up ads.  I threatened to do a death penalty for pop-up ad people, because, I mean, you couldn't get anything done.  And now we are all getting interrupted with these calls.

By the way, I have just downloaded your app.  I may move down the table here.  But I am going to be in the "get even" mode here real soon with these scammers.

Mr. <u>Garr.</u>  We are the "get even" guys.

The <u>Chairman.</u>  I like that a lot, because I think that is what you have to do, is create economic harm on them.  Because it is hard to chase them around the globe, right?

So when I get one of these calls, I have tried to like talk to them, and they are really sweet except they don't answer, it is a robovoice for a while. So what happens? Does somebody actually answer? And what are they really after, just my financial information?

Mr. Garr. It really depends on the nature of the call. And, again, like what is really incredible is how effective they can be at reaching their victims.

That IRS scam that was played at the beginning of this testimony, that particular robocall asks you to call back a specific phone number. That means when you call them back you are self-selecting yourself as a victim.

They don't want people who have RoboKiller. They don't want people who have another product. They want to get past them and get to the human being.

The Chairman. So they have a sweatshop caller center overseas most likely. Most of this is going on overseas, right?

Mr. Garr. They are not a monolith. I mean, I speak to a lot of scammers. I mean, you would think it is full-time job for me.

The Chairman. Is this your voice on one of these?

Mr. Garr. The one we played was my voice, yes.

We talk to a lot of these scammers. It is not one, there is not one image of them. It is three guys working together in disparate locations. It is a bullpen of 100 people.

I ask them, "How many people are in your room?" And sometimes you get, "Oh, there is just me. It is just me." And sometimes you

can hear people in the background.  Sometimes you can tell it is a big

bullpen.

The <u>Chairman.</u>  Stunning they are not truthful to you.

Mr. <u>Garr.</u>  Yes, exactly.  We really encourage consumers not to

trust anything the spammers say or do.  Don't press 1 to get off their

list because why would you trust someone who is out to get you in the

first place?

The <u>Chairman.</u>  Right.  I was going to ask you that, because they

do have, like, press 1 if you want off, you do this or that.  Bottom

line is you should just hang up, right, or, no, do your deal.

Mr. <u>Garr.</u>  Yeah.  If you have RoboKiller we will take care of it

for you.  But, yes, I think if you are going to engage never give out

personal identifying information.

The <u>Chairman.</u>  And so when somebody is using, let's just say, your

app, I am trying not to hawk one service over another here, but let's

say they use your app.  Is that counting against their phone minutes

or anything like that?  Our phone minutes, I mean the consumers.

Mr. <u>Garr.</u>  For our users?  No.

The <u>Chairman.</u>  So it is not tying up my phone line?

Mr. <u>Garr.</u>  No, no, no.  The call is being forwarded to us, and

then we are answering that call.  So the user is just getting a

notification on their phone saying RoboKiller has blocked this call,

that it is a spam call.

The <u>Chairman.</u>  And how do you know that it is not a real call?

Mr. <u>Garr.</u>  That is our special sauce.  We are using a lot of

tools.  When we won the FTC's competition, we demonstrated how audio

fingerprinting could be used to attack this problem.  That is one of

the tools we use, along with machine learning, lists that we find and

build, using our own consumer's consumer information.  As we grow we

are building a larger and larger ecosystem to learn from.

The <u>Chairman.</u>  Okay.  My time has expired.  But thank you all for

the good work you are doing.  This is what it is going to take.  And

I am all about getting even with these people.

Thank you.

Mr. <u>Latta.</u>  Thank you very much.  The gentleman's time has

expired.

And the chair now recognizes the gentleman from Texas for

5 minutes.

Mr. <u>Green.</u>  Thank you, Mr. Chairman, again, for holding this

hearing.

Ms. Mahoney, I appreciate the work Consumers Union does trying

to make America aware of options they do have to protect.  I am

especially concerned about protecting those more vulnerable to fraud.

Do you think the elderly specifically are likely to know about

the apps and the technologies that exist to protect them from robocalls?

Ms. <u>Mahoney.</u>  We think more consumers should be made aware of some

of the options that are out there.  We would like to see consumers

taking more advantage of them.

Oftentimes elderly consumers do have traditional landline

phones, and existing call-blocking solutions are not adequate for those

types of phone service.

So we would like to see more technologies that are available to them, as well as more education and awareness for these consumers to be able to take advantage of existing tools.

Mr. Green.  Several witnesses have mentioned that AT&T and T-Mobile have begun offering free robocall-blocking tools to at least to some of their customers, and I am glad to hear, especially since you also mentioned that some of the competitors only provide products that consumers have to pay for.

How can we explain why only some of their customers have access to these tools and not all their customers?

Ms. Mahoney.  Thank you for your question.

Again, we think that all consumers should have access to these tools, and we do think the FCC should require the phone companies to offer to all of their customers these tools.

I think it is possible that phone companies in the short-term do not see market incentives for providing these solutions to all of their customers.  So that is why we would like to see more pressure on them to take action.

Mr. Green.  Mr. Hambuchen, in your testimony you mentioned there are over 400 apps available to consumers that offer robocall and spoofing protection.  Since these apps are so widely available, what do you think are the biggest obstacles to better protection from robocalls for these consumers that are particularly vulnerable to scammers?

Mr. <u>Hambuchen.</u>  Thank you for your question, Congressman.

One of the largest issues is that the scammers are very savvy, very technologically savvy, and so a lot of these apps work based off of just a list of numbers that are going to be blocked or identified. And so that takes time to compile that information.

What the scammers have learned is that rotating that number or these neighbor spoofing-type solutions they can avoid those simple lists of numbers that should be blocked.

And so part of what First Orion is doing is developing technology that allows us to rapidly look at all that information and instead of just looking at the number, looking at the characteristics of the incoming call and identifying that information so that, regardless of what number that scammer may call from, we can identify that information and block that call or label it as a scam.

Mr. <u>Green.</u>  Of these 500 apps that are available, what kinds of options are available to customers that don't have a smartphone?

Mr. <u>Hambuchen.</u>  Well, that is a tough one.  Most of the apps are really for the Google Play Store for Android devices, the Apple App Store, which are iOS devices, maybe a handful for Windows smartphones. But for the feature phone you really have to rely on the carriers' in-network solution for any of that scam protection.

Mr. <u>Green.</u>  Thank you, Mr. Chairman.  I yield back.

Mr. <u>Latta.</u>  Thank you.  The gentleman yields back.

The chair now recognizes the gentleman from Illinois, the vice chairman of the subcommittee.

Mr. Kinzinger.   Thank you, Mr. Chairman.

And thank you all for being here.   It is good to have you here on this really important issue.

I just downloaded one of your apps, as well.   And I have been getting calls all the time, and I just don't even answer my phone anymore.   So I am eager to get a call and listen to the exchange if it happens.

But all of you, I appreciate you being here, and we will start out with Mr. Hambuchen.

What is about the distributed -- you answered a little bit of this, but I want to see if there is anything you missed out on that -- what is it about the distributed interconnected nature of the internet that allows bad actors to provision cheap and easy robocalls over VoIP? What is it just about nature of it, I guess.

Mr. Hambuchen.   Well, I think the distributed nature, what you just described, the internet is connected, right, all of it is connected.

So what has happened is the cost for any company to be able to create and launch call campaigns off the internet connected to the carrier networks, the cost of that has come down so dramatically over the last couple of years it makes it very easy for scammers to launch millions of calls at very low cost.   And it has also helped the legitimate businesses also reach their customers with legitimate services.

So again, I think what we have got to do is find ways to look at

that data, analyze that information, and apply it back into the carrier network.

Mr. Kinzinger.  Let me ask, so the internet itself obviously is old relatively, but it seems like these calls have been increasing really in the last few months, maybe the last year, exponentially.  Did something change or did they just figure something out?

Mr. Hambuchen.  I think as the solutions are deployed and starting to stop some of the calls, so you have heard from all of us the number of calls that we have been able to block or deter, again, the scammers are able to increase their volume.  So they are going to get their number of calls out there whatever it takes to hit their number of scams.

Mr. Kinzinger.  And to all the industry representatives, when a customer downloads your app, has your service added to their landline, what is their typical experience in the next few days and weeks, zero robocalls, 90 percent reduction?

Mr. Garr, if you want to start.

Mr. Garr.  We expect our customers to see more than 90 percent reduction in standard telemarketing calls.

Mr. Kinzinger.  That is awesome.

Mr. Foss.  We don't get any of the data back on the mobile side, there is a privacy issue over there, so I can't tell you the exact number.

But what I will tell you is from the very moment that you install Nomorobo and if you go back to your recent call lists and we start

labeling all those as robocallers, people will be like: Wow, I knew that that is what that was. So from the very, very moment they get a visceral feedback that it is working.

Mr. <u>Hambuchen.</u> About 12 percent of the calls that come to our consumers are labeled Scam Likely.

Mr. <u>Kinzinger.</u> Okay.

Mr. Foss, are you aware of robocallers spoofing the telephone numbers of fire department, EMS, police, sheriff, anything like that?

Mr. <u>Foss.</u> Yes. So the spoofing known and good robocallers, even on our -- like if there is something on a white list or something, does happen.

According to our data it is very, very small, and that attack is actually relatively easy to prevent. So, for instance, with our blacklist solution, when an attack is actually going on, that number is on our blacklist. When the attack stops it can be rolled off.

And as we get integrated with more and more carriers and things we can give those analytics back, and we can tell those public safety organizations: Hey, your numbers are being spoofed, switch on over to see it, something like that.

One of the new techniques that literally just started this week, though, it actually happened, it was attacking some people in Texas and California and New York, and it was aimed at Chinese Americans.

And they were using a variation on neighbor spoofing. They would call from a 212-244 number, which is where the Chinese consulate was. The message was in Mandarin. And when we started detecting this we

couldn't understand -- because the messages, again, were all in Mandarin -- we couldn't understand what was going on.

When we looked at the analytics and we looked at the area codes and the exchanges that this robocaller was targeting, it was absolutely places with high Asian populations.

One of the ones that popped up was Webster, Texas.  Like, I don't understand.  It was San Francisco, New York, those kinds of things, and then Webster, Texas.  When you go and look at the demographic makeup of Webster, Texas, it is predominantly Asian.

So these spoofing issues, yes, can they go and spoof real numbers like the Chinese consulate, like the public safety organizations? Yes.

But more importantly, it is much more important to stop them as they are happening in real time, report that back.  That is a solvable problem.

Mr. Kinzinger.  Thank you.

Mr. Garr, in 10 seconds do you have anything to add to that?

Mr. Garr.  I would just say that generally the bigger spammers, the cruise scams and things like that, are not using these highly targeted attacks.  It is less surgical.  They don't need to do that.

What they want to do is, again, they want to get past the people who are savvy enough to have call-blocking apps and services and get to the people who are vulnerable.  So they just want to make more and more calls.

And that is why we feel that time is such an important factor here.

We have to be hitting them where it hurts, which is in their wallet, and their wallet is connected directly to time.   And that is how Answer Bots fight that problem.

Mr. <u>Kinzinger.</u>  All right.  Thank you all for being here.

Mr. Chairman, I yield back.

[10:03 a.m.]

Mr. Latta.  Thank you very much.

The chair now recognizes the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

Ms. Schakowsky.  Thank you.

First, let me apologize.  I had another meeting I had to be at, and so I am sorry that I didn't hear your testimony.  I appreciate the written testimony that I have, though.

And I have heard horror stories about debt collectors taking advantage of robocall technology, harassing consumers, often several calls a day to a single recipient, hundreds of calls a month, even after the recipient has asked that the calls stop.

And, unfortunately, in 2015 Congress actually made it even easier for some debt collectors to harass consumers by allowing calls to be placed to a person's cell phone without the prior consent required for other robocalls.

So let me ask Ms. Mahoney, can you elaborate for us on what you are hearing from consumers about harassment by debt collectors?  And does debt collection make up a substantial portion of all robocalls.

Ms. Mahoney.  Thank you for your question.

We have had a similar experience.  We have heard from many consumers about unrelenting, harassing debt collection robocalls.

And oftentimes they are intended for another person.  It is very difficult to get these calls to stop because the caller does not believe that the consumer doesn't owe the debt.

We heard from one consumer who is on a fixed income, has a limited-minute cell phone plan.  She is constantly receiving unwanted debt collection robocalls that are intended for someone else and can't get them to stop.  So she is very frustrated that she is essentially paying for these robocalls.

And there are a couple of reasons why there are so many of these debt collection robocalls.  I think there are strong incentives because of the inexpensive cost of sending out these messages for debt collectors to reach out to consumers.

Also, as you note, exemption to the TCPA was slipped into the budget bill of 2015 that exempted debt collection robocalls made on behalf of the Federal Government.  For example, to collect Federal student loan debt or tax debt.

This was very unpopular when it passed.  Nearly 200,000 Consumers Union activists reached out to the FCC to ask them to implement strong rules in order to limit them.

So we don't think this provision should have been passed in the first place.  We do think it should be removed, for example, through the HANGUP Act.

But in the meantime, the FCC has yet to finalize rules implementing this provision, and we do urge them to do so, so that there is some clarity around the issue and that consumers know how to stop

these calls.

Ms. Schakowsky. Thank you. I would agree with that. I don't see why any debt collector, even for a Federal-backed loan, should be given free rein to harass consumers.

In 2016 the Federal Communications Commission voted to adopt protections that would have established guardrails on these calls to limit their abuse, but those rules never went into effect.

So, Ms. Mahoney, can you explain the status of those rules? And do you support them being allowed to go into effect? Is that what you were referring to earlier? The FCC. Okay.

Ms. Mahoney. Right. Exactly.

So in the summer of 2016, the FCC did issue strong rules that would limit the amount of these debt collection robocalls that would be allowed to be sent to consumers without their consent, and also provided them the opportunity to stop these calls if they wanted to. Without these rules, consumers wouldn't have the ability to do so.

However, those rules went to the OMB before they could go into effect, and in January 2017 they were withdrawn from consideration by the FCC.

Ms. Schakowsky. They were what?

Ms. Mahoney. Withdrawn.

Ms. Schakowsky. What did you say about consideration? They were dropped from?

Ms. Mahoney. I believe they were withdrawn by the FCC.

Ms. Schakowsky. Withdrawn. Oh, okay.

So you testified the Consumers Union supports a bill that would once again require Federal debt collectors to comply with the same rules as any other robocaller. Congresswoman Anna Eshoo is reintroducing the HANGUP Act, which you referred to, here in the House.

Until we pass legislation like the HANGUP Act, what are the minimum protections that you would want to see in place to stop abusive practices?

Ms. Mahoney. Right. So until these rules are implemented, actually that provision does not go into effect. However, there is a lack of clarity around the issue, so we are concerned that consumers will still get these unwanted robocalls from Federal debt collectors.

We would like to see rules issued in the meantime so that consumers have additional protections against them. We would like to see that provision reversed. And we would like consumers to have the opportunity to block all unwanted calls through the expansion of technology that is available to them to do so.

Ms. Schakowsky. All right. Thank you. And I yield back.

Mr. Latta. Thank you. The gentlelady yields back.

The chair now recognizes the gentleman from Florida for 5 minutes.

Mr. Bilirakis. Thank you, Mr. Chair. Thank you for holding this hearing as well.

And I thank the panel for their testimony. This is a very important issue. It affects our constituents.

Mr. Garr, you mentioned that your technology does not -- the

constituent or the customer, the person does not have to answer the phone.  In other words, it does not affect them, it doesn't interrupt them at all.  In other words, they just see on the caller ID that a call was made and you interrupt the call.  Is that correct?

Mr. Garr.  Yes, we block the call.

Mr. Bilirakis.  You block the call.

Mr. Garr.  And then answer it with our Answer Bots.

Mr. Bilirakis.  So no inconvenience for the constituent?

Mr. Garr.  No.  And all we do is we show them a notification on their phone so that they know that a call was received and that we blocked it.

Our job is to give users control of their phone.  I think what you are all talking about when you say, "I don't even pick up my phone anymore, you know, we unplugged our landline," when you hear those stories, people are saying they have lost control of their phone.

Our job, what we are passionate about at TelTech with RoboKiller, is making sure people have control of their phone once again.

Mr. Bilirakis.  And that is so very important because a lot of times when you have an elderly parent you want to make sure you pick up the phone.  You never know, it is an emergency, it could be.  I mean, even with a mobile phone, I see robocall, but I identify, I see the number, and I know it is somebody that I know.  So a lot of times I will pick up the phone.

Mr. Garr.  Absolutely.  I mean, one of our pioneering technologies is a product called TrapCall, which unmasks blocked calls,

which is a problem that is still prevalent today, but was a huge deal 8, 9 years ago, it was all over the news. When people were getting blocked calls, it was really important for them to know who was calling from behind those blocked calls.

We wanted to find a way to give people back that control of their phone without disrupting their whole life, without changing the way they interact with their phones.

Mr. Bilirakis. Yeah. And for the rest of the panel, is that correct? I mean, all this other technology, which is great, and thank you for continuing to innovate until we solve this terrible problem. You are not interrupting the consumer in any way? In other words, the phone doesn't ring during dinner or during your favorite program, is that correct, as well?

Mr. Foss. Correct. So on our landline product, the phone will ring once and then we answer it. It stops ringing, they will see the caller ID, so people can make sure that they know that it is working.

On our mobile product, we give consumers the option, do they want to identify it as a robocall or just send it directly to voice mail. In that case, it is even one better. The only calls that come through are from people that you know or the calls that should happen.

This is a story that literally just happened last month. My uncle wound up in the hospital unexpectedly. The ambulance had to come pick him up. And he called, and I didn't recognize the number. But I trust my product. I answered it. It turns out that he was in the hospital, and he told me what room he was. I had to go and pick up some stuff

from his house for him.

If I didn't answer unknown calls, I don't know what would have happened.  And, ironically, when I went to pick up his --

Mr. <u>Bilirakis.</u>  That is a good example.  That is my greatest fear.

Mr. <u>Foss.</u>  That is exactly right and it is really important. And, again, this is not a made-up story.  And, no joke, when I went to pick up his stuff, he has an old flip phone, feature phone, it rang. And I figured it was one of his friends who was calling to find out what is going on.  I answered it, and no exaggeration, it is, "You have won a free cruise."

So on that point I was laughing because of all that was going on. But I am like, even I can't protect my uncle because he doesn't have the latest technology.

So in one case the robocall blocking apps actually -- I was immediately able to get in touch with the people that I care about that are having issues, and on the other hand, it was, wait, this same call, the same technology could have taken advantage of my uncle.

Mr. <u>Bilirakis.</u>  Anyone else want to comment on that?

Mr. <u>Hambuchen.</u>  Yes, Congressman, I will just add that at First Orion consumer choice is paramount.  For our default solutions and carrier networks the labeling is what takes place.

So you see the call with a label of Scam Likely or some other label, and then the consumer has the option to actually block any of these calls in the future so that their phone won't ring.  And for non-Scam

Likely tags, those things can actually be forwarded over to their voice mail so they don't miss a call if something did get blocked.

Mr. <u>Bilirakis.</u>  I have a question here.  I know I am running out of time.  Mr. Chairman, would you allow me to ask a question?

Mr. <u>Latta.</u>  Sure.

Mr. <u>Bilirakis.</u>  Why don't I submit it for the record.

But I just want to make a statement.  Our constituents should not have to deal with this.  They should have the right to enjoy the privacy in their own home.  They shouldn't even have to play defense, in my opinion.  So we have to do something about this.

But I appreciate what you are doing to protect our constituents.

But this is an issue we hear about on a daily basis from family members.  My dad was a member of this committee.  He complains to me all the time about these robocalls, and he is right.

So thank you very much for what you do.

Thank you for holding the hearing, Mr. Chairman.  And I will yield back and submit the question.

Mr. <u>Latta.</u>  Thank you.  The gentlemen yields back.

The chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes.

Mr. <u>Pallone.</u>  Thank you, Mr. Chairman.

I am glad to hear that industry groups have been working on technology to root out caller ID spoofing with a system that can verify a call's true origin, and the call authentication trust anchor has been in development for some time now.

My questions are of Ms. Mahoney.

Do you support creating a call authentication trust anchor so that consumers know who is really calling them?

Ms. Mahoney. Thanks for your question.

There is broad consensus that caller ID authentication can be an important step in order to address the problem of call spoofing.

And as my copanelists have mentioned, call spoofing and neighbor spoofing have become increasingly concerning. They do make it difficult for many call-blocking technologies to function. They allow spoofers to hide detection, which makes enforcement difficult, and generally just makes the robocall problem worse.

So caller ID authentication has been in development for many years. This is a technology that would allow the originating provider to confirm or validate the accuracy of the caller ID information so that that can be traced all along the call path.

And we would like to see the phone companies be required to implement some form of caller ID authentication with a certain set of consumer-friendly standards. For example, it should be free. It should have the capability to block spoofed calls as well.

Mr. Pallone. Well, in July of last year the FCC started a process to explore the creation of a call authentication trust anchor, but the effort seems to have stalled out.

So today I am releasing a discussion draft of the Stopping Bad Robocalls Act, and one provision in my draft bill would set a 1-year deadline for the FCC to adopt rules to create such a trust anchor to

ensure consumers know who is calling when they answer the phone.

So, again, Ms. Mahoney, do I understand correctly that Consumers Union supports a deadline to get this call authentication program in place?

Ms. Mahoney. Again, thank you for your efforts to help spur this technology. We would like to see the FCC issue rules and require the phone companies to implement this technology by a certain deadline.

Mr. Pallone. Now, how would creating a call authentication system help put an end to bad actors masking their caller ID information or spoofing and preying on unsuspecting consumers, and seniors in particular?

Ms. Mahoney. Well, since call spoofing has made it so difficult for call blocking, again, from enforcement efforts, and it tricks consumers into picking up their phone, cracking down on call spoofing would improve the functioning of call-blocking tools and it would allow consumers to trust their caller identification information again.

Mr. Pallone. Now, would an authentication system also make enforcement easier by helping track the source of illegal robocalls?

Ms. Mahoney. Yes. That has been a focus of the phone companies in order to speed up this process. Since calls are routed through multiple carriers, it can be time consuming to track them down to their original location.

The phone companies have been exploring things like trace back to speed this process. But caller ID authentication would overall speed up this process and make it much more effective.

Mr. Pallone. Well, you mentioned in your testimony that because of a court ruling, the definition of autodialer is unclear. In the wake of that court case, do you generally support a clarification of that definition?

Ms. Mahoney. Yes. The ball is in the FCC's court in order to clarify a definition of an autodialer that protects all consumers and the existing autodialers that are in use. But we appreciate any assistance in that.

Mr. Pallone. And I have also heard that many consumers are plagued by robocalls they receive as a result of reassigned phone numbers.

Do you support requiring the FCC to establish a nationwide database of consumer telephone numbers that have been reassigned to other consumers so we can help stop these annoying calls?

Ms. Mahoney. Yes. We urge the FCC to implement regulations to create the reassigned number database, as proposed, in order to cut down on this problem of wrong number robocalls.

Mr. Pallone. And the bill I released, I mentioned, addresses the issue with the definition of an autodialer and would require the FCC to establish a database of reassigned numbers.

I know we have heard a lot of about neighbor spoofing, but I recently heard from a constituent about something perhaps even more alarming. Instead of the first six digits looking like her phone number, so she would think it was a neighbor calling, the first six digits looked like a phone number of a relative that frequently calls.

I don't know how the spoofing companies would know what calls are coming in, but if there is some sort of access to caller information, I think we should stop it.

Do you have any thoughts on this report that I am mentioning?

Ms. <u>Mahoney.</u>  I have not personally heard from any consumers about this happening, but scammers are smart and they are constantly thinking of ways in order to trick consumers into handing over their money or personal information, so I wouldn't put it past them.  And certainly we hear often about neighbor spoofing, in which the first six digits are spoofed.

Mr. <u>Pallone.</u>  All right.  Thank you so much.

Thank you, Mr. Chairman.

Mr. <u>Latta.</u>  Thank you.  The gentleman yields back.

The chair now recognizes the gentleman from South Carolina for 5 minutes.

Mr. <u>Duncan.</u>  Thank you, Mr. Chairman.  Thanks for this timely hearing.

I got a Facebook post on my feed the other day from a constituent. She said this:

"I realize we deregulated cell phone marketing awhile back. Woo-hoo.  But the Do Not Call options don't work.

"I am on a Do Not Call list," she said.  "I punched the number to take me off the list and they just call from another number, a number that, by the way, you can't call back.  Yes, you can block, and I do, but the bots just call from another number.

"What kind of scam business thinks this works?  I wouldn't in a million years get their extended warranty, health insurance, et cetera."

I, too, have been called just recently by the IRS.  Apparently I was involved in some tax fraud, and if I didn't call them right away, I face jail time.

I called them back, or I answered one of their calls, it came right in, I can't remember if I called back, whatever, because I wanted to know.  I told them who I was.  I told them that I was going to investigate whether they were legitimate.  And I said, "If you are a fraud, we will find out, and the authorities will knock on your door."

The guy offered to give me his badge number and to spell his name.  He didn't do a very good job pronouncing his name and definitely couldn't spell it.  He had to spell it per letter, A as in apple, that sort of thing.  I never did get his name right because he didn't speak English very well.

Then just this week I was called by the Social Security.  They were out of Texas.  But they called me and said that I was involved in Social Security fraud.

For the people that are watching, the IRS does not call you and the Social Security Administration does not call your phone.  They send you something in the mail and you call them.

So I want all the people across America not to fall for this scam.  But it raises an important issue that we are talking about today.

And I want to ask you guys.  Let's take a hypothetical scenario

that a robocaller would get hold of a home security company that a consumer uses or a bank number even, a number that they would recognize, and they started using that.

How would it work in your system if that happened, if they spoofed a legitimate number, not one of the cell phone exchanges from my area that I would recognize?  "Well, maybe that is somebody that I know and I don't have them in my contacts."  They use a legitimate number that might be your local bank, and the consumer wouldn't complain about that number because they don't want to not have their bank call them, right?  What would happen and how would that work?

Mr. Garr.  That is a great question.  And I think it is really important when you think about call-blocking technology that it is just as important that you are removing numbers from the list as adding numbers to the list, and that is what we think we do really well.

Our algorithms are working in real-time to understand patterns of calls.  So what you are describing, if it happens, it is very unlikely that it is a single call coming from that number.  It is multiple calls coming from the same number, even if they are spoofing a legitimate number.

We see that spike because we have a large ecosystem of users, we have just on RoboKiller 164,000 users now, a large ecosystem of users potentially seeing that call.

If we are seeing that call in real-time come in, we know that it is likely a scam, and we are able to prevent, block against that.  So we are an able to adapt really quickly.

And I think, going back to what you are saying, consumers should always remember when the phone rings, my grandfather's principle, which is honest people are always willing to put things in writing.

So if you get a call and someone is asking you for personally identifying information, even a company you work with, ask yourself why, and say, "You know what, if you want to ask me that question, send me a certified letter."

Scammers aren't going to take the time.  Again, this is all about time.  Scammers want to get past you, as a skeptic, and get to somebody they can target.  They want to get to the vulnerability people.

Mr. Duncan.  And it is the seniors that are the most vulnerable in this.  I really think there ought to be a public service commercial that runs on the TV during the time that seniors are watching to warn them that the IRS will never call you, don't give any of your personal information.

We have done a lot.  All of us have done messaging within our ability.

Let me ask you this.  Could they theoretically spoof the House of Representatives' number and put that in?

Mr. Garr.  Sure.  Caller ID is not something that you should automatically trust or can automatically trust.

But spoofing is a complicated issue.  I mean, I don't know what phone system you use, but there is a very good chance that the phone system in this building spoofs calls.  Spoofing is not a monolith. Spoofing is used for legitimate purposes all the time.

Mr. Duncan. Spoofing is used for legitimate purposes all the time?

Mr. Garr. Absolutely.

Mr. Duncan. Give me an example. Give the committee an example of that.

Mr. Garr. Sure. My stepfather is a veterinarian. When he has to call a client back at night for an emergency he spoofs his office number so that he is not giving away his personal home number or mobile number, and also so that his customer knows that it is him calling, it is his animal hospital calling.

Lots of people use spoofing for legitimate purposes all the time. Again, it is not just a monolith, you can't look at it and say all spoofing is bad.

Mr. Duncan. Just by the use of the word "spoof" tells me it is bad, that you have got to use that terminology.

Mr. Garr. Yeah, it has a terrible connotation.

Look, I am not saying that robocallers aren't using it for illegitimate purposes and that is not a problem we need to work on. What I am saying is that spoofing is a tool, and people are using it for legitimate purposes all the time.

Somebody used the example of your pharmacy calling you. When you see CVS calling you, it is always CVS. How do they do that calling from multiple CVS's? Probably using spoofing. I can't say that for 100 percent sure. But spoofing is used all the time to maintain a consistent --

Mr. <u>Duncan.</u>  Just that phrase, Mr. Chairman, that spoofing is used for legitimate purposes strikes me as odd.

I know I am out of time.  Thank you so much.  I yield back.

Mr. <u>Latta.</u>  Thank you very much.  The gentleman's time has expired.

The chair recognizes the gentleman from Kentucky for 5 minutes.

Mr. <u>Guthrie.</u>  So to follow on that point he just made.  So if one of us uses our personal cell and calls a constituent back and it shows up U.S. House of Representatives, our office number, that is spoofing, by definition?

Mr. <u>Garr.</u>  I think you are saying using your mobile number?

Mr. <u>Guthrie.</u>  Yeah, using my own personal number and the office number shows up on their caller ID.

Mr. <u>Garr.</u>  What I was more saying is that if you are calling from an office number here and it says U.S. House of Representatives, there is probably, in a building this size, hundreds of different phone numbers, hundreds of different phone lines.  The system, I think it is called the PBX, is using spoofing so that you maintain that unique number that the person on the outside sees on their caller ID.

Mr. <u>Guthrie.</u>  Okay.  I see what you are saying.  All right. Thanks.  I was just asking if that was an example.

So I have a question for the technology companies addressing the issue head on.  Mr. Foss and Mr. Garr and Mr. Hambuchen, do any of your companies approach the robocall problem by diverting calls to voice mail directly?  And have provider's legitimate call originators or any

regulators expressed concerns about that?

Mr. <u>Foss.</u>  I think you have touched on something very important. And the wording that we all use, again the spoof, the setting of the caller ID, when we say blocking or stopping, labeling those, I think it is really important, you have touched on something really important.

On our product, on mobile, when we say block the call, that is shorthand for it goes directly to voice mail.  One of the other representatives said, like, if you don't answer it, it is just like declining it and then they don't leave a message.

That is incredibly safe because everybody misses calls all the time.  Everybody is always kind of worried, "Oh, are we going to miss it."  Like, we just dump it to voice mail.

On our mobile product, when we say that we block a call or stop a call, we actually prompt the user to type in a captcha.  So it says, "This phone is protected by Nomorobo, please type the number 3286." It picks a random number.  And if they type it in, proving they are human, we let the call through.

So it is really important to understand that, right, blocking the call and making it disappear into the ether is not the right way to do it.

But putting up a challenge, getting them over to voice mail and then allowing the user to go and check that or to add that to their contacts, that is really what we are talking about when we are talking about stopping the call.  It is really important.

Mr. <u>Guthrie.</u>  Okay.  Any other answers from the other two of you?

Mr. Hambuchen. Sure. At First Orion the approach we take is we are labeling calls with Scam Likely when we know it is a scam. We also have other labels, such as Telemarketer or Nuisance Likely, based on what we know about that number.

As I mentioned, we think consumers should have choice. And so consumers can see the label for any of these calls, but can also have those calls what we would call blocked.

Scam Likely calls, when we say blocked, they go away, they don't go to voice mail. All the other types of calls would go to voice mail. So if it was a telemarketer, a survey, account service, or some other type of label, those would go to your voice mail.

Mr. Guthrie. Okay.

Mr. Garr. Yeah, if I can just say, some originators have complained. But, again, our users are looking for control of their phones. It is their phones, not the originator's, not anyone else's.

There is a difference between legal and illegal versus wanted and unwanted and our users are asking us to prevent unwanted calls.

Just because a debt collector may be a legal telemarketer and just because a political robocall -- and I understand why you guys may use them at times -- may be a legal call, that doesn't mean that the consumers want to receive them. So it is really important that we give them the control to do that.

But, again, we are forwarding the calls -- we are controlling -- we are answering the calls that we are blocking. That gives the users control over those calls to decide what to do with those

calls after the fact.  They can hear these Answer Bots.

Mr. <u>Guthrie.</u>  Okay.  Thank you, Mr. Garr.  I will continue with you.

What can be done to enhance consumer education from a parent's child who might be getting their very first smartphone, for a senior citizen with a traditional landline, and a mobile phone?

Mr. <u>Garr.</u>  Again, I think there are a couple things that you should always be teaching people about the use of their phones.  One is that caller ID is not something you can trust out of hand.  And when someone calls you, unless it is someone directly that you know, a really trusted source, there is no reason ever to give them your personally identifying information.

Especially when they are using time to put pressure on you, that is the time to push back and say, "If this is a legitimate call, if this is a legitimate request, put it in writing, I will be happy to answer you."

Like I said, my grandfather always said, honest people will always put things the writing, and I think that is a principle that we should always adhere to when we are thinking about this these calls.

But, again, if you put something like RoboKiller on your phone and you get Answer Bots working for you, you are preventing these calls from ever even reaching you and you are protecting yourself and the people around you.

Mr. <u>Guthrie.</u>  Okay.  Thank you.

And I am about out of time so I will yield back.

Mr. <u>Latta.</u> Thank you very much. The gentleman yields back.

The chair recognizes the gentleman from Oklahoma for 5 minutes.

Mr. <u>Mullin.</u> Thank you, Mr. Chairman.

And thank you guys for taking the time on this day to just come and visit with us. We all know it is a problem. It is just unique to find individuals that are putting so much time to it.

You know, used to be you could just kind of get rid of your landline and that solved the issue. Now even my cell phone, as my colleagues have stated up here, their cell phones are being called now.

So can you guys just kind of elaborate, how effective are the Do Not Call lists from State to national? Are they even worth the time that we put them in place?

Go ahead, Mr. Foss.

Mr. <u>Foss.</u> So the Do No Call Registry was created back in the early 1990s with the TCPA, it was implemented in the early 2000s. Think of the world back then. We didn't have cell phones. The Internet didn't exist.

Mr. <u>Mullin.</u> We did, but they were bag phones.

Mr. <u>Foss.</u> Exactly. Car phones, right.

The world has changed. So at that time it was legitimate telemarketers and there was no way to get off of the -- to tell them to stop. That made sense then as an opt-out mechanism. Legal robocallers, they will go and follow the rules.

Today the robocallers don't follow the rules. Nobody is downloading the Do Not Call list. It is like having a Don't Rob Me

list and that all the criminals have to go in.  And, look, it hasn't kept up with the time.

I personally think that we should clarify that everything is just opt-in.  If you are calling somebody to sell them something, anything with money, to collect a debt or something, I just think you need to have express written permission.  It would save a lot of this whole, you know, the patchwork of regulations and rules and clarifications, and this law came in and this was taken and that, if you have to opt in.

Mr. Mullin.  But how could you opt-in, because I don't think anybody gave them their phone numbers to begin with.

Mr. Foss.  Correct.

Mr. Mullin.  So how would that system work?  Because it is not enforceable the way that it is now.  I don't think anybody opted in to begin with.

Mr. Foss.  Correct.  If it was opt-in, and we could basically say, which is pretty much what we are trying to say right now, is that any of those types of calls are illegal, right, and therefore the --

Mr. Mullin.  My point is, is that if you are already on the Do Not Call list, it already is illegal, but it is not being enforced.

Mr. Foss.  If you are on the Do Not Call list and they call a landline, there are all these different kind of -- the truth in this lies in the gray area, right?

And then when the carriers, the different regulations and things, when it gets that one bad actor, and they say, well, common carrier,

we don't have to -- these criminals are always going to look for that one little sliver and go and run through there.  And at best, it is going to take years to go and litigate.

If those things were more, "Did you have express written permission to call that person?" okay, show it to me.

Mr. Mullin.  Even what you said earlier, though, you don't need more regulations, just what is put in place, you actually would.  If you put in opt-in, you would have to have regulations that stated that you have to opt-in, but then the enforcement arm is still there.  Well, the enforcement arm isn't working on the Do Not Call list.

So explain to me how that would work, because we are all in.  I mean, we would be all in on that.  Do you we need to give the FTC or the FCC more broad powers, more teeth?  Is that how that works?  Because you have got to have it -- regulations have got to take place for even the opt-in process.

Mr. Foss.  So let me give you an exact example of this.  They are always kind of skirting around this.

Mr. Mullin.  We know they are skirting around.

Ms. Foss.  Right.  What is an ATDS, what is an automated telephone dialing system?  Now there are a lot of the debt collection companies, HCI, they will manually push a button, they will have somebody, which gets around all the TCPA laws.

I don't even care if those calls are made with an automated dialer, I don't care if it is made from a computer, I don't care if it is somebody that is pushing that button, if you are trying to sell somebody, to

scam somebody, to take some money, do something like that, yeah, you should not be able to do that.

And then I would think it would give more teeth to the FTC to go after these and the FCC would be able to give a lot less cover.

Mr. Mullin. All that is great, but it still goes back to the same thing. It doesn't make any difference if it is not enforceable.

Mr. Foss. Correct.

Mr. Mullin. If someone else want to jump in this. How would you enforce it?

Ms. Mahoney. I do think it is important that consumers have legal protections against unwanted robocalls. Phone companies are reluctant to block so-called legal robocalls. So if consumers don't have these protections, they won't be able to take advantage of some of the blocking.

Mr. Mullin. How would it be enforced? That is what I am trying to get to. Does anybody have an idea how this thing could be enforced, how Congress could help push that to the next level?

Mr. Garr. Truthfully, I don't think a Do Not Call list is the solution.

Mr. Mullin. I agree. Well, it is not working, obviously.

Mr. Garr. I don't think it can. I mean, there is even a theory that the Do Not Call list actually empowers telemarketers, because if people get a call who are on the Do No Call list, they automatically by default think, "Well, it must be legitimate, I am on the Do Not Call list. So I will answer this question."

So the telemarketers have this thought that, "Hey, if I get someone on the Do Not Call list, they are an even better target." I don't think legislation alone is the solution.

Mr. <u>Mullin.</u> Just technology.

Mr. <u>Garr.</u> I think technology is the solution.

Mr. <u>Mullin.</u> So that leads to my question, where I was trying to get to. So it is not regulation in your-all's opinion, it is the private industry that is going to drive the end to robocalls essentially.

Mr. <u>Garr.</u> We believe we are already doing it.

Mr. <u>Mullin.</u> Do you agree?

Mr. <u>Hambuchen.</u> Sure. I would just add one thing. I think you are right in terms of technology and innovation are what is going to solve the problem. And recently, over the last couple of months, the rules were clarified on enabling carriers to start blocking scam calls, unwanted nuisance calls for consumers.

So allowing that, allowing industry to start spurring innovation on top of that, I think you are going to see an explosion over the next couple of years of solutions to combat the problem.

Mr. <u>Mullin.</u> Thank you. And I am out of time. Thank you so much, once again, for being here and taking the time.

This is something, I feel like, that we are going to be relying more and more on private industry to drive and help solve this problem, which is typically what happens in our country to begin, which is great. The government's responsibility is to help you guys, you entrepreneurs,

go out and thrive and create and solve problems or create opportunity.

So thank you for doing what you are doing.  Appreciate it.

Mr. Latta.  Thank you very much.  And the gentleman's time has expired, and seeing no other members wishing to ask question.

I also want to thank our witnesses for today's hearing.  It has been very, very informative.  Because, again, it is an issue out there that we all hear about, and I tell you, as the gentleman from South Carolina that not only heard from the IRS, but the Social Security. But it is an issue and we hear it.  And people say, "What are we supposed to do?"

And some people, I have heard, in our districts, they actually fall for it and they send the money in.  And all of a sudden they find out they are $5,000, $10,000 out, and they don't have $5,000 or $10,000 to be out.  So it is really important that the public is protected out there, and that is what we are here to do.

So again, I want to thank you all for being here.

But before we do conclude today, I want to also include the following documents to be submitted for the record by unanimous consent.  A joint letter from multiple trade associations.  A letter from the Electronic Privacy Information Center.  A letter from CTIA. A letter from USTelecom.  And a letter from the U.S. Chamber Institute for Legal Reform.

[The information follows:]


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

Mr. <u>Latta.</u>  Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record.  And I ask that witnesses submit the response within 10 business days upon receipt of the questions.

And without objection, the subcommittee will stand adjourned. Thank you very much for being here.

[Whereupon, at 10:38 a.m., the subcommittee was adjourned.]